科学研究費補助金 特定領域研究

新世代の計算限界
— その解明と打破 —

研究課題別成果報告書 分冊 B

平成 20 年 4 月

領域代表者　岩間 一雄
京都大学 大学院 情報学研究科　教授

目 次

文部科学省科学研究費補助金 特定領域研究 (課題番号 16092205)

B01: 代数的および確率的手法による離散構造の限界の究明

本研究では，置換族の構成，双対符号の距離構造，ネットワーク制御，電子商取引，VLSI 計算，可逆計算，及び耐故障計算などにに関する離散構造の限界を解明した．置換族の構成に関しては，最小値独立置換族と k-限定近似的独立置換族のサイズの上界・下界を導出した．双対符号の距離構造に関しては，共通鍵暗号への応用からの要請を満たす線形符号の双対符号に対して，その距離構造の下界を導出した．ネットワーク制御に関しては，QoS アルゴリズムの競合比の上界・下界を導出した．電子商取引に関しては，顧客数と商品数の比に関して，乱択化最適選好マッチングが存在するためのほぼ合致する上界と下界を導出した．VLSI 計算に関しては，特に 3 次元チャネル配線問題が $\mathcal{NP}$ 困難であることなどを明らかにした．可逆計算に関しては，特に可逆回路の縮退故障に対する最小完全テスト集合生成問題が $\mathcal{NP}$ 困難であることなどを示した．耐故障計算に関しては，特に様々なネットワークに対して効率的な確率的耐故障ネットワークを構成する統一的な手法などを提案した．

研究組織

研究代表者： 伊東 利哉　東京工業大学 学術国際情報センター
研究分担者： 上野 修一　東京工業大学 大学院 理工学研究科

交付決定額 (配分額)

平成 16 年度	3,900,000 円
平成 17 年度	3,700,000 円
平成 18 年度	3,600,000 円
平成 19 年度	2,600,000 円
合　計	13,800,000 円

研究成果の概要

- 学術誌
  Discrete Applied Mathematics (2004 年, 2005 年)，IEICE Trans. on Fundamentals (2004 年, 2005 年, 2006 年, 2007 年)，IEEE Trans. on Information Theory (2006 年)，Random Structures and Algorithms (2007 年) など
- 国際会議
  COCOON (Jeju Island, Korea, 2004 年)，SOFSEM (Liptovsky Jan, Slovakia, 2005 年)，ISCAS (神戸, 2005 年)，ISCAS (Island of Kos, Greece, 2006 年)，HJ-SDMA (仙台, 2007 年)，ISCAS (New Orleans, USA, 2007 年)，ISAAC (仙台, 2007 年) など
- 著書
  情報とアルゴリズム（2005 年），情報基礎数学（2007 年）など
- 受賞
  電子情報通信学会フェロー（2006 年）など

1 緒言

平成16年度から平成19年度の研究期間において，離散構造の限界の解明に関して研究を進めた．特に，伊東は，

(1) 置換族の構成に関する研究
  (a) 最小値独立置換族の構成に関する研究
  (b) k 制限独立置換族の構成に関する研究

(2) 線形符号の双対距離と共通鍵暗号への応用に関する研究

(3) ネットワーク制御に関する研究

(4) 電子商取引アルゴリズムに関する研究
  (a) 最適選好マッチングに関する研究
  (b) 価格設定問題に関する研究

を通じて離散構造の解明を行い，一方，上野は

(5) VLSI 計算に関する研究
  (a) 3 次元レイアウトに関する研究
  (b) 3 次元チャネル配線に関する研究
  (c) 3 次元単層配線に関する研究
  (d) グラフの直交描画に関する研究
  (e) VLSI 分解に関する研究

(6) 可逆計算に関する研究
  (a) 可逆回路の故障検出に関する研究
  (b) グラフの量子計算に関する研究

(7) 耐故障計算に関する研究
  (a) 逐次故障診断に関する研究
  (b) 確率的耐故障ネットワークに関する研究

(8) ネットワーク計算に関する研究
  (a) スケジューリングに関する研究
  (b) ルーチングに関する研究
  (c) 光結合ネットワークに関する研究

を通じて離散構造の解明を行った．個別の研究内容に関しては，第2章以降で詳細に述べるが，各テーマ毎の研究の概略は以下の通りである．

1.1 置換族の構成に関する研究

最小値独立置換族の構成に関する研究

最小値独立置換族 (とその拡張概念である ε 近似 k 制限最小値独立置換族) は，インターネット上に存在する類似した文書の特定に有用であることが知られている，また，これまでに最小値独立置換族と ε 近似 k 制限最小値独立置換族の構成法及び置換族のサイズに関する (非) 構成的上界・下界が数多く示されているが，未だに ε 近似 k 制限最小値独立置換族のサイズの上界・下界には大きな隔たりがある．そこで本研究では，代数的手法を用いて ε 近似 k 制限最小値独立置換族のサイズに関する良好な下界を導出した．

k 制限独立置換族の構成に関する研究

ε 近似 k 制限ランダム置換族は，乱択アルゴリズムの非乱択化などの応用を持つ理論計算機科学における重要な概念の一つとして知られているが，任意の $k \geq 4$ に対して，多項式時間抽出可能な ε 近似 k 制限ランダム置換族の構成法はこれまでに知られていなかった．そこで本研究では，代表的な共通鍵暗号 DES の基本要素である Feistel 変換を用いて対数領域抽出可能な ε 近似 k 制限ランダム置換族の構成法を導出し，カップリング法を用いてその近似精度の解析を行なった．

1.2 線形符号の双対距離と共通鍵暗号への応用に関する研究

共通鍵暗号の安全性は，差分攻撃及び線形攻撃に対する耐性によって評価されるため，差分攻撃及び線形攻撃に対してある種の一様性が保証されたブール関数の設計が重要となる．そのような一様性を持つ (コンパクトな) ブール関数の設計は，任意の整数 d と $d^{\perp}$ が与えられたとき，符号 $\mathcal{C}$ の最小距離は d であり，符号 $\mathcal{C}$ の双対符号 $\mathcal{C}^{\perp}$ の最小距離は $d^{\perp}$ であるような符号 $\mathcal{C}$ の最小符号長 $n = N(d, d^{\perp})$ を求める問題に帰着される．そこで本研究では，任意の整数 $d, d^{\perp}$ に対して $N(d, d^{\perp})$ の上界を評価するとともに，代数的手法を用いてその良好な下界を導出した．さらに，計算機実験により，これらの上界・下界の良好性を確認した．

1.3 ネットワーク制御に関する研究

QoS アルゴリズムの競合比の解析について考察した．各種のパケットをその優先度に応じて効率的

に転送制御するための複数キュー QoS アルゴリズムに関して検討した．一般に QoS スイッチに到来するパケットを事前に予測することは不可能であるので，QoS アルゴリズムはオンラインアルゴリズムとして定式化される．そして，キューに格納されているパケットを破棄することが許されるパケット破棄可能モデルと破棄することが許されないパケット破棄不可能モデルの双方に着目し，複数優先度を持つ複数キュー QoS アルゴリズムの競合比の解析を行ない，良好な上界を示すとともに，これまで知られていた下界を改善した．

1.4 電子商取引アルゴリズムに関する研究

最適選好マッチングに関する研究

n 人の顧客が各々の m 個の商品に対する希望リストを提示し，供給者が顧客の満足度を最大化する商品配分は最適選好マッチング (popular matching) と呼ばれる．本研究では，顧客が優先度に応じて 2 つのグループに分割されている場合において，各顧客の希望リストが商品集合上の一様独立な乱択ベクトルで与えられるとき，$n^{4/3}/m = o(1)$ であるならば高い確率で最適選好マッチングが存在し，$m/n^{4/3} = o(1)$ であるならば高い確率で最適選好マッチングが存在しないことが示した．

価格設定問題に関する研究

m 個の商品に対して n 人の顧客の各々が購入希望商品群に関する購入可能金額を提示するとする．ここで，売主が利益が最大となるように各商品の価格を設定す問題を価格設定問題という．本研究では，正値モデル・割引モデル・無損失割引モデルなどの様々な価格モデルにおける価格設定問題に関して，良好な近似アルゴリズムを導出した．

1.5 VLSI 計算に関する研究

VLSI 計算に関しては，3 次元レイアウト，3 次元チャネル配線，3 次元単層配線，グラフの直交描画，及び VLSI 分解などの研究を行った．そして，3 次元レイアウトの最小体積の上限・下限，3 次元チャネル配線の高さの上界・下界，多項式時間 3 次元単層配線可能性，外平面的グラフおよび直並列グラフの 2 次元直交描画可能性，d 値 D 次元の deBruijin ネットワーク族の万能ブロックの効率の上界・下界などを明らかにした．

1.6 可逆計算に関する研究

可逆回路の故障検出に関する研究

出力ベクトルの集合が入力ベクトルの集合の置換であるような論理回路を可逆論理回路と言い，低消費電力設計，デジタル信号処理，ナノ・量子計算などの応用を持つことが知られている．本研究では，可逆論理回路の全て配線上の縮退故障を検出する最小完全テスト集合生成問題が $\mathcal{NP}$ 困難であることを示し，可逆論理回路の故障検出問題の計算複雑度を明らかにした．

グラフの量子計算に関する研究

グラフの最小全域木問題や最短路問題などに対しては, 古典的アルゴリズムよりも高速である量子アルゴリズムが知られている．本研究では, 全点対間最短路問題の量子計算量の非自明な下界 $\Omega(\sqrt{m^3/n^2})$ を導出し，特に $m = \omega(n^{3/2})$ であるときには，この下界が既存の下界の改良となっていることを明らかにした．

1.7 耐故障計算に関する研究

逐次故障診断に関する研究

並列計算システムの故障診断において，一度に全ての故障ユニットを同定する同時診断と一度に一つの故障ユニットを同定する逐次診断が知られている．本研究では，様々なシステムでの逐次診断可能次数の非自明な上界・下界を導出した．

確率的耐故障ネットワークに関する研究

ネットワーク G に対して，ネットワーク G^* が G の確率的耐故障ネットワークであるとは，ネットワーク G^* において，定確率で独立にプロセッサが故障しても正常なプロセッサからなるネットワーク G を高い確率で含んでいることを言う．これに関して，N 個のプロセッサと M 本の通信リンクか

らなる任意のネットワーク G に対して，以下の公開問題が知られている．(1) $O(N)$ 個のプロセッサと $O(M\log^2 N)$ 本の通信リンクからなる確率的耐故障ネットワーク G^* が存在するか; (2) $O(N)$ 個のプロセッサと $o(M\log^2 N)$ 本の通信リンクからなる確率的耐故障ネットワーク G^* が存在するか否か．本研究では，様々なネットワーク — Cayley ネットワーク，deBruijin ネットワーク，シャッフル交換ネットワーク，部分 k 木ネットワーク — に対して，$O(N)$ 個のプロセッサと $O(M\log N)$ 本の通信リンクからなる確率的耐故障ネットワークが存在することを明らかにした．

1.8 ネットワーク計算に関する研究

ネットワーク計算に関しては，スケジューリング，ルーチング，及び光結合ネットワークなどの研究を行った．そして，通信網において先行制約のあるメッセージの集合の最短送信スケジュールを求める問題の困難性およびそれに対する近似アルゴリズムを提案した．また，マルチキャスト通信の通信コストに関して，直並列ネットワークに対する擬似多項式時間アルゴリズムを提案した．さらに，WDM 光ネットワークにおいて，ルーチング問題が $\mathcal{NP}$ 困難であることを示した．

2 置換族の構成に関する研究

2.1 最小値独立置換族の構成に関する研究

任意の整数 $a \le b$ に対して $[a,b] = \{a,\ldots,b\}$ とする．また，任意の整数 $n \ge 1$ に対して S_n を集合 $[0,n-1]$ 上の置換全体を表すものとする．

定義 2.1 任意の $0 < \varepsilon < 1$ と任意の整数 $k \ge 3$ に対して，置換族 $\mathcal{F} \subseteq S_n$ が ε 近似 k 制限最小値独立であるとは，以下が成り立つことを言う*:* 任意の (空でない) 集合 $X \subseteq [1,n]$ (ただし $|X| \le k$) と任意の $x \in X$ に対して，

$$\left| \Pr_{\pi\in\mathcal{F}}[\min\{\pi(X)\} = \pi(x)] - \frac{1}{|X|} \right| \le \frac{\varepsilon}{|X|}.$$

ただし，置換 π は置換族 $\mathcal{F}$ 上の分布 $\mathcal{D}$ に従って選択されるものとする．

これまでに ε 近似 k 制限最小値独立置換族 $\mathcal{F} \subseteq S_n$ のサイズに関して，以下のことが知られている:

$$\begin{aligned}
&\text{上界}: \quad |\mathcal{F}| = 2^{4k+o(k)}k^{2\log\log(n/\varepsilon)} \text{ (構成的)};\\
&\text{上界}: \quad |\mathcal{F}| = O\big(\tfrac{k^2}{\varepsilon^2}\log(n/k)\big) \text{ (非構成的)};\\
&\text{下界}: \quad |\mathcal{F}| = \Omega\big(k^2(1-\sqrt{8\varepsilon})\big);\\
&\text{下界}: \quad |\mathcal{F}| = \Omega\Bigg(\min\Bigg\{k^2 2^{k/2}\log(n/k),\\
&\qquad\qquad \tfrac{\log(1/\varepsilon)(\log n - \log\log(1/\varepsilon))}{\varepsilon^{1/3}}\Bigg\}\Bigg).
\end{aligned}$$

任意の整数 $k \ge 3$ に対して $s = k/3, L = n/s$ とする (簡単のため s, L は整数とする)．ここで集合 $[1,n]$ をサイズが s の互いに背反な L 個の部分集合 $X_0, X_1, \ldots, X_{L-1}$ に分割する: 各 $i \in [0, L-1]$ に対して $X_i = \{si+1, si+2, \ldots, (i+1)s\}$. 任意の定数 $\varepsilon > 0$ に対して置換族 $\mathcal{F} = \{\pi_1, \pi_2, \ldots, \pi_d\} \subseteq S_n$ を ε 近似 k 制限最小値独立とする．また $N = L - 1 = n/s - 1$ とし，各 $h \in [1,s]$ に対して，以下のような $N \times d$ 行列 $U_h = (u_{ij}^h)$ を定義する．

$$u_{ij}^h = \begin{cases} \dfrac{1}{\sqrt{d}} & \min\{\pi_j(X_0 \cup X_i)\} = \pi_j(h);\\ 0 & \text{その他}. \end{cases}$$

さらに各 $h \in [1,s]$ に対して，以下のような $N \times N$ 行列 $V_h = (v_{ij}^h)$ を定義する．

$$\begin{aligned}
V_h &= (v_{ij}^h) = U_h U_h^T\\
&= \begin{bmatrix}
\frac{\delta_{11}^h}{2s} & \frac{\delta_{12}^h}{3s} & \frac{\delta_{13}^h}{3s} & \cdots & \frac{\delta_{1N}^h}{3s}\\
\frac{\delta_{12}^h}{3s} & \frac{\delta_{22}^h}{2s} & \frac{\delta_{23}^h}{3s} & \cdots & \frac{\delta_{2N}^h}{3s}\\
\frac{\delta_{13}^h}{3s} & \frac{\delta_{23}^h}{3s} & \frac{\delta_{33}^h}{2s} & \cdots & \frac{\delta_{3N}^h}{3s}\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
\frac{\delta_{1N}^h}{3s} & \frac{\delta_{2N}^h}{3s} & \frac{\delta_{3N}^h}{3s} & \cdots & \frac{\delta_{NN}^h}{2s}
\end{bmatrix}.
\end{aligned}$$

仮定より置換族 $\mathcal{F} \subseteq S_n$ は ε 近似 k 制限最小値独立なので，任意の $i,j \in [1,N]$ に対して $1-\varepsilon \le \delta_{ij}^h \le 1+\varepsilon$ が成り立つ．従って以下を得る．

補題 2.1 行列 $V_h = (v_{ij}^h)$ に関して以下が成立*:*

(i) 任意の $i \in [1,N]$ に対して

$$\frac{1-\varepsilon}{2s} \le v_{ii}^h \le \frac{1+\varepsilon}{2s};$$

(ii) 任意の $i,j \in [1,N]$ *(ただし $i \neq j$)* に対して

$$\frac{1-\varepsilon}{3s} \leq v_{ij}^h \leq \frac{1+\varepsilon}{3s}.$$

行列 U_h の定義より，任意の $h,g \in [1,s]$ (ただし $h \neq g$) に対して $U_h U_g^T = 0$ が成り立つ．ここで $Ns \times d$ 行列 U を $U^T = [U_1^T, U_2^T, \ldots, U_s^T]$ とし，以下のような $Ns \times Ns$ 行列 V を定義する．

$$V = UU^T = \begin{bmatrix} U_1 \\ U_2 \\ \vdots \\ U_s \end{bmatrix} \begin{bmatrix} U_1^T, U_2^T, \ldots, U_s^T \end{bmatrix} = \begin{bmatrix} V_1 & 0 & \cdots & 0 \\ 0 & V_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & V_s \end{bmatrix}.$$

このとき以下の事実に注意する．

$$\begin{aligned} \mathrm{rank}(V) &= \mathrm{rank}(UU^T) \\ &\leq \min\{\mathrm{rank}(U), \mathrm{rank}(U^T)\} \\ &= \mathrm{rank}(U) \leq \min\{d, Ns\} \leq d \end{aligned}$$

これより以下の命題を得る．

補題 2.2 任意の ε 近似 k 制限最小値独立置換族 $\mathcal{F} \subseteq S_n$ に対して以下が成り立つ．

$$\begin{aligned} |\mathcal{F}| = d &\geq \mathrm{rank}(V) \\ &= \mathrm{rank}(V_1) + \mathrm{rank}(V_2) + \cdots + \mathrm{rank}(V_s). \end{aligned}$$

補題 2.2より，ε 近似 k 制限最小値独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの下界は，行列 $V_1, V_2, \ldots, V_s$ の階数の下界に還元される．以下の補題は，行列 $V_1, V_2, \ldots, V_s$ の階数を評価する際に重要となる．

補題 2.3 $t \times t$ 行列 $A = (a_{ij})$ が以下の条件を満たすならば，行列 A は正則である．

(1) 任意の $i,j \in [1,t]$ *(ただし $i \neq j$)* に対して $a_{ij} = a > 0$;

(2) $\min\{a_{11}, a_{22}, \ldots, a_{tt}\} > a$.

ここで $K_\ell = (V,E)$ を ℓ 個の節点を持つ完全グラフとし，$\mathcal{C}_m = \{c_1, c_2, \ldots, c_m\}$ を異なる m 色の色集合とする．また，$\chi : E \to \mathcal{C}_m$ を色集合 $\mathcal{C}_m$ による完全グラフ K_ℓ の枝の色塗りとする．任意の整数 $t_1, t_2, \ldots, t_m \geq 3$ に対して，$R(t_1, t_2, \ldots, t_m)$ を以下の条件を満たす最小の整数 ℓ とする:

- 任意の枝の色塗り $\chi : E \to \mathcal{C}_m$ に対して，ある $i \in [1,m]$ が存在し，単一色 c_i のみで塗られたの枝集合を持つ節点数 t_i の完全部分グラフ $K_{t_i} = (V_i, E_i) \subseteq K_\ell$ が存在する．

特に $t_1 = t_2 = \cdots = t_m = t$ であるとき，簡単のため $R_m(t)$ と表記することとする．

補題 2.4 任意の整数 $m \geq 2, t \geq 1$ に対して，

$$R_m(t) \leq m^{mt-(m-1)}.$$

補題 2.3及び補題 2.4より，以下の補題が導かれる．

補題 2.5 任意の定数 $0 < \varepsilon < 1/5$ と任意の整数 $k \geq 3$ に対して置換族 $\mathcal{F} \subseteq S_n$ を ε 近似 k 制限最小値独立とする．また，任意の整数 $m \geq 1$ に対して $|\mathcal{F}| < \frac{k}{2\varepsilon} m$ と仮定すると，各行列 V_h に関して以下が成り立つ．

$$\mathrm{rank}(V_h) \begin{cases} = N & m = 1; \\ \geq \lfloor \dfrac{\log(3n/k)}{m \log m} \rfloor & m \geq 2. \end{cases}$$

補題 2.5より，以下の ε 近似 k 制限最小値独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの下界が導出される．

定理 2.1 任意の定数 $0 < \varepsilon < 1/5$ と任意の整数 $k \geq 3$ に対して，置換族 $\mathcal{F} \subseteq S_n$ が ε 近似 k 制限最小値独立であるとする．このとき，十分大きな整数 n に関して，以下が成り立つ．

$$|\mathcal{F}| = \Omega\left(k \cdot \frac{\log^{1/2-o(1)}(n/k)}{\varepsilon^{1/2+o(1)}} \right).$$

さらに，上記の議論において $Ns \times Ns$ 行列 V の評価を厳密化することで，以下の結果を導出した．

定理 2.2 $\mathcal{F} \subset S_n$ を分布 $\mathcal{D}$ に関する ε 近似 k 制限最小値独立置換族とする．このとき，任意の

$0 < \varepsilon < 1/8$ と任意の $k \geq 3$ および十分に大きな n に対して，以下が成り立つ：

$$|\mathcal{F}| \geq \Omega\left(\frac{k}{\varepsilon^2 \log(1/\varepsilon)} \log n\right).$$

定理 2.3 $\mathcal{F} \subset S_n$ を分布 $\mathcal{D}$ に関する ε 近似 k 制限最小値独立置換族とする．このとき，任意の $0 < \varepsilon < 1/11$ と任意の $k \geq 3$ および十分に大きな n に対して，以下が成り立つ：

$$|\mathcal{F}| \geq \Omega\left(\frac{k^2}{\varepsilon \log(1/\varepsilon)} \log n\right).$$

2.2 k 制限独立置換族の構成に関する研究

任意の整数 $n \geq 1$ に対して S_n を集合 $[0, n-1]$ 上の置換全体とする．また，任意の整数 $n \geq k \geq 1$ に対して $[n]_k = n(n-1)\cdots(n-k+1)$ とする．このとき置換族 $\mathcal{F} \subseteq S_n$ が "ε-近似 k-対独立" であるとは，任意の k 個の異なる $x_1, x_2, \ldots, x_k \in [0, n-1]$ と任意の k 個の異なる $y_1, y_2, \ldots, y_k \in [0, n-1]$ に対して，以下が成り立つことを言う．

$$\Pr_{\pi \in \mathcal{F}}\left[\left|\bigwedge_{i=1}^{k} \pi(x_i) = y_i\right] - \frac{1}{[n]_k}\right| \leq \frac{\varepsilon}{[n]_k}.$$

特に $\varepsilon = 0$ の場合を "k-対独立" であると言う．

単純な数え上げ論法により，任意の k-対独立置換族 $\mathcal{F} \subseteq S_n$ に対して $|\mathcal{F}| \geq [n]_k$ が成り立つことが示される．一方，これまでに $k = 2$ の場合，任意の $n = p^m$ (p: 素数) に対して $|\mathcal{G}_2| = [n]_2$ となるような 2-対独立置換族 $\mathcal{G}_2 \subseteq S_{p^m}$ の構成法が知られている．具体的には

$$\mathcal{G}_2 = \big\{\pi_{a,b} : \pi_{a,b}(x) = ax + b, \\ a \in \mathbf{GF}(p^m) - \{0\}, b \in \mathbf{GF}(p^m)\big\}.$$

同様に $k = 3$ の場合，任意の $n = p^m + 1$ (p: 素数) に対して $|\mathcal{G}_3| = [n]_3$ となる 3-対独立置換族 $\mathcal{G}_3 \subseteq S_{p^m+1}$ の構成法が知られている．任意の $a, b, c, d \in \mathbf{GF}(p^m)$ に対して $A = \binom{ab}{cd}$ とすると，

$$\mathcal{G}_3 = \begin{cases} \big\{\pi_A : \pi_A(x) = \frac{ax+b}{cx+d}, \\ \qquad ad - bc = 1\big\} & p = 2; \\ \big\{\pi_A : \pi_A(x) = \frac{ax+b}{cx+d}, \\ \qquad ad - bc \in \{1, e\}\big\} & p \neq 2. \end{cases}$$

ただし $e \in \mathbf{GF}(p^m)$ は任意に固定された平方非剰余であり，任意の $x \in \mathbf{GF}(p^m) \cup \{\infty\}$ に対して，

$$c = 0: \quad \pi_A(x) = \begin{cases} \frac{ax+b}{d} & x \neq \infty; \\ \infty & x = \infty; \end{cases}$$

$$c \neq 0: \quad \pi_A(x) = \begin{cases} \frac{ax+b}{cx+d} & x \notin \{-dc^{-1}, \infty\}; \\ \infty & x = -dc^{-1}; \\ ac^{-1} & x = \infty. \end{cases}$$

ε-近似 k-対独立置換族の構成 [I]

ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの下界と非構成的上界を導出し，さらにその非構成的上界を下回る ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ の具体的な構成法を提案した．

まず始めに，代数的手法を用いて，以下のような ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの下界を導出した．

定理 2.4 任意の実数 $\varepsilon \geq 0$ と任意の整数 $n \geq k \geq 1$ に対して，置換族 $\mathcal{F} \subseteq S_n$ が ε-近似 k-対独立であるならば，以下が成り立つ．

$$|\mathcal{F}| \geq \begin{cases} n(n-1)\cdots(n-k+1) & \varepsilon < 1; \\ \dfrac{n(n-1)\cdots(n-k+1)}{1+\varepsilon} & \varepsilon \geq 1. \end{cases}$$

一般的に $\varepsilon \geq 1$ に対して，この下界はこれ以上改善することはできない．実際，第 2.2節の冒頭で定義した置換族 $\mathcal{G}_2 \subseteq S_{p^m}$ と $\mathcal{G}_3 \subseteq S_{p^m+1}$ に対して，

$$\begin{aligned} \mathcal{G}_2' &= \big\{\pi \in \mathcal{G}_2 : |\mathcal{G}_2'| = |\mathcal{G}_2|/2\big\} \subseteq \mathcal{G}_2; \\ \mathcal{G}_3' &= \big\{\pi \in \mathcal{G}_3 : |\mathcal{G}_3'| = |\mathcal{G}_3|/2\big\} \subseteq \mathcal{G}_3. \end{aligned}$$

とすると $\varepsilon = 1$ において

$$\begin{aligned} |\mathcal{G}_2'| &= p^m(p^m - 1)/2; \\ |\mathcal{G}_3'| &= (p^m + 1)p^m(p^m - 1)/2, \end{aligned}$$

となり，それぞれ定理 2.4の等号を満たす．

次に，確率的手法を用いて，以下のような ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの非構成的上界を導出した．

定理 2.5 任意の実数 $0 < \varepsilon < 1$ と任意の整数 $n \geq k \geq 1$ に対して，以下を満たす ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ が存在する．

$$|\mathcal{F}| = O\left(\frac{k \ln n}{\varepsilon^2}[n]_k\right).$$

さらに，定理2.4および定理2.5より，任意の$\varepsilon > 0$ に対して，コンパクトで多項式時間標本可能なε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ の構成法を提案した．

定理 2.6 任意の実数 $\varepsilon > 0$ と任意の整数 $n = p^m - 1 \geq \lceil \gamma/\varepsilon \rceil$ (p: 素数) に対して

$$|\mathcal{F}| = \left\lceil \frac{\gamma}{\varepsilon} \right\rceil (1 + o(1))[n]_2$$

を満たす多項式時間標本可能なε-近似 2-対独立置換族 $\mathcal{F} \subseteq S_n$ が構成可能である．ただし，

$$\gamma = \begin{cases} 4 & x^2 - x + 1 \text{ が } \mathbf{GF}(p^m) \text{ 上で既約;} \\ 6 & x^2 - x + 1 \text{ が } \mathbf{GF}(p^m) \text{ 上で可約.} \end{cases}$$

定理 2.7 任意の実数 $\varepsilon > 0$ と任意の整数 $n = p^m \geq \lceil \gamma/\varepsilon \rceil$ (p: 素数) に対して

$$|\mathcal{F}| = \left\lceil \frac{\gamma}{\varepsilon} \right\rceil (1 + o(1))[n]_3$$

を満たす多項式時間標本可能なε-近似 3-対独立置換族 $\mathcal{F} \subseteq S_n$ が構成可能である．ただし，

$$\gamma = \begin{cases} 6 & x^2 + x + 1 \text{ が } \mathbf{GF}(p^m) \text{ 上で既約;} \\ 12 & x^2 + x + 1 \text{ が } \mathbf{GF}(p^m) \text{ 上で可約.} \end{cases}$$

ε-近似 k-対独立置換族の構成 [II]

研究会等論文 1 において，共通鍵暗号方式 DES (Data Encryption Standard) の設計において本質的な役割を果たすフェイステル変換を繰り返し用いて置換族を構成し，カップリング法を用いて以下が成り立つことを明らかにした．

定理 2.8 任意の $n = p^{2h}$ (p: 素数; h: 正整数) に対して $k = O(\log n)$ であるならば，

$$|\mathcal{F}| = \left(\frac{n^{k^2}}{\varepsilon^k} \right)^{3+o(1)}$$

を満たす ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ が構成可能である．

これは ε-近似 k-対独立置換族 $\mathcal{F} \subseteq S_n$ の非自明 (対称群・交代群以外) な最初の構成法である．さらに，本研究で構成された置換族が $O(\log n)$-領域要素別法本可能であることを示した．

3 線形符号の双対距離と共通鍵暗号への応用に関する研究

共通鍵暗号の安全性は，差分攻撃及び線形攻撃に対する耐性によって評価されるため，差分攻撃及び線形攻撃に対してある種の一様性が保証されたブール関数の設計が重要となる．そのような一様性を持つ (コンパクトな) ブール関数の設計は，任意の整数 d と $d^\perp$ が与えられたとき，以下の条件を満たすような線形符号 $\mathcal{C}$ の最小符号長 $n = N(d, d^\perp)$ を求める問題に帰着される:

(1) 符号 $\mathcal{C}$ の最小距離は d;

(2) 符号 $\mathcal{C}$ の双対符号 $\mathcal{C}^\perp$ の最小距離は $d^\perp$.

これまでに本研究では，任意の整数 $d, d^\perp$ に対して，代数的手法などにより，以下に示す $N(d, d^\perp)$ の上界・下界を導出している．

定理 3.1 ($N(d, d^\perp)$の上界) 任意の整数 $n \geq m$ と任意の整数 $d, d^\perp$ が与えられたとき $N(d, d^\perp) \leq n$．ただし n は以下を満たす最小の整数とする．

$$\frac{2^m - 1}{2^n - 1} \sum_{i=1}^{d-1} \binom{n}{i} + \frac{2^{n-m} - 1}{2^n - 1} \sum_{i=1}^{d^\perp - 1} \binom{n}{i} < 1.$$

定理 3.2 ($N(d, d^\perp)$の下界) 任意の整数 $d, d^\perp$ が与えられたとき，以下が成り立つ．

$$N(d, d^\perp) \geq \min\{n : n \geq \lg \ell(n, d) + \lg \ell(n, d^\perp)\},$$

ただし，任意の整数 $n \geq d$ に対して

$$\ell(n, d) = \begin{cases} \displaystyle\sum_{i=0}^{(d-1)/2} \binom{n}{i} & d \text{ は奇数;} \\ \displaystyle\sum_{i=0}^{d/2-1} \binom{n}{i} + \binom{n-1}{\frac{d}{2}-1} & d \text{ は偶数.} \end{cases}$$

そこで，本研究では，新たに以下に示すような $N(d, d^\perp)$ に対する下界を導出した．

定理 3.3 ($N(d, d^\perp)$の下界) 任意の整数 $d, d^\perp$ が与えられたとき，以下が成り立つ．

$$N(d, d^\perp) \geq \min \left[n : 2n \geq d + d^\perp + \min_{1 \leq m \leq n-1} \left\{ \sum_{i=1}^{m-1} \left\lceil \frac{d}{2^i} \right\rceil + \sum_{i=1}^{n-m-1} \left\lceil \frac{d^\perp}{2^i} \right\rceil \right\} \right].$$

表 1: $N(d, d^{\perp})$ の上界・下界

d	$d^{\perp}$	$N(d,d^{\perp})$	上界	下　界			
		実験結果	定理 3.1	定理 3.2	定理 3.3	定理 3.4	定理 3.5
3	3	6	17	6	5	6	6
4	3	7	21	7	6	7	7
4	4	8	25	8	7	8	8
5	3	11	24	9	7	11	8
5	4	13	29	11	8	13	9
5	5	16	34	14	11	14	10
6	3	12	28	10	8	12	9
6	4	14	33	12	9	14	10
6	5	17	38	15	12	17	11
6	6	18	42	16	13	18	10
7	3	14	31	12	9	14	10
7	4	15	37	14	10	15	11
8	3	15	35	14	10	15	11
8	4	16	40	15	11	16	12

定理 3.4 ($N(d, d^{\perp})$の下界) 任意の整数 $d, d^{\perp}$ が与えられたとき $N(d, d^{\perp}) \geq n$，ただし n は以下を満たす最小の整数とする．

$$\begin{aligned} A_i &\geq 0 && d \leq i \leq n; \\ \sum_{i=d}^{n} A_i P_w(i) &= -\binom{n}{w} && 1 \leq w \leq d^{\perp} - 1; \\ \sum_{i=d}^{n} A_i P_w(i) &= -\binom{n}{w} && d^{\perp} \leq w \leq n; \end{aligned}$$

(1) d が偶数の場合: 以下のどちらか．

$$\begin{cases} \sum_{i:\text{ 偶数}} A_i = \sum_{i:\text{ 奇数}} A_i; \\ A'_n = 0. \end{cases}$$

$$\begin{cases} A_i = 0 & i:\text{ 奇数}; \\ 4\sum_{i:4|i} A_i \geq \sum_{i=0}^{n} A_i; \\ A'_n = 1; \\ A'_i = A'_{n-i} & 0 \leq i \leq n-1. \end{cases}$$

(2) d が偶数の場合:

$$\begin{cases} \sum_{i:\text{ 偶数}} A_i = \sum_{i:\text{ 奇数}} A_i; \\ A'_n = 0. \end{cases}$$

(3) $d^{\perp}$ が偶数の場合: 以下のどちらか．

$$\begin{cases} \sum_{i:\text{ 偶数}} A'_i = \sum_{i:\text{ 奇数}} A'_i; \\ A_n = 0. \end{cases}$$

$$\begin{cases} A'_i = 0 & i:\text{ 奇数}; \\ 4\sum_{i:4|i} A'_i \geq \sum_{i=0}^{n} A'_i; \\ A_n = 1; \\ A_i = A'_{n-i} & 0 \leq i \leq n-1. \end{cases}$$

(4) $d^{\perp}$ が偶数の場合:

$$\begin{cases} \sum_{i:\text{ 偶数}} A'_i = \sum_{i:\text{ 奇数}} A'_i; \\ A_n = 0. \end{cases}$$

ただし，任意の線形符号 $\mathcal{C}$ とその双対符号 $\mathcal{C}^{\perp}$ に対して，$A_w, A'_w, P_w(i)$ は以下で与えられる．

$$\begin{aligned} A_w &= |\{c \in \mathcal{C} : w(c) = w\}|; \\ A'_w &= |\{c \in \mathcal{C}^{\perp} : w(c) = w\}|; \\ P_w(i) &= \sum_{j=0}^{w} (-1)^j \binom{i}{j}\binom{n-i}{w-j}. \end{aligned}$$

定理 3.5 ($N(d, d^\perp)$の下界) 任意の整数$d, d^\perp$が与えられたとき，以下が成り立つ．

$$N(d, d^\perp) \geq \begin{cases} d + d^\perp - 2 & d, d^\perp \geq 1; \\ d + d^\perp & d, d^\perp \geq 3. \end{cases}$$

また，計算機実験により上記の上界・下界を検証し，表1のような結果を得た．表1より明らかに，上界 (定理3.1) は実際の$N(d, d^\perp)$と大きな隔たりがあるものの，下界 (定理3.3・定理3.5) は実際の$N(d, d^\perp)$を良好に評価している．

今後の課題として実際の$N(d, d^\perp)$を良好に評価する上界の導出が挙げられる．

4 ネットワーク制御に関する研究

近年のインターネットの爆発的な普及に伴い，ネットワーク機器に過剰な負荷がかかり，また帯域損失・パケット消失・応答遅延などの通信品質の劣化が深刻化している．このような通信品質の劣化を防ぐために Quality of Service (QoS) の概念が注目されている．一般に QoS スイッチはm個のキューを持ち，各キューは到来するパケットを格納するためのB個のスロットを有する．また各パケットはその優先順位を表す “優先度” が割り当てられている．ネットワーク上の通信量はしばしば変化するため，QoS スイッチは転送パケットの優先度の総和を最大にするように到来するパケットの制御を行う．ここで QoS スイッチは，将来到来するパケットの情報を得ることが不可能であるので QoS アルゴリズムはオンラインアルゴリズムとして定式化され，その効率は競合比によって評価される．QoS アルゴリズム ALG がc-競合的であるとは，全てのパケット列σに対して

$$\frac{\mathrm{OPT}(\sigma)}{\mathrm{ALG}(\sigma)} \leq c$$

が成り立つことを言う．ただし$\mathrm{ALG}(\sigma)$はパケット列σに対して QoS アルゴリズム ALG が転送したパケットの優先度の総和を表すものとし，一方$\mathrm{OPT}(\sigma)$は，パケット列σに対して最適なオフラインアルゴリズム OPT が転送したパケットの優先度の総和を表すものとする．また，各パケットの優先度がβ以上α以下に制限されたパケット列集合を$\Pi_{[\beta,\alpha]}$と表すものとする．

一般に QoS アルゴリズムは，

- **パケット破棄可能モデル:** 新たなパケットが到来した際に，既にキューに格納されているパケットの破棄を許すポリシー
- **パケット破棄不可能モデル:** 新たなパケットが到来した際に，既にキューに格納されているパケットの破棄を許さないポリシー

に大別される．本研究では，パケット破棄不可能 QoS 問題に関して，その競合比の上界と下界の解析を行い，以下の結果を導出した．

定理 4.1 任意の QoS アルゴリズム ALG と任意の$\alpha \geq 1$に対して，パケット列σが存在し，

$$\frac{\mathrm{OPT}(\sigma)}{\mathrm{ALG}(\sigma)} \geq \begin{cases} 1 + \frac{1}{\alpha \ln\left(\frac{\alpha}{\alpha-1}\right)} - \Theta\left(\frac{1}{\min\{m,B\}}\right) & \alpha \geq \alpha^*; \\ \frac{1}{1-e^{-\tau_0}} - \Theta\left(\frac{1}{\min\{m,B\}}\right) & 1 \leq \alpha < \alpha^*. \end{cases}$$

ただしτ_0は$e^{-\tau}(1/\alpha + \tau) = 1 - e^{-\tau}$の根である．

またこの結果より，単一優先度決定性パケット破棄不可能 QoS 問題に関して，その競合比の下界が1.466以上となることが容易に導出される．これは単一優先度決定性 QoS 問題の競合比に関する既知の下界1.366を改善するものである．

さらに本研究では，優先度が1と$\alpha \geq 1$に制限された決定性パケット破棄可能 QoS 問題に関して，その競合比の下界の解析を行い，以下の結果を導出した．

定理 4.2 任意の$\alpha \geq 1$に対する QoS 問題$\Pi_{[1,\alpha]}$に関して，パケット破棄可能モデル QoS アルゴリズム TLH は$(3 - 1/\alpha)$-競合的である：任意のパケット列$\sigma \in \Pi_{[1,\alpha]}$に対して，

$$\frac{\mathrm{OPT}(\sigma)}{\mathrm{ALG}(\sigma)} \leq 3 - \frac{1}{\alpha}.$$

定理 4.3 任意の$\alpha \geq 1$に対して，以下を満たすパケット列$\sigma_\alpha \in \Pi_{[1,\alpha]}$が存在する:

$$\frac{\mathrm{OPT}(\sigma_\alpha)}{\mathrm{TLH}(\sigma_\alpha)} \geq \frac{3 - 1/m}{1 + 1/B + 1/\alpha},$$

ただし，mはキューの数，$B = B_1 + B_2 + \cdots + B_m$で$B_i$は各キューのパケット格納可能数とする．

定理 4.2は，既知の結果 — QoS 問題 $\Pi_{[0,\alpha]}$ に対するパケット破棄可能 QoS アルゴリズム TLH が 3-競合的である — を改善するものである．また，定理 4.3は，十分大きな α, m, B に対して，パケット破棄可能 QoS アルゴリズム TLH の競合比 $3-1/\alpha$ が良好な評価であることを保証するものである．

定理 4.4 任意の $\alpha \geq 1$ と任意のパケット破棄可能 QoS アルゴリズム ALG に対して，以下を満たすパケット列 $\sigma_\alpha \in \Pi_{[0,\alpha]}$ が存在する*:*

$$\frac{\mathrm{OPT}(\sigma_\alpha)}{\mathrm{ALG}(\sigma_\alpha)} \geq 1.514 - \Theta(0.559^m).$$

定理 4.4は，既知の結果 — QoS 問題 $\Pi_{[0,\alpha]}$ に対する競合比の下界は 1.419 である — を改善するものである．

5 電子商取引アルゴリズムに関する研究

5.1 最適選好マッチングに関する研究

n 人の顧客が各々の m 個の商品に対する希望リストを提示し，供給者が顧客の満足度を最大化する商品配分は最適選好マッチング (popular matching) と呼ばれる．顧客全てが同一グループに属する場合，与えられた問題に対して最適選好マッチングが存在するならば，それを $O(n+m)$ 時間で求めるアルゴリズムが知られている．また，顧客が優先度に応じて複数のグループに分割されている場合に関しても，与えられた問題に対して最適選好マッチングが存在するならば，それを $O(n+m)$ 時間で求めるアルゴリズムが知られている．一方，顧客全てが同一グループに属する場合，各顧客の希望リストが商品集合上の一様独立な乱択ベクトルで与えられるとき，$m > 1.42n$ であるならば確率 $1-o(1)$ で最適選好マッチングが存在し，$m < 1.42n$ であるならば確率 $1-o(1)$ で最適選好マッチングが存在しないことが知られている．そこで，本研究では，顧客が優先度に応じて 2 つの同一グループに分割されれいる場合に関して，各顧客の希望リストが商品集合上の一様独立な乱択ベクトルで与えられるとき，以下が成り立つことを明らかにした．

定理 5.1 顧客が優先度に応じて *2*つの同一グループに分割されれいる場合，一様独立な乱択入力に対して，$n^{4/3}/m = o(1)$ であるならば確率 $1-o(1)$ で最適選好マッチングが存在する．

定理 5.2 顧客が優先度に応じて *2*つの同一グループに分割されれいる場合，一様独立な乱択入力に対して，$m/n^{4/3} = o(1)$ であるならば確率 $1-o(1)$ で最適選好マッチングが存在しない．

5.2 価格設定問題に関する研究

m の商品に対して n 人の顧客の各々が購入希望商品群に関する購入可能金額を提示するとする．ここで，売主が利益が最大となるように各商品の価格を設定す問題を価格設定問題という．価格設定問題は，各々の顧客の購入希望商品数に制限がない場合はハイパーグラフとして定式化されるが，各々の顧客の購入希望商品数が 2 以下に制限される場合はグラフとして定式化される．一方，各商品には製造コストがあるため，各商品の販売価格はその製造コスト以上とすることが通常である．このような価格モデルは正値モデル (positive price mdel) と呼ばれる．しかし，販売価格として製造コスト未満を許す場合，販売価格として製造コスト未満を許さない場合に比べて，全体の利益が増大する場合が知られている．このような価格モデルに関しては，割引価格モデル (discount model)・制限付き割引価格モデル (B-bounded discount model)・無損失割引価格モデル (coupon model) などが知られている．

本研究では，正値モデルに関して以下のことを明らかにした．

定理 5.3 星グラフで与えられる価格設定問題は完全多項式時間近似スキームを持つ．

定理 5.4 木グラフで与えられる価格設定問題は完全多項式時間近似スキームを持つ．

定理 5.5 次数が d に制限された *2* 部グラフで与えられる価格設定問題は $\alpha(\varepsilon, d)$-近似アルゴリズムを持つ．ただし，任意の $\varepsilon > 0$ に対して，

$$\alpha(\varepsilon, d) = \frac{1-\varepsilon}{2}\left\{1 + \frac{1}{d(d-1)+1}\right\}.$$

定理 5.6 次数が d に制限されたグラフで与えられる価格設定問題は $\alpha(d)$-近似アルゴリズムを持つ．ただし，

$$\alpha(d) = \begin{cases} \frac{1}{4}\left(1+\frac{1}{d}\right) & d\text{が奇数の場合;} \\ \frac{1}{4}\left(1+\frac{1}{d+1}\right) & d\text{が偶数の場合.} \end{cases}$$

定理 5.7 グラフで与えられる価格設定問題において，購入可能金額比 (購入可能金額の最小値 s と最大値 ℓ の比) が $r = s/\ell$ であるとき，$\alpha(r)$-近似アルゴリズムを持つ．ただし，

$$\alpha(r) = \begin{cases} \frac{2+r}{8} & 0 \le r < 2/3; \\ \frac{1}{2}\frac{1}{2-r} & 2/3 \le r \le 1. \end{cases}$$

さらに本研究では，無損失割引モデルに関して，以下の結果を導出した．

定理 5.8 線状高速道路価格設定問題において，購入可能金額比 (購入可能金額の最小値 s と最大値 ℓ の比) が $r = s/\ell$ であるとき，$\alpha(r)$-近似アルゴリズムを持つ．ただし $\beta \approx 0.3824$ であり，

$$\alpha(r) = \begin{cases} 4(1-\ln r) & 0 \le r \le \beta, 1/\sqrt{e} \le r \le 1; \\ 3/r & \beta < r \le 1/2; \\ 6 & 1/2 < r < 1/\sqrt{e}. \end{cases}$$

定理 5.9 環状高速道路価格設定問題において，購入可能金額比 (購入可能金額の最小値 s と最大値 ℓ の比) が $r = s/\ell$ であるとき，$4(1-\ln r)$-近似アルゴリズムを持つ．

定理 5.10 線状高速道路価格設定問題において，購入可能金額比 (購入可能金額の最小値 s と最大値 ℓ の比) が $r = s/\ell$ であるとき，2.747-近似アルゴリズムを持つ．

6 VLSI 計算に関する研究

VLSI 計算に関しては，3 次元レイアウト，3 次元チャネル配線，3 次元単層配線，グラフの直交描画，及び VLSI 分解などの研究を行った．

6.1 3 次元レイアウトに関する研究

バタフライネットワークは並列計算機の相互結合網や ATM スイッチの結線構造としてよく用いられている．また，ハイパーキューブは並列計算機の相互結合網としてよく用いられている．

バタフライネットワーク

N 点バタフライネットワーク B_N の 3 次元レイアウトに関しては，$\mathrm{vol}(B_N)$ を B_N の 3 次元レイアウトの最小体積としたときに，

$$\begin{aligned} \mathrm{vol}(B_N) &\ge 0.75N^{3/2} + o(N^{3/2}); \\ \mathrm{vol}(B_N) &\le 723\sqrt{2}N^{3/2} + o(N^{3/2}), \end{aligned}$$

であることが知られている．本研究では，B_N の具体的な 3 次元レイアウトを示すことにより，

$$\mathrm{vol}(B_N) \le 8\sqrt{2}N^{3/2} + o(N^{3/2})$$

であることを証明している．これは既存の上界に対して大幅な改良になっている．

ハイパーキューブ

N 点からなるハイパーキューブ Q_N の 2 次元レイアウトに関しては，$\mathrm{A}(Q_N)$ を Q_N の 2 次元レイアウトの最小面積としたときに，$\mathrm{A}(Q_N) = \Theta(N^2)$ であることがよく知られている．

一方，Q_N の 3 次元レイアウトに関しては，$\mathrm{vol}(Q_N)$ を Q_N の 3 次元レイアウトの最小体積としたときに，$\mathrm{vol}(Q_N) = \Omega(N^{3/2})$ であることが知られていが，$\mathrm{vol}(Q_N)$ の上界を明示的に考察している文献は見当たらない．

そこで本研究では，Q_N の具体的な 3 次元レイアウトを初めて示し，$\mathrm{vol}(Q_N) = O(N^{3/2})$ であることを証明し，$\mathrm{vol}(Q_N) = \Theta(N^{3/2})$ であることを明らかにしている．Q_N の 3 次元レイアウトは，Q_N のよく知られている最適な 2 次元レイアウトの自然な一般化になっている．すなわち，Q_N を $N^{2/3}$ 個の $Q_{N^{1/3}}$ に分解し，これらの $Q_{N^{1/3}}$ の 3 次元線形レイアウトを組み合わせて Q_N の 3 次元レイアウトを構成している．

6.2 3 次元チャネル配線に関する研究

3 次元チャネル配線は，3 次元レイアウトの詳細配線に用いられており，3 次元集積回路設計における基本的な問題の一つである．いくつかの先駆的研究が散見されるが，いずれも本質的には 2 次元あるいは 2.5 次元のチャネル配線モデルであり，本来の 3 次元チャネル配線のモデルは見当たらない．

3 次元チャネル配線のモデル

そこで本研究では，初めて自然で一般的な 3 次元チャネル配線の以下のようなモデルを提案している．一対の平行な境界面上に端子が配置されている 3 次元格子グラフを 3 次元チャネルという．同一ネットの端子を木で連結し，異なるネットに対する木が点非共有であるとき，これを 3 次元チャネル配線という．3 次元チャネル配線においては，端子が配置されている一対の平行な境界面の間の距離（これを 3 次元チャネルの高さという）を最小化する問題が基本的である．

3 次元チャネルの高さの上下界

また本研究では，このモデルの下で与えられた 2 端子ネットの組を配線するために必要な 3 次元チャネルの高さの上界・下界を明らかにしている．特に，n 個の 2 端子ネットは高さ $O(\sqrt{n})$ の 3 次元チャネル内で長さ $O(\sqrt{n})$ の配線を用いて配線可能であることを示すと共に，配線するためには高さ $\Omega(\sqrt{n})$ の 3 次元チャネルを必要とするような n 個の 2 端子ネットの組の存在を示している．高さの上界は，多項式時間の 3 次元チャネル配線アルゴリズムを示して，構成的に証明されている．

3 次元チャネル配線問題の $\mathcal{NP}$ 困難性

さらに本研究では，3 次元チャネル配線に付随する判定問題は $\mathcal{NP}$ 完全であることを明らかにしている．$\mathcal{NP}$ 困難性は，すでに $\mathcal{NP}$ 完全であることが知られている「(n^2-1) パズル」に付随する判定問題から 3 次元チャネル配線問題への多項式時間還元を示している．この多項式時間還元は自然なものであり，大変見通しのよい証明である．また，3 次元チャネル配線に付随する判定問題が $\mathcal{NP}$ に属することは自明ではなく，配線のベンド数に関する詳細な検討に基づいて証明されている．

一方，2 次元チャネル配線問題の計算複雑度は四半世紀以上の間未解決のままである懸案である．また，3 次元チャネル配線問題を解く多項式時間近似アルゴリズムの設計は今後の課題である．

6.3 3 次元単層配線に関する研究

3 次元単層配線においては，すべての端子が同一の（最上あるいは最下）層上に存在している．したがって，3 次元単層配線は 3 次元チャネル配線の特別な場合である．既に，すべての端子が偶数座標上に存在する場合には，n 個のネットは $6\sqrt{n}$ 層の 3 次元チャネル内で単層配線できること，及び単層配線するためには $\sqrt{n}/4$ 層の 3 次元チャネルを必要とするような n 個のネットの組が存在することなどが知られている．

本研究では既存の結果を改良し，すべての端子が偶数座標上に存在する場合には，n 個のネットは $5\sqrt{n}/2$ 層の 3 次元チャネル内で単層配線できることを明らかにしている．この上界は，多項式時間の単層配線アルゴリズムにより，構成的に証明されている．この多項式時間単層配線アルゴリズムは，前節で述べた多項式時間 3 次元チャネル配線アルゴリズムを修正して設計されている．

一方，3 次元単層配線問題の計算複雑度は未解決であり，今後の課題ある．

6.4 グラフの直交描画に関する研究

グラフの辺を座標軸に平行な直線分の系列で描画し，異なる辺の描画が端点以外で交差しないとき，これをそのグラフの直交描画であるという．グラフの直交描画は集積回路の設計などに幅広い応用があるために，従来から活発に研究されている．特に，グラフをベンドなしで 2 次元あるいは 3 次元空間に直交描画できるか否かを判定する問題は $\mathcal{NP}$ 完全であることが知られている．また，最大次数が高々4 の平面的グラフは，八面体を除外して，各辺に対するベンド数が高々2 で 2 次元直交描画できること，最大次数が高々3 の平面的グラフは，4 点完全グラフを除外して，各辺に対するベンド数が高々1 で 2 次元直交描画できること，最大次数が高々5 の任意のグラフは各辺に対するベンド数が高々2 で 3 次元直交描画できること，及び最大次数が高々6 の任意のグラフは各辺に対するベンド数が高々3 で 3 次元直交描画できることなどが知られている．

本研究では，特別な平面的グラフである外平面的グラフと直並列グラフに対して，少ないベンド

を用いて2次元及び3次元空間に直交描画する多項式時間アルゴリズムを提案している．

最大次数が高々6の任意のグラフが各辺に対するベンド数が高々2で3次元直交描画できるか否かを決定することは興味深い未解決問題である．

外平面的グラフ

外平面的グラフの直交描画に関する研究では，まず最大次数が高々3で三角形を含まない外平面的グラフはベンドなしで2次元直交描画できることを明らかにしている．ベンドなしでは2次元直交描画できないような，最大次数が4で三角形を含まない外平面的グラフが存在するので，この結果は限界的であることが分かる．また，本研究では，最大次数が高々6で三角形を含まない外平面的グラフはベンドなしで3次元直交描画できることも示している．なお，未発表であるが，最大次数が高々5である任意の外平面的グラフは各辺に対するベンド数が高々1で3次元直交描画できることを明らかにしている．

直並列グラフ

直並列グラフの直交描画に関する研究では，まず最大次数が高々4の任意の直並列グラフは各辺に対するベンド数が高々1で2次元直交描画できることを明らかにしている．ベンドなしでは2次元直交描画できないような，最大次数が高々4の直並列グラフが存在するので，この結果は限界的であることが分かる．また，本研究では，最大次数が高々6の任意の直並列グラフは各辺に対するベンド数が高々2で3次元直交描画できることを明らかにしている．

最大次数が高々6の任意の直並列グラフが各辺に対するベンド数が高々1で3次元直交描画できるか否かを明らかにすることは今後の課題である．

6.5 ネットワークのVLSI分解に関する研究

グラフ G の同型で点非共有な部分グラフの族は，G の全域部分グラフであるとき，G のVLSI分解であると言い，各部分グラフに同型なグラフ H を G の構成ブロックと言う．G の辺数に対する部分グラフの辺数の総和の比率を H の効率という．グラフ H がグラフの族 $\{G_n\}$ の任意のグラフの構成ブロックであるとき，H は $\{G_n\}$ の万能構成ブロックであるという．2値 D 次元deBruijnネットワーク $B(2,D)$ の族 $\{B(2,D)|D \geq n\}$ の万能構成ブロックの効率の下界は $1-O(1/n)$ であり，上界は $1-\Omega(1/n)$ であることが知られている．

本研究では，d 値 D 次元deBruijnネットワーク $B(d,D)$ の族 $\{B(d,D)|D \geq n\}$ の万能構成ブロックの効率は少なくとも $1-O(d/n)$ であり，多くとも $1-\Omega(1/n)$ であることを明らかにしている．

これらの上下界の間隙を埋めることは今後の課題である．

7 可逆計算に関する研究

可逆計算に関しては，可逆回路の故障検出及びグラフの量子計算などの研究を行った．

7.1 可逆回路の故障検出に関する研究

出力ベクトルの集合が入力ベクトルの集合の置換であるような論理回路を可逆論理回路という．可逆論理回路は，低消費電力設計，デジタル信号処理，ナノ・量子計算などに応用できることから，最近活発に研究されている．

全単射である論理関数を計算する論理ゲートを可逆であるという．可逆ゲートをファンアウトあるいはフィードバックを用いずに結合して得られる論理回路を可逆であるという．可逆論理回路 C のすべての配線上の（単一及び多重）縮退故障を検出できるテストの集合を C に対する完全テスト集合という．C に対する完全テスト集合のテストの数の最小値を $\tau(C)$ で表す．

k-CNOTゲートは $k+1$ 入力の可逆ゲートである．制御ビットとよばれる k 個の入力は値が変化することなく出力される．ターゲットビットとよばれる残りの1個の入力の値は，制御ビットの入力値がすべて1であるときに反転して出力される．0-CNOTゲートは古典的なNOTゲートである．CNOTゲートだけで構成される可逆論理回路をCNOT回路という．2-CNOTゲートでNAND関

数を実現できるので，任意の論理関数は CNOT 回路で実現できることが分かる．

任意の可逆回路 C に対して，

$$\tau(C) = O(\log m)$$

であること，n 入力 CNOT 回路 C が 0-CNOT ゲートも 1-CNOT ゲートも含まないならば，

$$\tau(C) \leq n$$

であることが知られている．ここで，m は C の配線の数である．

本研究では，可逆論理回路 C に対して $\tau(C)$ を計算する問題は $\mathcal{NP}$ 困難であることを示して，可逆論理回路の故障検出問題の計算複雑度を初めて明らかにしている．$\mathcal{NP}$ 困難性は，3SAT から CNOT 回路 C に対する $\tau(C)$ の判定問題への多項式時間還元を示して証明されている．

また本研究では，$\tau(C) = \Omega(\log\log m)$ であるような可逆回路 C が存在すること，及び $\tau(C) \geq \log n$ であるような 0-CNOT ゲートも 1-CNOT ゲートも含まない n 入力 CNOT 回路 C が存在することを明らかにしている．

$\tau(C)$ の上下界の間隙を埋めることは今後の課題である．

7.2 量子計算に関する研究

グラフの最小全域木問題や最短路問題などに対しては，古典的アルゴリズムよりも高速である量子アルゴリズムが知られている．実際，単一始点最短路問題の古典的時間計算量は $\Theta(m+n\log n)$ であるが，量子クエリ計算量は $O(\sqrt{mn}\log^2 n)$ 及び $\Omega(\sqrt{mn})$ であることが知られている．ここで，m と n はそれぞれグラフの辺数と点数である．

一方，全点対間最短路問題の古典的時間計算量は $O(mn + n^2\log\log n)$ 及び $\Omega(mn)$ であることが知られているが，量子クエリ計算量に関しては，単一始点最短路問題の下界から得られる自明な下界 $\Omega(\sqrt{mn})$ しか知られていない．

そこで，本研究では，全点対間最短路問題の量子計算量の非自明な下界 $\Omega(\sqrt{m^3/n^2})$ を示している．この下界は，$m = \omega(n^{3/2})$ であるときには，自明な下界よりも真に大きいことが分かる．

$m = O(n^{3/2})$ であるときの非自明な下界の導出と古典的アルゴリズムよりも高速である量子アルゴリズムの設計は今後の課題である．

8 耐故障計算に関する研究

耐故障計算に関しては，逐次故障診断及び確率的耐故障ネットワークなどの研究を行った．

8.1 並列計算システムの逐次故障診断に関する研究

並列計算システムの故障診断の研究には長い歴史があるが，一度にすべての故障ユニットを同定する同時診断と一度に 1 つの故障ユニットを同定する逐次診断に分類して活発に研究されている．従来から，同時診断可能性に関するシステムの特徴付けはよく知られているが，逐次診断可能性に関するシステムの特徴付けについては知られていない．そこで本研究では，様々なシステムの逐次診断可能次数の上界・下界を統一的な手法を用いて示している．特に，逐次診断可能次数の非自明な上界は初めて示されたものである．

より詳細には，まず新しい自然な逐次診断アルゴリズムを提案し，N 個のプロセッサからなる任意のシステムの逐次診断可能次数が少なくとも $\Omega(\sqrt{N})$ であることを明らかにしている．また，非常に一般的な統一的手法を用いて，N 点からなる d 次元グリッドは逐次 $O(N^{d/(d+1)})$ 診断可能であること，及び N 点からなる k 分木は $O(\sqrt{kN})$ 診断可能であることを示している．さらに，N 点からなるハイパーキューブの逐次診断可能次数は少なくとも $\Omega(N/\sqrt{\log N})$ であり，多くとも $O(N\log\log N/\sqrt{\log N})$ であることを明らかにすると共に，N 点からなる CCC, シャッフル交換グラフ，及び deBruijn グラフの逐次診断可能次数は $\Theta(N/\log N)$ であることを示している．

この統一的な手法を用いて，逐次診断可能性に関するシステムの特徴付けを与えることは今後の課題である．

8.2 確率的耐故障ネットワークに関する研究

ネットワーク G^* は，定確率で独立にプロセッサが故障しても正常なプロセッサからなるネットワーク G を高い確率で含んでいるとき，G の確率的耐故障ネットワークであるという．この概念は参考文献 [1] で提案され，様々な考察がなされている．特に，N 個のプロセッサと M 本の通信リンクからなる任意のネットワークに対して，$O(N)$ 個のプロセッサと $O(M \log^2 N)$ 本の通信リンクからなる確率的耐故障ネットワークが存在することを明らかにすると共に，$O(N)$ 個のプロセッサと $o(M \log^2 N)$ 本の通信リンクからなる確率的耐故障ネットワークが存在するか否かという興味深い公開問題を提案している．

本研究では，様々な実際的なネットワークに対して，この公開問題を肯定的に解決している．すなわち，確率的故障ネットワークを構成する統一的な手法を提案し，N 個のプロセッサと M 本の通信リンクからなる Cayley, deBruijn, シャッフル交換, 及び部分 k 木などのネットワークに対しては，$O(N)$ 個のプロセッサと $O(M \log N)$ 本の通信リンクからなる確率的耐故障ネットワークが存在することを明らかにしている．ここで，Cayley ネットワークは circulant, ハイパーキューブ, CCC, バタフライ, 星, 及びパンケーキなどのよく知られている多くのネットワークを含んでいることに注意されたい．この統一的な手法を用いて，N 個のプロセッサと M 本の通信リンクからなる任意のネットワークに対して，$O(N)$ 個のプロセッサと $O(M \log N)$ 本の通信リンクからなる確率的耐故障ネットワークを構成することができるか否かを明らかにすることは，興味深い今後の課題である．

本研究では，さらに閉路ネットワークの確率的耐故障ネットワークについても考察している．参考文献 [1] において，N 個のプロセッサからなる閉路ネットワークに対して，$O(N)$ 個のプロセッサと $O(N)$ 本の通信リンクからなる確率的耐故障ネットワークが存在することが述べられているが，その証明には不備があり，不完全なものであった．そこで本研究では，この不備を補い，完全な証明を与えると共に，この証明で構成している確率的耐故障ネットワークは極めて実際的であることを計算機実験により明らかにしている．

参考文献

[1] P. Fraigniaud, C. Kenyon, A. Pelc, Finding a target subnetwork in sparse networks with random faults, Inform. Process. Lett. 48 (1993) 297-303.

9 ネットワーク計算に関する研究

本研究では，スケジューリング，ルーチング，及び光結合ネットワークなどの研究を行った．

9.1 ネットワークのスケジューリングに関する研究

本研究では，通信網において先行制約のあるメッセージの集合の最短送信スケジュールを求める問題を考察している．特に，この問題が $\mathcal{NP}$ 困難である場合と多項式時間アルゴリズムで解ける場合の境界を明らかにし，$\mathcal{NP}$ 困難な場合に，近似アルゴリズムの近似比の評価を改善している．

9.2 ネットワークのルーチングに関する研究

本研究ではマルチキャスト通信について考察している．マルチキャスト通信において，1 つの送信元と複数の受信先を張るスタイナー木をマルチキャスト木という．マルチキャスト木のリンクの通信コストの総和をそのマルチキャスト木の通信コストという．また，マルチキャスト木上の送信元から各受信先へのパスのリンクの通信遅延の総和の最大値をそのマルチキャスト木の通信遅延という．マルチキャスト通信においては，通信コストと通信遅延を共に最小化するマルチキャスト木を求める問題が基本的である．

これに関連して，通信遅延を制限したときに通信コストを最小化するマルチキャスト木を求める問題が従来から活発に研究されている．この問題は，直並列ネットワークに対してさえも，$\mathcal{NP}$ 困難であることが知られており，多くのヒューリスティックアルゴリズムが提案されているが，多項式時間近似アルゴリズムとしては，受信先の数が定数で制限されているという非常に限定された場

合に完全多項式時間近似スキームが知られているのみである．本研究では，直並列ネットワークに対して，この問題を解く擬似多項式時間アルゴリズムを初めて提案している．

直並列ネットワークに対してこの問題を解く多項式時間近似アルゴリズムが存在するか否かを解明することは今後の課題である．

また，本研究では，通信コストを制限したときに通信遅延を最小化するマルチキャスト木を求める問題について初めて考察している．この問題もまた，直並列ネットワークに対してさえも，$\mathcal{NP}$ 困難であることを明らかにすると共に，直並列ネットワークに対して，この問題を解く完全多項式時間近似スキームを提案している．

より広いクラスのネットワークに対して多項式時間近似アルゴリズムが存在するか否かを解明することは今後の課題である．

9.3 WDM 光ネットワークのルーチングに関する研究

WDM 光ネットワークのトポロジーが一般化 2 分キャタピラーと呼ばれる特別な木である場合に，通信要求が置換と呼ばれる特別な場合でさえも，ルーチング問題が $\mathcal{NP}$ 困難であることを示している．また，一般化 2 分キャタピラーの置換通信要求に対するルーチングのために必要な波長の数の下界を与えている．

9.4 光結合ネットワークに関する研究

光転置結合システム (OTIS) はネットワークを 3 次元自由空間の光結合によって実現する一つの手法である．deBruijn ネットワークは並列計算機の相互結合網や FFT などの並列計算の基礎構造としてよく用いられている．d 値 D 次元 deBruijn ネットワーク $B(d, D)$ の OTIS 実現に関しては，OTIS 実現に必要なレンズの数が $\Omega(\sqrt{dN})$ であることが知られている．ここで，$N = d^D$ は $B(d, D)$ の点数である．また，D が偶数であるときに，OTIS 実現に必要なレンズの数は $O(d\sqrt{N})$ であることも知られている．

本研究では，任意の正整数 D に対して，OTIS 実現に必要なレンズの数の上界を与えている．すなわち，OTIS 実現に必要なレンズの数は:

$D \equiv 1 \pmod 4$ であるとき，$O(d^{5/2}\sqrt{N})$；
$D \equiv 3 \pmod 4$ であるとき，$O(d^{3/2}\sqrt{N})$；
D が偶数であるとき，$O(d\sqrt{N})$

であることを明らかにしている．

これらの上界と下界の間隙を埋めることは今後の課題である．

研究業績一覧

著書

1. 上野修一，高橋篤司:
“情報とアルゴリズム（電子情報通信工学シリーズ）”, 森北出版株式会社, 2005 年.
概要: グラフ理論，アルゴリズム理論，及び計算複雑度の理論の入門書である．

2. 佐藤泰介，高橋篤司，伊東利哉，上野修一:
“情報基礎数学”, 昭晃堂, 2007 年.
概要: 写像・関係などの概念と離散数学における代表的な証明技法 (数え挙げ・鳩ノ巣原理・対角線論法・数学的帰納法など) の入門書である．

学術論文

1. T. Itoh, Y. Takei, and J. Tarui:
“Constructing Families of ε-Approximate k-Wise Independent Permutations”, IEICE Trans. on Fundamentals, Vol.E87-A, pp.993-1003, 2004.
概要: The notion of k-wise independent permutations has several applications. From the practical point of view, it often suffices to consider almost (i.e., ε-approximate) k-wise independent permutation families rather than k-wise independent permutation families, however, we know little about how to construct families of ε-approximate k-wise independent permutations of small size. For any $n > 0$, let S_n be the set of all permutations on $\{0, 1, \ldots, n-1\}$. In this paper, we investigate the size of families of

ε-approximate k-wise independent permutations and show that (1) for any constant $\varepsilon \geq 0$, if a family $\mathcal{F} \subseteq S_n$ of permutations is ε-approximate k-wise independent, then $|\mathcal{F}| \geq n(n-1)\cdots(n-k+1)$ if $\varepsilon < 1$; $|\mathcal{F}| \geq \{n(n-1)\cdots(n-k+1)\}/(1+\varepsilon)$ otherwise; (2) for any constant $0 < \varepsilon \leq 1$, there exists a family $\mathcal{F} \subseteq S_n$ of ε-approximate k-wise independent permutations such that $|\mathcal{F}| = O(\frac{k \ln n}{\varepsilon^2} n(n-1)\cdots(n-k+1))$; (3) for any constant $\varepsilon > 0$ and any $n = p^m - 1$ with p prime, it is possible to construct a polynomial time samplable family $\mathcal{F} \subseteq S_n$ of ε-approximate pairwise independent permutations such that $|\mathcal{F}| = O(n(n-1)/\varepsilon)$; (4) for any constant $\varepsilon > 0$ and any $n = p^m$ with p prime, it is possible to construct a polynomial time samplable family $\mathcal{F} \subseteq S_n$ of ε-approximate 3-wise independent permutations such that $|\mathcal{F}| = O(n(n-1)(n-2)/\varepsilon)$. Our results are derived by combinatorial arguments, i.e., probabilistic methods and linear algebra methods.

2. K. Nomura, S. Tayu, and S. Ueno:
"On the Orthogonal Drawing of Outerplannar Graphs", Lecture Notes in Computer Science, Vol.3106, pp.300-308, 2004.
概要: In this paper we show that an outerplanar graph G with maximum degree at most 3 has a 2-D orthogonal drawing with no bends if and only if G contains no triangles. We also show that an outerplanar graph G with maximum degree at most 6 has a 3-D orthogonal drawing with no bends if and only if G contains no triangles.

3. T. Yamada, K. Nomura, and S. Ueno:
"Sparse networks tolerating random faults", Discrete Applied Mathematics, Vol.137, pp.223-235, 2004.
概要: A network G^* is called random-fault-tolerant (RFT) network for a network G if G^* contains a fault-free isomorphic copy of G with high probability even if each processor fails independently with constant probability. This paper proposes a general method to construct an RFT network G^* for any network G with N processors such that G^* has $O(N)$ processors. Based on the construction, we also show that if G is a Cayley, de Bruijn, shuffle-exchange, or partial k-tree network with N processors and M communication links then we can construct an RFT network for G with O(N) processors and $O(M \log N)$ communication links. Cayley networks contain many popular networks such as circulant, hypercube, CCC, wrapped butterfly, star, and pancake networks.

4. T. Yamada, T. Ohtsuka, A. Watanabe, and S. Ueno:
"On sequential diagnosis of multiprocessor systems", Discrete Applied Mathematics, Vol.146, pp.311-342, 2005.
概要: This paper considers the problem of sequential fault diagnosis for various multiprocessor systems. We propose a simple sequential diagnosis algorithm and show that the degree of sequential diagnosability of any system with N processors is at least $\Omega(\sqrt{N})$. We also show upper bounds for various networks. These are the first nontrivial upper bounds for the degree of sequential diagnosability, to the best of our knowledge. Our upper bounds are proved in a unified manner, which is based on the very definition of sequential diagnosability. We show that a d-dimensional grid and torus with N vertices are sequentially $O(N^{d/(d+1)})$-diagnosable, and an N-vertex k-ary tree is $O(\sqrt{kN})$-diagnosable. Moreover, we prove that the degree of sequential diagnosability of an N-vertex hypercube is at least $\Omega(N/\sqrt{\log N})$ and at most $O(N \log\log N/\sqrt{\log N})$, and those of an N-vertex CCC, shuffle-exchange graph, and de Bruijn graph are $\Theta(N/\log N)$.

5. S. Tayu, T. Ghazi Al-Mutairi, and S. Ueno: "Cost-Constrained Minimum-Delay Multicasting", Lecture Notes in Computer Science, vol.3381, pp.330-339, 2005.
概要: We consider a problem of cost-constrained minimum-delay multicasting in a network, which is to find a Steiner tree spanning the source and destination nodes such that the maximum total delay along a path from the source node to a destination node is minimized, while the sum of link costs in the tree is bounded by a constant. The problem is $\mathcal{NP}$-hard even if the network is series-parallel. We present a fully polynomial time approximation scheme for the problem if the network is series-parallel.

6. T. Itoh and T. Nagumo:
"Improved Lower Bounds for Competitive Ratio of Multi-Queue Switches in QoS Networks", IEICE Trans. Fundamentals, Vol.E88-A, No.5, pp.1155-1165, 2005.
概要: The recent burst growth of the Internet use overloads networking systems and degrades the quality of communications, e.g., bandwidth loss, packet drops, delay of responses, etc. To overcome such degradation of the communication quality, the notion of Quality of Service (QoS) has received attention in practice. In general, QoS switches have several queues and each queue has several slots to store arriving packets. Since network traffic changes frequently, QoS switches need to control arriving packets to maximize the total priorities of transmitted packets, where the priorities are given by nonnegative values and correspond to the quality of service required for each packet. In this paper, we derive lower bounds for the competitive ratio of deterministic multi-queue nonpreemptive QoS problem of priorities 1 and $\alpha \geq 1$: $1+/\alpha \ln(\frac{\alpha}{\alpha-1})$ if $\alpha \geq \alpha^*$; $1/(1-e^{-\tau_0})$ if $1 \leq \alpha < \alpha^*$, where $\alpha^* \approx 1.657$ and τ_0 is a root of the equality that $e^{-\tau}(1/\alpha+\tau) = 1-e^{-\tau}$. As an immediate result, this shows a lower bound 1.466 for the competitive ratio of deterministic multi-queue nonpreemptive QoS problem of single priority, which slightly improves the best known lower bound 1.366.

7. K. Ogata, T. Yamada, and S. Ueno:
"A Note on the Implementation of de Bruijn Networks by the Optical Transpose Interconnection System", IEICE Trans. Fundamentals, Vol.E88-A, No.12, pp.3661-3662, 2005.
概要: This note shows an efficient implementation of de Bruijn networks by the Optical Transpose Interconnection System (OTIS) extending previous results by Coudert, Ferreira, and Perennes.

8. K. Nomura, S. Tayu, and S. Ueno:
"On the Orthogonal Drawing of Outerplanar Graphs", IEICE Trans. Fundamentals, Vol.E88-A, No.6, pp.1583-1588, 2005.
概要: In this paper we show that an outerplanar graph G with maximum degree at most 3 has a 2-D orthogonal drawing with no bends if and only if G contains no triangles. We also show that an outerplanar graph G with maximum degree at most 6 has a 3-D orthogonal drawing with no bends if and only if G contains no triangles.

9. T. Yamada, H. Kawakita, T. Nishiyama, and S. Ueno:
"On VLSI Decompositions for d-ary de Bruijn Graphs (Extended Abstract)", Proceedings of the IEEE International Symposium on Circuits and Systems, pp.1358-1361, 2005.
概要: A VLSI decomposition of a graph G is a collection of isomorphic vertex-disjoint subgraphs (called building blocks) of G which together span G. The efficiency of a VLSI decomposition is the fraction of the edges of G which are present in the subgraphs. This paper gives a necessary con-

dition and a sufficient condition for a graph to be a building block for d-ary de Bruijn graphs. We also show building blocks for d-ary de Bruijn graphs with asymptotically optimal efficiency. Furthermore, we list the most efficient universal d-ary de Bruijn building blocks we know of.

10. S. Tayu, P. Hurtig, Y. Horikawa, and S. Ueno:
"On the Three-Dimensional Channel Routing", Proceedings of the IEEE International Symposium on Circuits and Systems, pp.180-183, 2005.
概要: The 3-D channel routing is a fundamental problem on the physical design of 3-D integrated circuits. The 3-D channel is a 3-D grid G and the terminals are vertices of G located in the top and bottom layers. A net is a set of terminals to be connected. The object of the 3-D channel routing problem is to connect the terminals in each net with a tree (wire) in G using as few layers as possible and as short wires as possible in such a way that wires for distinct nets are disjoint. This paper shows that any set of n 2-terminal nets can be routed in a 3-D channel with $O(n^{1/2})$ layers using wires of length $O(n^{1/2})$. We also show that there exists a set of n 2-terminal nets that requires a 3-D channel with $\Omega(n^{1/2})$ layers to be routed.

11. K. Goda, T. Yamada, and S. Ueno:
"A Note on the Complexity of Scheduling for Precedence Constrained Messages in Distributed Systems", IEICE Trans. Fundamentals, Vol.E88-A, No.4, pp.1090-1092, 2005.
概要: This note considers a problem of minimum length scheduling for a set of messages subject to precedence constraints for switching and communication networks, and shows some improvements upon previous results on the problem.

12. K. Ogata, T. Yamada, and S. Ueno:
"A Note on the Implementation of de Bruijn Networks by the Optical Transpose Interconnection System", IEICE Trans. Fundamentals, Vol.E88-A, No.12, pp.3661-3662, 2005.
概要: This note shows an efficient implementation of de Bruijn networks by the Optical Transpose Interconnection System (OTIS) extending previous results by Coudert, Ferreira, and Perennes.

13. K. Nomura, S. Tayu, and S. Ueno:
"On the Orthogonal Drawing of Outerplanar Graphs", IEICE Trans. Fundamentals, Vol.E88-A, No.6, pp.1583-1588, 2005.
概要: In this paper we show that an outerplanar graph G with maximum degree at most 3 has a 2-D orthogonal drawing with no bends if and only if G contains no triangles. We also show that an outerplanar graph G with maximum degree at most 6 has a 3-D orthogonal drawing with no bends if and only if G contains no triangles.

14. T. Yamada, H. Kawakita, T. Nishiyama, and S. Ueno:
"On VLSI Decompositions for d-ary de Bruijn Graphs (Extended Abstract)", Proceedings of the IEEE International Symposium on Circuits and Systems, pp.1358-1361, 2005.
概要: A VLSI decomposition of a graph G is a collection of isomorphic vertex-disjoint subgraphs (called building blocks) of G which together span G. The efficiency of a VLSI decomposition is the fraction of the edges of G which are present in the subgraphs. This paper gives a necessary condition and a sufficient condition for a graph to be a building block for d-ary de Bruijn graphs. We also show building blocks for d-ary de Bruijn graphs with asymptotically optimal efficiency. Furthermore, we list the most efficient universal d-ary de Bruijn building blocks we know of.

15. S. Tayu, P. Hurtig, Y. Horikawa, and S. Ueno:
"On the Three-Dimensional Channel Routing", Proceedings of the IEEE International Symposium on Circuits and Systems, pp.180-183, 2005.
概要: The 3-D channel routing is a fundamental problem on the physical design of 3-D integrated circuits. The 3-D channel is a 3-D grid G and the terminals are vertices of G located in the top and bottom layers. A net is a set of terminals to be connected. The object of the 3-D channel routing problem is to connect the terminals in each net with a tree (wire) in G using as few layers as possible and as short wires as possible in such a way that wires for distinct nets are disjoint. This paper shows that any set of n 2-terminal nets can be routed in a 3-D channel with $O(n^{1/2})$ layers using wires of length $O(n^{1/2})$. We also show that there exists a set of n 2-terminal nets that requires a 3-D channel with $\Omega(n^{1/2})$ layers to be routed.

16. K. Goda, T. Yamada, and S. Ueno:
"A Note on the Complexity of Scheduling for Precedence Constrained Messages in Distributed Systems", IEICE Trans. Fundamentals, Vol.E88-A, No.4, pp.1090-1092, 2005.
概要: This note considers a problem of minimum length scheduling for a set of messages subject to precedence constraints for switching and communication networks, and shows some improvements upon previous results on the problem.

17. R. Matsumoto, K. Kurosawa, T. Itoh, T. Konno, and T. Uematsu:
"Primal-Dual Bounds of Linear Codes with Application to Cryptography", IEEE Transactions on Information Theory, Vol.52, No.9, pp.4251-4256, September 2006.
概要: Let $N(d, d^{\perp})$ be the minimum code length n of a linear code $\mathcal{C}$ with d and $d^{\perp}$, where d is the minimum Hamming distance of the code $\mathcal{C}$ and $d^{\perp}$ is the minimum Hamming distance of its dual code $\mathcal{C}^{\perp}$. In this paper, we show several lower bounds and an upper bound on $N(d, d^{\perp})$. Futhermore, for small values of d and $d^{\perp}$, we determine $N(d, d^{\perp})$ and give a generator matrix of the optimal linear code. This problem is directly related to the design method of cryptograpic Boolean functions suggested by Kurosawa, et al.

18. T. Itoh and N. Takahashi:
"Competitive Analysis of Multi-Queue Preemptive QoS Algorithms for General Priorities", IEICE Transactions on Fundamentals, Vol.E89-A, No.5, pp.1186-1197, 2006.
概要: The recent burst growth of the Internet use overloads networking systems and degrades the quality of communications, e.g., bandwidth loss, packet drops, delay of responses, etc. To overcome such degradation of communication quality, the notion of Quality of Service (QoS) has received attention in practice. In general, QoS switches have several queues and each queue has several slots to store arriving packets. Since network traffic changes frequently, QoS switches need to control arriving packets to maximize the total priorities of transmitted packets, where the priorities are given by nonnegative values and correspond to the quality of service required to each packet. In this paper, we first derive the upper bounds for the competitive ratio of multi-queue preemptive QoS problem with priority between $1/\alpha$ and 1, i.e., for any $\alpha \geq 1$, the algorithm TLH is $(3 - 1/\alpha)$-competitive. This is a generalization of known results—for the case that packets have only priority 1 ($\alpha = 1$), the algorithm GREEDY (or TLH) is 2-competitive; for the case that packets have priorities between 0 and 1 ($\alpha = \infty$), the algorithm TLH is 3-

competitive. Then we consider the lower bounds for the competitive ratio of multi-queue preemptive QoS problem with priority between 0 and 1, and show that the competitive ratio of any multi-queue preemptive QoS algorithm is at least 1.514.

19. S. Tayu, K. Nomura, and S. Ueno:
"On the Two-Dimensional Orthogonal Drawing of Series-Parallel Graphs", Proceedings of the 2006 IEEE International Symposium on Circuits and Systems, pp.1796-1799, 2006.
概要: It has been known that every planar 4-graph has a 2-bend 2-D orthogonal drawing with the only exception of octahedron, every planar 3-graph has a 1-bend 2-D orthogonal drawing with the only exception of K_4, and every outerplanar 3-graph with no triangles has a 0-bend 2-D orthogonal drawing. We show in this paper that every series-parallel 4-graph has a 1-bend 2-D orthogonal drawing.

20. N. Alon, T. Itoh, and T. Nagatani:
"On (ε, k)-min-wise independent permutations", Random Structures and Algorithms, Vol.31, No.3, pp.384-389, 2007.
概要: A family of permutations $\mathcal{F}$ of $[n] = \{1, 2, \ldots, n\}$ is (ε, k)-min-wise independent if for every nonempty subset X of at most k elements of $[n]$, and for any $x \in X$, the probability that in a random element π of $\mathcal{F}$, $\pi(x)$ is the minimum element of $\pi(X)$, deviates from $1/|X|$ by at most $\varepsilon/|X|$. This notion can be defined for the uniform case, when the elements of $\mathcal{F}$ are picked according to a uniform distribution, or for the more general, biased case, in which the elements of $\mathcal{F}$ are chosen according to a given distribution D. It is known that this notion is a useful tool for indexing replicated documents on the web. We show that even in the more general, biased case, for all admissible k and ε and all large n, the size of $\mathcal{F}$ must satisfy

$$|\mathcal{F}| \geq \Omega\left(\frac{k}{\varepsilon^2 \log(1/\varepsilon)} \log n\right),$$

as well as

$$|\mathcal{F}| \geq \Omega\left(\frac{k^2}{\varepsilon \log(1/\varepsilon)} \log n\right).$$

This improves the best known previous estimates even for the uniform case.

21. S. Tayu and S. Ueno:
"The Complexity of Three-Dimensional Channel Routing", Proceedings of the 5th Hungarian-Japanese Symposium on Discrete Mathematics and Its Applications, pp.279-288, 2007.
概要: The 3-D channel routing is a fundamental problem on the physical design of 3-D integrated circuits. The 3-D channel is a 3-D grid G and the terminals are vertices of G located in the top and bottom layers. A net is a set of terminals to be connected. The objective of the 3-D channel routing problem is to connect the terminals in each net with a tree (wire) in G using as few layers as possible and as short wires as possible in such a way that wires for distinct nets are disjoint. This paper shows that the problem is intractable.

22. S. Tayu and S. Ueno:
"On the Complexity of Three-Dimensional Channel Routing", Proceedings of 2007 IEEE International Symposium on Circuits and Systems, pp.3399-3402, 2007.
概要: The 3-D channel routing is a fundamental problem on the physical design of 3-D integrated circuits. The 3-D channel is a 3-D grid G and the terminals are vertices of G located in the top and bottom layers. A net is a set of terminals to be connected. The objective of the 3-D channel routing problem is to connect the terminals in each net with a tree (wire) in G using as few layers as possible and as short wires as

possible in such a way that wires for distinct nets are disjoint. This paper shows that the problem is intractable.

23. S. Tayu, S. Ito, and S. Ueno:
"On the Fault Testing for Reversible Circuits", Lecture Notes in Computer Science, Vol.4835, pp.812-821, 2007.
概要: This paper shows that it is $\mathcal{NP}$-hard to generate a minimum complete test set for stuck-at faults on the wires of a reversible circuit. We also show non-trivial lower bounds for the size of a minimum complete test set.

24. R. Hamane and T. Itoh:
"Improved Approximation Algorithms for Item Pricing with Bounded Degree and Valuation", to appear in IEICE Transactions on Fundamentals, 2008.
概要: When a store sells items to customers, the store wishes to decide the prices of the items to maximize its profit. If the store sells the items with low (resp. high) prices, the customers buy more (resp. less) items, which provides less profit to the store. It would be hard for the store to decide the prices of items. Assume that a store has a set V of n items and there is a set C of m customers who wish to buy those items. The goal of the store is to decide the price of each item to maximize its profit. We refer to this maximization problem as an *item pricing* problem. We classify the item pricing problems according to how many items the store can sell or how the customers valuate the items. If the store can sell every item i with unlimited (resp. limited) amount, we refer to this as *unlimited* supply (resp. *limited* supply). We say that the item pricing problem is *single-minded* if each customer $j \in C$ wishes to buy a set $e_j \subseteq V$ of items and assigns valuation $w(e_j) \geq 0$. For the single-minded item pricing problems (in unlimited supply), Balcan and Blum regarded them as weighted k-hypergraphs and gave several approximation algorithms. In this paper, we focus on the (pseudo)degree of k-hypergraphs and the valuation ratio, i.e., the ratio between the smallest and the largest valuations. Then for the single-minded item pricing problems (in unlimited supply), we show improved approximation algorithms (for k-hypergraphs, general graphs, bipartite graphs, etc.) with respect to the maximum (pseudo)degree and the valuation ratio.

研究会等

1. T. Itoh, T. Nagatani, and J. Tarui:
"Explicit Construction of k-Wise Nearly Random Permutations by Iterated Feistel Transform", IEICE Technical Report, Vol.COMP2004-7, pp.45-52, 2004.
概要: A notion of k-wise random permutations has several theoretical applications. From the practical point of view, it often suffices to consider ε-approximate k-wise random permutation families rather than k-wise random permutation families, however, we know little about how to construct families of ε-approximate k-wise random permutations of small size. For any integer $n > 0$, we use S_n to denote the set of all permutations on $\{0, 1, \ldots, n-1\}$. In this paper, we iteratively apply the *Feistel Transform* and show that for any $n = p^{2h}$ with p prime and any $k = O(\log n)$, there exists a family $\mathcal{F} \subseteq S_n$ of ε-approximate k-wise random permutations such that $|\mathcal{F}| = (n^{k^2}/\varepsilon^k)^{3+o(1)}$. This is the first nontrivial construction for families of ε-approximate k-wise random permutations. To capture efficient evaluation of permutation families in practice, we introduce a notion of "$s(n)$-space pointwise samplability" and show that the family $\mathcal{F} \subseteq S_n$ of permutations constructed in this paper is

$O(\log n)$-space pointwise samplable.

2. K. Nomura, S. Tayu, and S. Ueno:
"On the Orthogonal Drawing of Series-Parallel Graphs", IPSJ SIG Technical Report, Vol.2004-AL-98, pp.25-32, 2004.
概要: We show in this paper that every series-parallel graph with maximum degree at most 4 has a 1-bend 2-D orthogonal drawing. We also show that every series-parallel graph with maximum degree at most 6 has a 2-bend 3-D orthogonal drawing.

3. S. Tayu, P. Hurtig, Y. Horikawa, and S. Ueno:
"On the Three-Dimensional Channel Routing", IPSJ SIG Technical Report, Vol.2004-AL-98, pp.19-23, 2004.
概要: The 3-D channel routing is a fundamental problem on the physical design of 3-D integrated circuits. The 3-D channel is a 3-D grid G and the terminals are vertices of G located in the top and bottom layers. A net is a set of terminals to be connected. The object of the 3-D channel routing problem is to connect the terminals in each net with a tree (wire) in G using as few layers as possible and as short wires as possible in such a way that wires for distinct nets are disjoint. This paper shows that any set of n 2-terminal nets can be routed in a 3-D channel with $O(\sqrt{n})$ layers using wires of length $O(\sqrt{n})$. We also show that there exists a set of n 2-terminal nets that requires a 3-D channel with $\Omega(\sqrt{n})$ layers to be routed.

4. S. Tayu, T. Ghazi Al-Mutairi, and S. Ueno:
"Cost-Constrained Minimum-Delay Multicasting", Technical Report of IEICE, Vol.104, no.115, pp.43-48, 2004.
概要: We consider a problem of cost-constrained minimum-delay multicasting in a network, which is to find a Steiner tree spanning the source and destination nodes such that the maximum total delay along a path from the source node to a destination node is minimized, while the sum of link costs in the tree is bounded by a constant. The problem is $\mathcal{NP}$-hard even if the network is series-parallel. We present a fully polynomial time approximation scheme for the problem if the network is series-parallel. %

5. S. Tayu, K. Nomura, and S. Ueno:
"On the Two-Dimensional Orthogonal Drawing of Series-Parallel Graphs", IEICE Technical Report, Vol.105, No.387, pp.51-56, 2005.
概要: It has been known that every planar 4-graph has a 2-bend 2-D orthogonal drawing with the only exception of octahedron, every planar 3-graph has a 1-bend 2-D orthogonal drawing with the only exception of K_4, and every outerplanar 3-graph with no triangles has a 0-bend 2-D orthogonal drawing. We show in this paper that every series-parallel 4-graph has a 1-bend 2-D orthogonal drawing.

6. S. Ito, Y. Ito, S. Tayu, and S. Ueno:
"On the Complexity of Fault Testing for Reversible Circuits", IEICE Technical Report, Vol.105, No.387, pp.13-16, 2005.
概要: This paper shows that it is $\mathcal{NP}$-hard to generate a minimum complete test set for stuck-at faults on a set of wires of a reversible circuit.

7. T. Itoh, T. Nagatani, and J. Tarui:
"Explicit Construction for k-Wise Nearly Random Permutations by Iterated Feistel Transform", Proceedings of Randomness and Computation, 2005.
概要: A notion of k-wise random permutations has several applications. From the practical point of view, it often suffices to consider ε-approximate k-wise random permutation families rather than k-wise random permutation families, however, we know little about how to construct fam-

ilies of ε-approximate k-wise random permutations of small size. For any integer $n > 0$, we use S_n to denote the set of all permutations on $\{0, 1, \ldots, n-1\}$. In this paper, we iteratively apply the *Feistel Transform* to construct a family of ε-approximate k-wise random permutations and we show that for any $n = p^{2h}$ with p prime and any $k = O(\log n)$, there exists a family $\mathcal{F} \subseteq S_n$ of ε-approximate k-wise random permutations such that $|\mathcal{F}| = (n^{k^2}/\varepsilon^k)^{3+o(1)}$. This is the first nontrivial construction for families of ε-approximate k-wise random permutations. To capture efficient evaluation of permutation families in the practical point of view, we introduce a notion of "$s(n)$-space pointwise samplability," and show that the family $\mathcal{F} \subseteq S_n$ of permutations constructed in this paper is $O(\log n)$-space pointwise samplable.

8. R. Matsumoto, K. Kurosawa, and T. Itoh:
"Primal-Dual Distance Bounds of Linear Codes with Application to Cryptography", Cryptology ePrint Archive, Report2005/194, 2005.
概要: We propose upper and lower bounds on the minimum code length of linear codes with specified minimum Hamming distance and dual distance. From these bounds we can estimate the minimum input length of Boolean functions with specified cryptographic strength constructed by the design method of Kurosawa et al. %

9. S. Tayu, K. Nomura, and S. Ueno:
"On the Two-Dimensional Orthogonal Drawing of Series-Parallel Graphs", IEICE Technical Report, Vol.105, No.387, pp.51-56, 2005.
概要: It has been known that every planar 4-graph has a 2-bend 2-D orthogonal drawing with the only exception of octahedron, every planar 3-graph has a 1-bend 2-D orthogonal drawing with the only exception of K_4, and every outerplanar 3-graph with no triangles has a 0-bend 2-D orthogonal drawing. We show in this paper that every series-parallel 4-graph has a 1-bend 2-D orthogonal drawing.

10. S. Ito, Y. Ito, S. Tayu, and S. Ueno:
"On the Complexity of Fault Testing for Reversible Circuits", IEICE Technical Report, Vol.105, No.387, pp.13-16, 2005.
概要: This paper shows that it is $\mathcal{NP}$-hard to generate a minimum complete test set for stuck-at faults on a set of wires of a reversible circuit.

11. T. Itoh, T. Nagatani, and J. Tarui:
"Explicit Construction for k-Wise Nearly Random Permutations by Iterated Feistel Transform", Proceedings of Randomness and Computation, 2005.
概要: A notion of k-wise random permutations has several applications. From the practical point of view, it often suffices to consider ε-approximate k-wise random permutation families rather than k-wise random permutation families, however, we know little about how to construct families of ε-approximate k-wise random permutations of small size. For any integer $n > 0$, we use S_n to denote the set of all permutations on $\{0, 1, \ldots, n-1\}$. In this paper, we iteratively apply the *Feistel Transform* to construct a family of ε-approximate k-wise random permutations and we show that for any $n = p^{2h}$ with p prime and any $k = O(\log n)$, there exists a family $\mathcal{F} \subseteq S_n$ of ε-approximate k-wise random permutations such that $|\mathcal{F}| = (n^{k^2}/\varepsilon^k)^{3+o(1)}$. This is the first nontrivial construction for families of ε-approximate k-wise random permutations. To capture efficient evaluation of permutation families in the practical point of view, we introduce a notion of "$s(n)$-space pointwise samplability," and show that the family $\mathcal{F} \subseteq S_n$ of permutations constructed

in this paper is $O(\log n)$-space pointwise samplable.

12. T. Itoh:
"Improved Lower Bounds for Families of ε-Approximate k-Restricted Min-Wise Independent Permutations", Electronic Colloquium on Computational Complexity, TR06-017, 2006.
概要: A family $\mathcal{F}$ of min-wise independent permutations is known to be a useful tool of indexing replicated documents on the Web. For any integer $n > 0$, let S_n be the family of all permutations on $[1, n] = \{1, 2, \ldots, n\}$. For any integer k such that $1 \leq k \leq n$ and any $\varepsilon > 0$, we say that a family $\mathcal{F} \subseteq S_n$ of permutations is ε-approximate k-restricted min-wise independent if for any (nonempty) subset $X \subseteq [1, n]$ such that $|X| \leq k$ and any element $x \in X$, $|\Pr[\min\{\pi(X)\} = \pi(x)] - |X|^{-1}| \leq \varepsilon/|X|$, when π is chosen from $\mathcal{F}$ uniformly at random (where $|A|$ denotes the cardinality of a finite set A). For the size of families $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, the following results are known: For any integer k such that $1 \leq k \leq n$ and any real $\varepsilon > 0$, (constructive upper bound) $|\mathcal{F}| = 2^{4k+o(k)} k^{2 \log\log(n/\varepsilon)}$; (nonconstructive upper bound) $|\mathcal{F}| = O\big(\frac{k^2}{\varepsilon^2} \log(n/k)\big)$; (lower bound) $|\mathcal{F}| = \Omega\big(k^2(1 - \sqrt{8\varepsilon})\big)$ and $|\mathcal{F}| = \Omega\big(\min\{k^2 2^{k/2} \log(n/k), \frac{\log(1/\varepsilon)(\log n - \log\log(1/\varepsilon))}{\varepsilon^{1/3}}\}\big)$. In this paper, we first derive an upper bound for the Ramsey number of the edge coloring with $m \geq 2$ colors of a complete graph K_ℓ of ℓ vertices, and by the linear algebra method, we then derive a slightly improved lower bound, i.e., we show that for any family $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, $|\mathcal{F}| = \Omega\big(k\sqrt{\frac{1}{\varepsilon} \log(n/k)}\big)$.

13. T. Itoh and T. Nagatani:
"Improved Lower Bounds for Families of *varepsilon*-Approximate k-Restricted Min-Wise Independent Permutations", IEICE Technical Report, Vol.COMP2006, No.66, pp.23-30, 2006.
概要: A family $\mathcal{F}$ of min-wise independent permutations is known to be a useful tool of indexing replicated documents on the Web. For any integer $n > 0$, let S_n be the family of all permutations on $[1, n] = \{1, 2, \ldots, n\}$. For any integer k such that $1 \leq k \leq n$ and any real $\varepsilon > 0$, we say that a family $\mathcal{F} \subseteq S_n$ of permutations is *ε-approximate k-restricted min-wise independent* if for any (nonempty) subset $X \subseteq [1, n]$ such that $|X| \leq k$ and any element $x \in X$, $|\Pr[\min\{\pi(X)\} = \pi(x)] - |X|^{-1}| \leq \varepsilon/|X|$, when π is chosen from $\mathcal{F}$ uniformly at random (where $|A|$ denotes the cardinality of a finite set A). For the size of families $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, the following results are known: For any integer k such that $1 \leq k \leq n$ and any real $\varepsilon > 0$, (constructive upper bound) $|\mathcal{F}| = 2^{4k+o(k)} k^{2 \log\log(n/\varepsilon)}$; (nonconstructive upper bound) $|\mathcal{F}| = O\big(\frac{k^2}{\varepsilon^2} \log(n/k)\big)$; (lower bound) $|\mathcal{F}| = \Omega\big(k^2(1 - \sqrt{8\varepsilon})\big)$ and $|\mathcal{F}| = \Omega\big(\min\{k^2 2^{k/2} \log(n/k), \frac{\log(1/\varepsilon)(\log n - \log\log(1/\varepsilon))}{\varepsilon^{1/3}}\}\big)$. In this paper, we first derive an upper bound for the Ramsey number of the edge coloring with $m \geq 2$ colors of a complete graph K_ℓ of ℓ vertices, and by the linear algebra method, we then derive a slightly improved lower bound, i.e., we show that for any family $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, $|\mathcal{F}| = \Omega\big(k\sqrt{\frac{1}{\varepsilon} \log(n/k)}\big)$.

14. S. Tayu, K. Nomura, and S. Ueno:
"On the Three-Dimensional Orthogonal Drawing of Series-Parallel Graphs", IEICE Technical Report, Vol.105, No.502, pp.7-12, 2006.

概要: It has been known that every 6-graph has a 3-bend 3-D orthogonal drawing, while it has been open whether every 6-graph has a 2-bend 3-D orthogonal drawing. For the interesting open question, it is known that every 5-graph has a 2-bend 3-D orthogonal drawing, and every outerplanar 6-graph without triangles has a 0-bend 3-D orthogonal drawing. We show in this paper that every series-parallel 6-graph has a 2-bend 3-D orthogonal drawing.

15. T. Itoh:
"Improved Lower Bounds for Families of ε-Approximate k-Restricted Min-Wise Independent Permutations", Electronic Colloquium on Computational Complexity, TR06-017, 2006.
概要: A family $\mathcal{F}$ of min-wise independent permutations is known to be a useful tool of indexing replicated documents on the Web. For any integer $n > 0$, let S_n be the family of all permutations on $[1, n] = \{1, 2, \ldots, n\}$. For any integer k such that $1 \leq k \leq n$ and any $\varepsilon > 0$, we say that a family $\mathcal{F} \subseteq S_n$ of permutations is ε-approximate k-restricted min-wise independent if for any (nonempty) subset $X \subseteq [1, n]$ such that $|X| \leq k$ and any element $x \in X$, $|\Pr[\min\{\pi(X)\} = \pi(x)] - |X|^{-1}| \leq \varepsilon/|X|$, when π is chosen from $\mathcal{F}$ uniformly at random (where $|A|$ denotes the cardinality of a finite set A). For the size of families $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, the following results are known: For any integer k such that $1 \leq k \leq n$ and any real $\varepsilon > 0$, (constructive upper bound) $|\mathcal{F}| = 2^{4k+o(k)} k^{2 \log\log(n/\varepsilon)}$; (nonconstructive upper bound) $|\mathcal{F}| = O\big(\frac{k^2}{\varepsilon^2} \log(n/k)\big)$; (lower bound) $|\mathcal{F}| = \Omega\big(k^2(1 - \sqrt{8\varepsilon})\big)$ and $|\mathcal{F}| = \Omega\big(\min\{k^2 2^{k/2} \log(n/k), \frac{\log(1/\varepsilon)(\log n - \log\log(1/\varepsilon))}{\varepsilon^{1/3}}\}\big)$. In this paper, we first derive an upper bound for the Ramsey number of the edge coloring with $m \geq 2$ colors of a complete graph K_ℓ of ℓ vertices, and by the linear algebra method, we then derive a slightly improved lower bound, i.e., we show that for any family $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, $|\mathcal{F}| = \Omega\big(k\sqrt{\frac{1}{\varepsilon} \log(n/k)}\big)$.

16. T. Itoh and T. Nagatani:
"Improved Lower Bounds for Families of *varepsilon*-Approximate k-Restricted Min-Wise Independent Permutations", IEICE Technical Report, Vol.COMP2006, No.66, pp.23-30, 2006.
概要: A family $\mathcal{F}$ of min-wise independent permutations is known to be a useful tool of indexing replicated documents on the Web. For any integer $n > 0$, let S_n be the family of all permutations on $[1, n] = \{1, 2, \ldots, n\}$. For any integer k such that $1 \leq k \leq n$ and any real $\varepsilon > 0$, we say that a family $\mathcal{F} \subseteq S_n$ of permutations is *ε-approximate k-restricted min-wise independent* if for any (nonempty) subset $X \subseteq [1, n]$ such that $|X| \leq k$ and any element $x \in X$, $|\Pr[\min\{\pi(X)\} = \pi(x)] - |X|^{-1}| \leq \varepsilon/|X|$, when π is chosen from $\mathcal{F}$ uniformly at random (where $|A|$ denotes the cardinality of a finite set A). For the size of families $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, the following results are known: For any integer k such that $1 \leq k \leq n$ and any real $\varepsilon > 0$, (constructive upper bound) $|\mathcal{F}| = 2^{4k+o(k)} k^{2 \log\log(n/\varepsilon)}$; (nonconstructive upper bound) $|\mathcal{F}| = O\big(\frac{k^2}{\varepsilon^2} \log(n/k)\big)$; (lower bound) $|\mathcal{F}| = \Omega\big(k^2(1 - \sqrt{8\varepsilon})\big)$ and $|\mathcal{F}| = \Omega\big(\min\{k^2 2^{k/2} \log(n/k), \frac{\log(1/\varepsilon)(\log n - \log\log(1/\varepsilon))}{\varepsilon^{1/3}}\}\big)$. In this paper, we first derive an upper bound for the Ramsey number of the edge coloring with $m \geq 2$ colors of a complete graph K_ℓ of ℓ vertices, and by the linear algebra method, we then derive a slightly improved lower bound, i.e., we show that for any family

$\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, $|\mathcal{F}| = \Omega\big(k\sqrt{\frac{1}{\varepsilon}\log(n/k)}\big)$.

17. S. Tayu, K. Nomura, and S. Ueno:
"On the Three-Dimensional Orthogonal Drawing of Series-Parallel Graphs", IEICE Technical Report, Vol.105, No.502, pp.7-12, 2006.
概要: It has been known that every 6-graph has a 3-bend 3-D orthogonal drawing, while it has been open whether every 6-graph has a 2-bend 3-D orthogonal drawing. For the interesting open question, it is known that every 5-graph has a 2-bend 3-D orthogonal drawing, and every outerplanar 6-graph without triangles has a 0-bend 3-D orthogonal drawing. We show in this paper that every series-parallel 6-graph has a 2-bend 3-D orthogonal drawing.

18. R. Matsumoto, K. Kurosawa, and T. Itoh:
"Primal-Dual Distance Bounds of Linear Codes with Application to Cryptography", Cryptology ePrint Archive, Report2005/194, 2005.
概要: We propose upper and lower bounds on the minimum code length of linear codes with specified minimum Hamming distance and dual distance. From these bounds we can estimate the minimum input length of Boolean functions with specified cryptographic strength constructed by the design method of Kurosawa et al.

19. S. Tayu and S. Ueno:
"The Complexity of Three-Dimensional Channel Routing", IEICE Technical Report, Vol.106, No.366, pp.37-41, 2006.
概要: The 3-D channel routing is a fundamental problem on the physical design of 3-D integrated circuits. The 3-D channel is a 3-D grid G and the terminals are vertices of G located in the top and bottom layers. A net is a set of terminals to be connected. The objective of the 3-D channel routing problem is to connect the terminals in each net with a Steiner tree (wire) in G using as few layers as possible and as short wires as possible in such a way that wires for distinct nets are disjoint. This paper shows that the problem is intractable.

20. R. Hamane and T. Itoh:
"Improved Approximation Algorithms for Item Pricing with Bounded Degree and Valuation", IEICE Technical Report, Vol.COMP2007, No.1, pp.1-8, 2007.
概要: When a store sells items to customers, the store wishes to decide the prices of the items to maximize its profit. If the store sells the items with low (resp. high) prices, the customers buys more (resp. less) items, which provides less profit to the store. So it would be hard for the store to decide the prices of items. Assume that a store has a set V of n items and there is a set C of m customers who wish to buy those items. The goal of the store is to decide the price of each item to maximize its profit. We refer to this maximization problem as an *item pricing* problem. We classify the item pricing problem according to how many items the store can sell and how the customers valuate the items. If the store can sell every item i with unlimited (resp. limited) amount, we refer to this as an *unlimited* supply model (resp. a *limited* supply model). The item pricing problem is said to be *single-minded* if each customer $j \in C$ wishes to buy a set $e_j \subseteq V$ of items and assigns its valuation $w(e_j) \geq 0$. Balcan and Blum regarded the single-minded item pricing problems (in unlimited supply model) as weighted k-hypergraphs and described several approximation algorithms. In this paper, we consider the maximum (pseudo)degree of k-hypergraphs and the valuation ratio, i.e., the ratio between the smallest and the largest valuations. Then for the single-minded unlimited supply

item pricing problems, we show improved approximation algorithms w.r.t. the maximum (pseudo)degree and the valuation ratio.

21. T. Itoh and O. Watanabe:
"Weighted Random Popular Matchings", IEICE Technical Report, Vol.COMP2007, No.23, pp.41-48, 2007.
概要: Let A be the set of n applicants and I be the set of m items. We assume that the set A is partitioned into $A_1, A_2, \ldots, A_k$ and each A_i is assigned a weight w_i such that $w_1 > w_2 > \cdots > w_k > 0$. Let us consider the problem of matching applicants to items, where each applicant $x \in A$ provides a *preference list* defined on items. We say that an applicant x prefers an item p than an item q if p is located at higher position than q in the preference list. For any matchings $\mathcal{M}$ and $\mathcal{M}'$, we say that an applicant x prefers $\mathcal{M}$ over $\mathcal{M}'$ if x prefers $\mathcal{M}(x)$ over $\mathcal{M}'(x)$. We say that $\mathcal{M}$ is *more popular* than $\mathcal{M}'$ if the total weight of applicants preferring $\mathcal{M}$ over $\mathcal{M}'$ is larger than that of applicants preferring $\mathcal{M}'$ over $\mathcal{M}$, and define $\mathcal{M}$ to be a *k-weighted popular matching* if there are no other matchings that are more popular than $\mathcal{M}$. For the case where $k = 1$, Mahdian showed that if $m > 1.42n$, then a random instance of the matching problem has a popular matching with high probability, but nothing is known for the k-weighted matching problems. In this paper, we analyze the k-weighted matching problems, and show that for any β such that $m = \beta n$, (lower bound) if $\beta/n^{1/3} = o(1)$, then a random instance of the 2-weighted matching problems does not have a 2-weighted popular matching with probability $1 - o(1)$; (upper bound) if $n^{1/3}/\beta = o(1)$, then a random instance of the 2-weighted matching problems has a 2-weighted popular matching with probability $1 - o(1)$.

22. R. Hamane, T. Itoh, and K. Tomita:
"Approximation Algorithms for the Highway Problem under the Coupon Model", arXiv.org, arXiv:0712.2629, 2007.
概要: When a store sells items to customers, the store wishes to decide the prices of items to maximize its profit. Intuitively, if the store sells the items with low (resp. high) prices, the customers buy more (resp. less) items, which provides less profit to the store. So it would be hard for the store to decide the prices of items. Assume that the store has a set V of n items and there is a set E of m customers who wish to buy the items, and also assume that each item $i \in V$ has the production cost d_i and each customer $e_j \in E$ has the valuation v_j on the bundle $e_j \subseteq V$ of items. When the store sells an item $i \in V$ at the price r_i, the profit for the item i is $p_i = r_i - d_i$. The goal of the store is to decide the price of each item to maximize its total profit. We refer to this maximization problem as the *item pricing* problem. In most of the previous works, the item pricing problem was considered under the assumption that $p_i \geq 0$ for each $i \in V$, however, Balcan, et al. [In Proc. of WINE, LNCS 4858, 2007] introduced the notion of "loss-leader," and showed that the seller can get more total profit in the case that $p_i < 0$ is allowed than in the case that $p_i < 0$ is not allowed. In this paper, we consider the line highway problem (in which each customer is interested in an interval on the line of the items) and the cycle highway problem (in which each customer is interested in an interval on the cycle of the items), and show approximation algorithms for the line highway problem and the cycle highway problem in which the smallest valuation is s and the largest valuation is ℓ (this is called an $[s, \ell]$-valuation setting) or all valuations are identical (this is called a single valuation setting).

23. S. Tayu, S. Ito, and S. Ueno:
"On the Fault Testing for Reversible Circuits", IPSJ SIG Technical Reports, Vol. 2007, No.66, pp.25-30, 2007.
概要: This paper shows that it is $\mathcal{NP}$-hard to generate a minimum complete test set for stuck-at faults on the wires of a reversible circuit. We also show non-trivial lower bounds for the size of a minimum complete test set.

24. A. M. S. Shrestha, S. Tayu, and S. Ueno:
"On the Permutation Routing in All-Optical Caterpillar Networks", IEICE Technical Report, Vol. 107, No. 361, pp. 23-27, 2007.
概要: We consider the optical routing for permutation requests in a WDM all-optical tree network. We show that the optical routing problem is $\mathcal{NP}$-hard even for permutation requests in a binary generalized caterpillar. We also show a lower bound for the number of wavelengths to route permutation requests in a binary generalized caterpillar.

学会大会等

1. K. Nomura, S. Tayu, and S. Ueno:
"On the Two-Dimensional Orthogonal Drawing of Series-Parallel Graphs", Proceedings of the 2004 IEICE Society Conference, 2004.

2. S. Tayu, P. Hurtig, Y. Horikawa, and S. Ueno:
"On the Three-Dimensional Channel Routing", Proceedings of the 2004 IEICE Society Conference, 2004.

3. H. Kawakita, T. Yamada, and S. Ueno:
"Efficient VLSI Decompositions for de Bruijn Graphs", Proc. of the 66th National Convention of IPSJ, Vol.1, pp.265-266, 2004.

4. S. Tayu and S. Ueno:
"A Note on the Three-Dimensional Channel Routing", Proceedings of the 2005 IEICE General Conference, p.30, 2005.

5. K. Inoue, K. Nomura, S. Tayu, and S. Ueno:
"A Note on Sparse Networks Tolerating Random Faults for Cycles", Proceedings of the 2005 IEICE General Conference, p.31, 2005.

6. S. Tayu, Y. Horikawa, and S. Ueno:
"On the Three-Dimensional Layout of Butterfly Networks", Proceedings of the 2005 IEICE Society Conference, A-1-27, p.27, 2005.

7. S. Ito, Y. Ito, S. Tayu, and S. Ueno:
"On the Complexity of Fault Testing for Reversible Circuits", Proceedings of the 2005 IEICE Society Conference, A-1-26, p.26, 2005.

8. S. Tayu, Y. Horikawa, and S. Ueno:
"On the Three-Dimensional Layout of Butterfly Networks", Proceedings of the 2005 IEICE Society Conference, A-1-27, p.27, 2005.

9. S. Ito, Y. Ito, S. Tayu, and S. Ueno:
"On the Complexity of Fault Testing for Reversible Circuits", Proceedings of the 2005 IEICE Society Conference, A-1-26, p.26, 2005.

10. T. Yamaguchi, S. Tayu, and S. Ueno:
"On the Complexity of Three-Dimensional Channel Routing", Proceedings of the 68th National Convension of IPSJ, pp.1-193 – 1-194, 2006.

11. T. Yamaguchi, S. Tayu, and S. Ueno:
"On the Complexity of Three-Dimensional Channel Routing", Proceedings of the 68th National Convension of IPSJ, pp.1-193 – 1-194, 2006.

12. S. Ito, S. Tayu, and S. Ueno:
"The Complexity of Fault Testing for Reversible Circuits", Proceedings of the 2006 IEICE Society Conference, pp.S-1 - S-2, 2006.

13. S. Tayu and S. Ueno:
"Three-Dimensional Channel Routeing is in $\mathcal{NP}$", Proceedings of the 2006 IEICE Society Conference, pp.S-5 - S-6, 2006.

14. T. Kubo, S. Tayu: and S. Ueno:
"On the Three-Dimensional Layout of Hypercubes", Proceedings of the 2006 IEICE Society Conference, pp.S-7 - S-8, 2006.

15. F. Cai, S. Tayu, and S. Ueno:
"On the Quantum Query Complexity of All-Pairs Shortest Paths", Proceedings of the 2007 IEICE General Conference, p.20, 2007.

16. Y. Arai, S. Tayu, and S. Ueno:
"A Note on the Three-Dimensional Single-Active Layer Routing", Proceedings of the 2007 IEICE General Conference, p.21, 2007.

文部科学省科学研究費補助金 特定領域研究 (課題番号 160922106)

B02: 暗号解析手法の計算量理論による改良とそれに基づく暗号方式

暗号解析手法の計算量理論による改良とそれに基づく暗号方式の提案を行うために，暗号の安全性および効率に関する精密な解析手法の開発に関して以下のような研究を行った。戸田はグラフ同型性判定問題の計算量解析を主に行った。渡辺は、NP-困難な問題に対するヒューリスティックスの理論的な解析、NP-困難な問題に対する低指数関数計算量アルゴリズムの開発、NP-困難な問題の構造的な計算量解析、学習アルゴリズムに関する研究を主に行った。河内は、量子質問計算量の上下界の解析、量子計算量理論に基づく暗号系設計を主に行った。田中は、上記の研究をもとに具体的な暗号プロトコルの提案を主に行った。これらの研究に関連して本特定研究のイベントとして、戸田が 2005 年にグラフアルゴリズムに関するミニ研究集会を、田中が 2006 年と 2007 年に暗号理論に関するミニ研究集会を開催した。

研究組織

研究代表者：	田中 圭介	東京工業大学 大学院 情報理工学研究科
研究分担者：	渡辺 治	東京工業大学 大学院 情報理工学研究科
	戸田 誠之助	日本大学 文理学部
	河内 亮周	東京工業大学 大学院 情報理工学研究科
		(平成 17–19 年度)

交付決定額 (配分額)

平成 16 年度	5,800,000 円
平成 17 年度	5,500,000 円
平成 18 年度	5,500,000 円
平成 19 年度	5,800,000 円
合　計	22,600,000 円

研究成果の概要

- 学術誌
  SIAM Journal on Computing (2004), Theoretical Computer Science (2005, 2007), Information Processing Letters (2004) を含む 23 件.
- 国際会議
  EUROCRYPT (2005), PKC (2005, 2007) ICALP (2006) を含む 25 件.
- 国内研究会
  SCIS (2005, 2006, 2007, 2008) を含む 51 件.

1　研究の目的

暗号解析手法の計算量理論による改良とそれに基づく暗号方式の提案を行うために，具体的な目標を以下のように三つ定める．これらは独立に存在するわけではなく，おおまかには，目標 3 が，目標 1 および 2 をふまえた最終的な目標となる．また，それぞれの目的における成果は他への研究指針となり互いに密接に関連する．

目的 1：暗号の安全性に関する精密な解析手法の開発

暗号方式に対する攻撃はある種の計算問題であるとみなすことができる．また，暗号方式のモデルはある種の計算モデルであるとみなすことができる．計算量理論は，これまで多種の計算問題に内在する計算構造を明らかにしてきているが，グラフ同型性判定問題や群に関わる様々な計算問題などに象徴される『計算構造が不明な離散的計算問題』もまた数多く存在する．暗号方式に対する攻撃についても，このような計算構造が不明な離散的計算問題であると考えられる．そこで本研究ではまず，このような計算問題に関して，それらに内在するはずの本質的な計算構造を探究する．また，その解析をもとに，それらの計算問題を様々な計算モデル上で計算する際の限界と可能性を明らかにする．この解析手法を応用し，暗号の安全性に関する精密な解析手法を開発する．

目的 2：暗号の効率に関する精密な解析手法の開発

暗号方式は安全であるだけでなく効率的に動作する必要がある．また，通常のコンピュータ上での動作だけではなく，携帯電話や IC カードなどのプロセッサの処理スピードが遅い状況やメモリが少ない状況での動作がしばしば要求される．理論的解析については，定数係数は無視してオーダーで議論するのが主流であり，様々な状況における暗号アルゴリズムの効率の詳細な解析は計算機を用いたシミュレーションを行うなど実験的な手法に頼らざるを得なかった．そこで本研究ではまず，細かな尺度で計算コストを測るための手法として，定数係数までも考慮に入れた計算量理論を開発する．この計算量理論を応用し，暗号の効率に関する精密な解析手法を開発する．

目的 3：目的 1 および 2 に基づく具体的暗号方式の提案

暗号プロトコルのうち最も基本的なものとしては公開鍵暗号がある．そこでまず，この公開鍵暗号に対する具体的方式の提案を行う．設計にあたっては目的１および２の考察をふまえて行う．すなわち，暗号の安全性および効率に関する精密な解析手法のもとで優れた暗号方式の提案を目的とする．さらには，公開鍵暗号以外の，電子署名，認証など，他の暗号プロトコルに対する具体的方式の提案も行う．

2　暗号の安全性に関する精密な解析手法に関する活動概要

暗号の安全性に関する精密な解析手法に関しては戸田が担当した。

2.1　グラフ同型性判定問題の計算量解析

本研究において，戸田はグラフ同型性判定問題の計算量に関する研究を行った。グラフ同型性判定問題は計算量の不明な離散的計算問題の代表格であり，その計算量を明らかにすることは計算量理論における主要な未解決問題とされている。戸田は，離散的な計算問題に内在する計算構造を明らかにしていくことに最も関心があり，その観点からグラフ同型性判定問題の研究を進めてきている。

本研究期間の前半は，おもにコーダルグラフに対して研究を行った。なお，コーダルグラフ（のクラス）はクリーク木による構造的特徴付けや完全消去列によるアルゴリズム的特徴付けなどを持つ数学的に見て良質のグラフクラスであるにも関わらず，それに対するグラフ同型性判定問題は GI-完全であることが古くから知られている。

本研究では，まず初めに，コーダルグラフの定義を二部グラフへと適用して得られるコーダル二部グラフと，コーダルグラフの部分クラスである強コーダルグラフに関してグラフ同型性判定問題

の計算量が明らかになっていないことに注目し，上原氏（北陸先端大）および名古屋氏（東京電機大）と共同で，これらの計算量を明らかにすべく研究を行った。その結果，両方のグラフクラスに対してもグラフ同型性判定問題が GI-完全となることを示した。

さらに，コーダルグラフが単体成分と呼ばれる連結成分（注：この連結成分はクリークになる）へと一意的に分解されることに注目し，各連結成分が十分小さいときには同型性判定問題が多項式時間で解けるのでないかと予想し，その研究を行った。その予想の背景には，コーダルグラフのクリーク木による特徴付けに基づく多項式時間アルゴリズムが従来より知られており，そこで開発されていた手法がうまく利用できるのではないかと期待したことがある。ところが，その手法を利用することはできず，最終的には群論的手法を用いた多項式時間アルゴリズムを設計することとなった。この予想に関しても一応の成果は得られたものの，当初の目標としていたグラフ論的手法に基づく多項式時間計算可能性の証明は依然として未解決のままである。

本研究期間の後半は，コーダルグラフから離れて一般のグラフに関する研究を行った。一般のグラフに対して，その固有値多重度が（頂点数や辺数に依存しない）定数であるときには同型性を判定するための多項式時間アルゴリズムが従来から知られている。ただし，そのときの時間量は固有値多重度を指数とする多項式時間となっている。そこで，指数が固有値多重度とは無関係な多項式時間のアルゴリズムを設計できるか否か，言い換えると，固有値多重度に関して parameterized tractable なアルゴリズムを設計できるか否かといった問題に取り組んだ。研究を進めていく調査の過程で，この問題に対してすでに肯定的な解答が示されていたことを知ったのだが，そこでは celluler algebra や置換群の表現論などを用いていたので，より単純な組み合わせ的なアルゴリズムが設計できるか否かを考察することにした。その考察の過程で，元々の問題が行列集合の自己同型群（の生成集合）を求める問題に帰着できることを発見し，考察の対象を行列集合の自己同型群へと移行した。ここで，行列集合とは，行数が元々のグラフの固有値多重度以下であり，列数が元々のグラフの頂点数と一致するような複数の行列からなる集合のことである。また，各行列は元々のグラフの固有空間に対応する。より正確に言うならば，元々のグラフの頂点を基底ベクトルとするベクトル空間から固有空間への（適当な基底のもとでの）線形写像を表現している。その行列集合の自己同型群は，各行列の行への作用がその行列に対応する固有空間上の直交群となり，列への作用が頂点集合上の置換群となっており，その置換群が元々のグラフの自己同型群になっているといった構造を持っている。行への作用が直交群となっていることからその作用を直接計算することは困難と思われたので，列への作用に注目して研究を進めたのだが，残念ながら現在に至るまで解決に至っていない。ただし，行への作用も置換群となっている場合には単純な動的計画アルゴリズムが設計できることを見いだし，さらにそれが小さな辺集合から構成されるハイパーグラフの自己同型群を求める問題と論理的に等価でもあることから，それらの結果をまとめて研究報告を行った。

さらに，名古屋氏（東京電機大）が非自明な自己同型写像の部分情報から非自明な自己同型写像全体を求める問題を考察し，その問題に対して一定の成果を示していることを知って，戸田からその結果をさらに強めることができるのではないかと提案して共同研究を進めることにした。名古屋氏による従来の結果では，非自明な自己同型写像によって相互に移される頂点対が与えられたときに非自明な自己同型写像を多項式時間内に計算できるというものであったが，共同研究を進めた結果，頂点対である必要はなく，非自明な自己同型写像に移される頂点（注：ここで，相手の頂点は不明である）が与えられるだけでも同様の結果を導けることが明らかとなった。

3 暗号の効率に関する精密な解析手法に関する活動概要

暗号の効率に関する精密な解析手法に関しては渡辺と河内が担当した。渡辺の行った研究は大きく以下の４つに分けられる．

1. NP-困難な問題に対するヒューリスティックスの理論的な解析

2. NP-困難な問題に対する低指数関数計算量アルゴリズムの開発

3. NP-困難な問題の構造的な計算量解析

4. 学習アルゴリズムに関する研究

河内の行った研究は大きく以下の２つに分けられる．

1. 量子質問計算量の上下界の解析

2. 量子計算量理論に基づく暗号系設計

3.1 NP-困難な問題に対するヒューリスティックスの理論的な解析

NP-困難が示されている問題の中にも平均的にはうまく働く（と主張されている）「ヒューリスティックス」が数多く提案されている．こうしたヒューリスティックスに対する理論的な解析を与え，それに基づいた新たな，よりよいヒューリスティックス（もしくはアルゴリズム）を提案する研究を行なった．以下では，いくつかのサブテーマに分けてその研究成果を説明する．(以下では，時間的な経緯に従ってではなく，内容的な順序関係に基づき説明する．)

平均を議論する枠組みに関する研究

提案されている「ヒューリスティックス」は，すべての入力例で正しく働く，あるいは効率的に働くわけではない.「平均的に」うまく働くものである．その「平均」を議論するためには，入力例の分布を考えなければならない．その分布の与え方に関する研究を行なった．

その初期の研究では，たとえば MAX-2SAT 問題という問題を選び，その難しさの平均的な解析をする際の入力例の分布に対する確率モデルを提案した．MAX-2SAT 問題のような最適化問題に対しては，これまで，そのような確率モデルとして妥当なものがなかったが，山本と共同で，MAX-2SAT 問題に対して，テスト例題生成，という観点から入力例生成の手法を提案した．さらに，それを単純化して，MAX-2SAT 問題の入力例に対する自然な確率分布を提案することができた。

渡辺は，その中で得られた考え方，ならびに，最近，いろいろな問題の平均的な解析に用いられはじめている planted solution model という分布の背後にある考え方を分析した．その結果，一般的で，かつ，その分布の妥当性がわかりやすい「平均的解析」の枠組みにまとめることができ，それを Most Likely Solution 発見問題として提唱した．

局所探索アルゴリズムの平均的振る舞いを解析する手法の開発

局所探索アルゴリズムは，多くの「ヒューリスティックス」の基本となるアルゴリズムである．これは構造が簡単だが，平均的に非常によい効率を出す場合があることが知られている．

渡辺を中心に，こうした局所探索アルゴリズムの平均的な効率を解析する研究が行なってきた．まず，その解析手法の核の 1 つである「疑似平均」の近似度についての解析を行なった．その結果，単純なマルコフ過程においては，平均状態を解析する手法として，この疑似平均が有効であることを厳密に証明することができた。

さらに，その解析手法を活かして，二種類の充足可能問題（パリティ SAT 問題と 3-SAT 問題）における局所探索法を解析した．その結果，(i) 局所探索法が成功する場合の理由を準理論的に示すことができた．さらに，(ii) SAT 問題群の中でも，局所探索法に対する相性に差があること，(iii) タブー探索の効果，なども明らかにすることができた。

確率伝播法の理論的な解析

Perl により提案された確率伝播法 belief propagation は，確率構造を表わすグラフに閉路がないときには正しく動くことが示されているが，一般には，正しく動かない場合がある．しかし，この確率伝播法を，いくつかの NP-困難な問題に適用させると，確率構造のグラフに多数の閉路があるにもかかわらず，平均的に非常によく働くことが発見され，最近，注目を集めている．渡辺は Onsjo と，グラフの等分割問題 Graph Bisection Problem を対象とし，この確率伝播法により構成

されたアルゴリズムの平均的な性能を解析する研究を行ない，まず，限定された状況における結果を得た。さらに最近，山本と共同で，確率伝播法と，すでによく知られている固有値分解法との関係を示すことができ，この種の確率伝播法にはじめて理論的な正当性を与えることに成功した。

3.2 NP-困難な問題に対する低指数関数計算量アルゴリズムの開発

NP-困難な問題のほとんどに対しては，問題のサイズ n に関して指数関数の計算量を持つアルゴリズムしか知られていない．しかし，同じ指数関数でも，たとえば，$O(2^n)$ の場合と，$O(1.2^n)$ の場合では，実際の計算時間では大きな差が出てくる．そこで，この指数関数（より具体的には指数の底）を改善するアルゴリズムの研究が盛んになりつつある．これを「低指数関数計算量アルゴリズムの開発」と呼ぶことにする．

本計画研究の一部において，この低指数関数計算量アルゴリズムの開発を，おもに充足可能性問題 SAT 問題に対して行なった．充足可能性問題の中でも最も標準的な 3-SAT 問題を対象にした研究は，すでに多くの研究がなされている．とくに，最近では，計算過程で乱数を用いる乱択型のアルゴリズムを Schoning が提案して依頼，その開発競争が進んでいる．本研究でも，Schoning らとともに，さらに効率のよい最悪時計算時間 $O(1.330^n)$ の乱択アルゴリズムを提案し，その当時の世界記録となった。なお，現在は，岩間（本特定研究代表）らのグループのアルゴリズムが最速の計算量 $O(1.324^n)$ になっている．

また，一般の CNF-SAT 問題では，山本（渡辺が指導する博士課程の学生）が，従来の効率を改善する決定性のアルゴリズム（現在でも最速）を提案することができた．この SAT 問題に対するアルゴリズムの応用として，渡辺が中心となって，他の組み合わせ問題のアルゴリズムの改良を試み，独立点集合の一般化である Domatic Number Problem に対して，従来のアルゴリズムの効率解析の改善を示すことができた。

なお，この分野の活性化のため，渡辺は Rolf Niedermeier とともに，Improving Exponential-Time Algorithms (iETA) というワークショップを，本特定研究の事業の一つとして企画し，ヨーロッパ理論計算機学会 European Assoc. Theoret. Comput. Sci. の年次総会 ICALP'06 のときに開催した．このワークショップは，関連分野の多くの研究者に交流の場を与え，その後の研究の発展に貢献している．

3.3 NP-困難な問題の構造的な計算量解析

NP-困難な問題の難しさを（アルゴリズム的な方法でなく）示す手法についての研究も行なった．まず，相対化の枠組みに関する研究である．相対化とは，たとえば，計算量クラス P と NP の差を議論することの難しさを示すための手法として，1970 年代に導入され，盛んに研究された手法である．渡辺は Cai とともに，この相対化計算の枠組について再考する研究を行い，これまでの相対化の議論には妥当でない比較が含まれていることを指摘し，新たな妥当な相対化の枠組み stringent relativization を提案した．

具体的には，たとえば P = NP のような等号関係をシミュレーションにより示す際に，これまでの相対化の議論では，シミュレーションする側が，シミュレーションされる側より，より多くのオラクル情報を利用できることを用いてシミュレーションを行なっていた．これでは妥当な比較ができない，と考えたのである．

そこで，妥当な比較をするための制限を導入し，新しい相対化比較の枠組を提案した．当初の枠組みには，一般性に欠ける不備があったが（注：論文で述べられている結果自体は正しい），それを修正し，健全な枠組みを再提案するとともに，最終的には P と NP の関係をもその枠組みの中で相対化できることを示した。この枠組みは，新たなアプローチとして注目され，この分野の研究者の重要な情報交換誌である ACM SIGACT News へも招待され寄稿した。

この他に，従来からあまり例がないと言われていたクラス Σ_2^{P} に対する自然な完全問題としてトーナメントグラフにおける king 同定問題が，Σ_2^{P}-完全であることをしめした。

3.4　学習アルゴリズムに関する研究

学習アルゴリズムの重要な設計法に「ブースティング技法」がある．渡辺は，以前よりこのブースティング技法の研究を行ない，様々な改良やその応用を提案してきた．本計画研究においても，乱択アルゴリズムの研究の一貫として，誤り度が偏る場合にそれを生かしたブースティングを行なう技法を畑埜と提案した。こららの結果を総合して，ブースティング技法の背景にあるＰＡＣ学習の話から始め，ブースティングによる学習アルゴリズムの基礎を解説した本を出版した。

3.5　量子質問計算量の上下界の解析

量子アルゴリズムの分野において質問計算量は著名な 1996 年の Grover のアルゴリズムの提案以来，その分野の中心的な研究課題として数多くの研究者により研究が進められてきた．与えられた未知の関数（オラクル）を関数値の評価（オラクルへの質問）を通じて同定する，という問題（オラクル同定問題）は非常に一般的であり，暗号理論のみならず，計算量理論，機械学習理論に幅広い応用を持つ．例えば暗号理論における安全性証明ではオラクルへの質問回数がそのまま安全性の高さと直結している．このオラクル同定問題に対して量子計算的な質問計算量について研究を行った．オラクル同定問題とは M 個のブール関数集合 $\{f_i : \{0,\ldots,N-1\} \to \{0,1\}(i = 0,\ldots,M-1)\}$ に属するある関数が与えられたときに，その関数の値を何回質問することで同定できるか，という問題である．この問題は量子計算で頻繁に扱われる探索問題の一般化として [リスト中 STACS 2004 の論文] によって初めて定式化され，$M \leq N$ の場合の量子アルゴリズム（質問計算量の上界）とそれがほぼ最適である証明（質問計算量の下界）が与えられた．さらに論文 [リスト中 TCS 2007] ではより一般的でかつ誤りに対して頑健なアルゴリズムが提案され，更に広範囲の M に対しても最適性の証明が与えられた．またオラクル同定問題に関連して，同定する対象が関数ではなく量子状態である問題に関してもサンプル計算量（同定に必要な状態のサンプル数）についてもこの研究で考察を行った．特に [リスト中 QIC Journal の論文] では隠れ部分群問題と呼ばれる問題を解くためのサンプル計算量の上下界を求める手法を与えている．隠れ部分群問題は素因数分解問題や離散対数問題をはじめ，整数格子問題，グラフ同型問題など，暗号理論でしばしば利用される問題との関連性が数多く指摘されており，暗号理論的な観点からも高い重要性を持っている．

3.6　量子計算量理論に基づく暗号系設計

従来，量子情報を利用した暗号系として著名なのは 1984 年に Bennett と Brassard によって提案された量子鍵配送プロトコルである．このプロトコルの特徴として，計算量理論的な仮定を置かずに情報理論的に安全性が評価できるという点である．古典情報に基づいた現代暗号のほとんどのプロトコルが一方向性関数の存在性などの計算量理論的仮定に依存しているのに対して，この結果は量子情報の重要性に注目を大きく集める一因となった．しかしその一方で情報理論的な量子ビットコミットメントプロトコルは不可能であることが Mayers や Lo と Chau によって指摘されており，達成すべき目的によっては必ずしも情報理論的安全性が保証できないことも知られている．また公開鍵暗号系においては現在の主要なプロトコルは Shor のアルゴリズムを用いることで容易に解読できることも知られているため，量子情報を操ることのできる敵対者を考える上で，妥当な計算量理論的仮定の下で安全性を議論することも重要であると言える．本研究では，特に (1) 量子一方向性置換の検査法，(2) 量子情報を利用した公開鍵暗号系，(3) 量子リスト復号を利用したハードコア関数の構成について考察を行った．以下，それぞれについて順に説明を行う．

量子一方向性置換の検査法

計算論的な暗号では通常，最も基本的な基本的構成要素として一方向性関数の存在性が仮定される．一方向性関数 f とは入力 x が与えられたときに $f(x)$ は容易に計算できるが，その逆計算は困難であるような関数である．一方向性関数の存在性は非常に重要かつ解決困難な未解決問題であるが，暗号理論研究者からはその存在性仮定は強く支持されている．特にその逆計算の計算困難性

が量子アルゴリズムに対しても成立する場合，その関数は量子一方向性関数と呼ばれる．またその特殊な場合として関数が置換になっているのが量子一方向性置換である．例えば現代暗号における RSA 暗号の暗号化関数や離散対数問題は古典的には一方向性置換であると多くの研究者が考えられているが，量子一方向性置換ではないことが既に Shor により証明されている．実際，現在のところ古典の場合と異なり，良い量子一方向性置換の候補は知られていない．その一方で，量子一方向性置換は Dumais らの非対話型量子ビットコミットメントや Watrous の耐量子攻撃性を持つゼロ知識証明系の構成に利用されており，その候補を見つけるのは重要な研究課題である．[リスト中 TCS 2005 の論文] では，その候補を探し出すための量子一方向性関数の特徴づけを行った．当該論文では与えられた関数が量子一方向性置換のための必要十分条件を与え，それを利用した量子一方向性置換の検査法を提案している．

量子情報を利用した公開鍵暗号系

前述のように，RSA 暗号などの現在利用されている主要な暗号系は量子アルゴリズムによって安全性を保証ができなくなってしまっており，耐量子攻撃性を持つ公開鍵暗号系の構成は重要な研究課題である．[リスト中 Eurocrypt 2005 の論文] ではそのような暗号系設計のための基本構成要素としてある特殊な量子状態の識別問題を提案し，その暗号理論的性質を明らかにした．更にこの基本構成要素を元に量子アルゴリズムに対しても難しいと考えられている問題の計算困難性に安全性帰着可能な量子公開鍵暗号系の構成を行った．具体的にはその特殊な量子状態識別問題が (i) 落とし戸情報を持つ，(ii) 平均時の困難性が最悪時の困難性と等価である，(iii) 最悪時の困難性が少なくともグラフ自己同型性判定問題の最悪時困難性と同等かそれ以上である，という三つの暗号論的性質を満たすことを証明した．この問題を公開鍵暗号系に利用することを考えた場合，敵対者には暗号文が区別できないが，落とし戸情報を持つ受信者には暗号文を正しく解読できるという性質が必要となる．性質 (i) はこの機能を提供するものである．また，ある計算困難な問題を暗号に利用した場合，実際にはランダムに問題生成を行うため、その問題の最悪時困難性が保証されているだけでは不十分である．性質 (ii) はこの識別問題の平均時困難性が最悪時困難性によって保証されることを示している．さらにその最悪時困難性は性質 (iii) により保証されている．なお，このグラフ自己同型性判定問題は量子計算機を用いても効率良く解けるかどうか判明しておらず，少なくとも現在のいくつかの量子計算機上のアルゴリズムの設計手法では解けないという否定的な結果もいくつか知られている．この三つの性質を利用することで量子公開鍵暗号系を構成することが可能となった．この公開鍵暗号系における暗号の解読は少なくともグラフ自己同型性判定問題を解くことと同等かそれ以上に難しいことが証明可能であるため，現在知られている量子計算機上のアルゴリズムでは解読困難であるといえる．

量子リスト復号を利用したハードコア関数の構成

計算量理論に基づいた量子暗号系の安全性証明の新たなテクニックとして，誤り訂正符号に対する量子リスト復号法を導入し，ハードコア関数の新たな一般的構成方法を与えた．更に今回の結果を応用することで 1988 年に提案されて以来，未解決であった Dangaard の擬似乱数生成器の安全性を量子一方向性関数に基づいて証明することができた．リスト復号法とは，与えられた符号語に誤りが多すぎて一意的に元々の符号化された情報が復元できないような状況でも符号化された情報の候補を比較的短いリストとして与えてくれるような復号法である．元来，リスト復号法は符号理論で考案された概念であったが，近年，リスト復号法が現代暗号理論や計算量理論で応用できることが判明し，急速に研究が進んでいる．またハードコア関数は一方向性関数に対して定義される暗号理論における非常に基本的な道具であり，例えばハードコア関数を利用して擬似乱数生成器やビットコミットメントプロトコルが構成できることが知られている．今回の結果はリスト復号法の量子計算版の有用性を示しており，元々のリスト復号法と同様に量子リスト復号法も量子計算における暗号理論や量子計算量理論において今後幅広い応用を持つことが期待できる．

4 目的１および２に基づく具体的暗号方式に関する活動概要

目的１および２に基づく具体的暗号方式に関しては主に田中が担当した。具体的暗号方式に関して以下のような様々な考察および提案を行った.

4.1 匿名性をもつ暗号プロトコル

sampling twice テクニックと匿名性をもつ暗号プロトコル 公開鍵秘匿通信において，暗号文をみただけではその受信者が特定できないとき，もしくは，署名において，署名を生成した人が特定できないとき，その公開鍵秘匿通信方式，もしくは署名方式は，匿名性をみたすという．匿名性を達成するような方式を構成するためには，暗号文，または署名の値域を各ユーザーで共通にすることが必要である．本論文では，匿名性を達成するためのテクニックに着目し，RSA ベースの公開鍵秘匿通信，もしくは署名において有効な sampling twice と呼ばれる新たなテクニックを提案した．このテクニックは，$|N| = k$ をみたす任意の N について，$[0, N)$ 上の一様分布を $[0, 2^k)$ 上の一様分布に変換するものである．さらに，sampling twice テクニックを利用して，公開鍵秘匿通信，否認不可署名，指定検証者署名，リング署名を構成した．これらは匿名性を達成しており，さらに暗号文や署名のサイズ，復号や検証のコストに関して効率のよい方式となっている.

ElGamal 暗号と Cramer-Shoup 暗号をもとにした匿名性を持つ暗号方式 ElGamal 暗号と Cramer-Shoup 暗号をもとにした匿名性を持つ暗号方式を提案した。以前の方式は，ユーザー全員が共通の群を利用しなければ匿名性を達成することができなかった．我々の方式は，それよりも弱い制約の下で，匿名性を達成できる方式である．具体的には，各ユーザーは safe prime を選び，その素数の上での平方剰余群を利用している．ElGamal 暗号をベースにした方式は，選択平文攻撃に対する匿名性と判別不可能性を達成し，Cramer-Shoup 暗号は適応的選択暗号文攻撃に対する匿名性と判別不可能性を達成している.

データに関するプライバシーと鍵に関するプライバシーの関係 公開鍵暗号方式に要求される一般的な安全性は，暗号化されたデータに関するプライバシーを問題としている．データに関するプライバシーの定式化には，一方向性 (OW) や識別不可能性 (IND) などがある．一方向性は，暗号文から平文が復元できないという性質を定式化しており，識別不可能性は，暗号文から平文に関する情報が漏れないという性質を定式化したものである.

一方，Bellare, Boldyreva, Desai, Pointcheval は，新しい安全性の指標として，鍵に関するプライバシーを提案した．これは，暗号化に用いられた鍵に関するプライバシーを問題としている．すなわち，暗号文がどの鍵で暗号化されたかがわからないという性質である．この性質をもつ暗号方式を使うと，攻撃者には暗号文の受信者（最終的に復号する人）が誰だかわからないため，暗号文の受信者に関する匿名性がみたされると見なすことができる．彼らはこの性質を匿名性 (IK, 鍵の識別不可能性) として定式化した.

この安全性指標に関連して，Halevi はシンプルな十分条件 (IKR と呼ぶ) を与え，IND かつ IKR を満たせば IK を満たすことを示した．Hayashi, Tanaka は，Bellare, Boldyreva, Desai, Pointcheval の提案した定義を変形して，強匿名性と呼ばれる匿名性の新しい定義 (sIK と呼ぶ) を提案した.

我々は，以上の結果をふまえて，データに関するプライバシー (IND, OW) と鍵に関するプライバシー (IK, IKR, sIK) の関係を示した.

例えば，IK をみたしても，必ずしも OW をみたすとは限らないが，sIK は OW だけでなく IND もみたすことを示した．さらに，sIK は “IND かつ IKR” であること，IK は “IND かつ IKR” より弱いことも示した．これにより，sIK と “IND かつ IKR” は等価であることがわかった.

適応的選択暗号文攻撃に対する匿名性を得るための一般的な変換 Bellare らによる匿名性の定義は，選択平文攻撃と適応的選択暗号文攻撃の二つの攻撃のもとで定式化されている．この二つの安全性をそれぞれ IK-CPA と IK-CCA と呼ぶ.

我々は，2 つの鍵のもとでの plaintext aware-

ness の概念を提案した．これを PA2 と呼ぶ．公開鍵暗号方式が PA2 の意味で安全であるとは，その方式が IK-CPA をみたし，かつ PA2 のための knowledge extractor が存在するときをいう．PA のための knowledge extractor と，PA2 のための knowledge extractor は相違点がある．

次に，公開鍵暗号方式が PA2 の意味で安全であるならば，IK-CCA の意味でも安全であることを示した．これは，公開鍵暗号方式が PA2 の意味で安全であることを示すことは，IK-CCA の意味で安全であることを示すことと比較して容易であると考えられるため，PA2 は公開鍵暗号方式に関する匿名性の性質として有用なものである．

さらに，匿名性を得るための一般的な変換方式を初めて提案した．具体的には，Fujisaki-Okamoto 変換方式によって，IK-CPA の意味で安全な基本的な暗号方式が，ランダムオラクルモデルにおいて IK-CCA の意味で安全な方式に変換されることを示した．

一般的匿名化可能な公開鍵暗号方式　我々は，一般的匿名化可能な公開鍵暗号方式の概念をはじめて提案した．同じセキュリティーパラメーターでつくられた暗号化データがあり，そのデータは匿名性の性質を満たすとする．ここでは，これらの暗号化データを復号することなしに匿名性をもつ暗号化データに変換したい状況を考える．

この状況を形式化するために，一般的匿名化可能と呼ばれる，公開鍵暗号のための新しい概念を提案した．この一般的匿名化可能な公開鍵暗号方式を用いることにより，暗号文を作成した人だけでなく，暗号化に用いられた秘密鍵を知らなくても暗号化データを匿名化できるようになる．

さらに，ElGamal 暗号方式，Cramer-Shoup 暗号方式，RSA-OAEP 方式を基にした一般的匿名化可能な公開鍵暗号方式を提案し，その安全性を示した．

4.2　特殊な機能をもつ暗号プロトコル

- バッチ検証機能付きの Signcryption に関する研究を行った．Signcryption とは，暗号化と署名を同時に 1 つのステップで行う方式であり，暗号化と署名を別々に行うよりも効率がよいという性質を持っている．Signcryption は，鍵生成アルゴリズム，暗号化と署名を同時に行う sincrypt アルゴリズム，復号と検証を同時に行う designcrypt アルゴリズムの 3 つから構成される．我々は，バッチ検証つきの Signcryption のモデルを提案する．このモデルでは，designcrypt アルゴリズムにおいてバッチ検証を行うことができる．バッチ検証を行うと，Signcrypt アルゴリズムにより変換されたメッセージ (signcrypted message) の検証を一括して行うことができるため，検証に必要なコストをおさえることができる．安全性としては，signcrypted message の平文に関する情報が漏れないこと，signcrypted message の偽造ができないこと，署名者と検証者に関する匿名性の 3 つを定式化した．さらに，我々はこのモデルのもとで具体的な方式を提案した．我々の方式は，効率の良いバッチ検証を行うことが可能で，さらに定式化した 3 つの安全性をみたしている．

- リング署名を拡張し，指定検証者リング署名の概念の提案を行った．リング署名において，その検証が誰にでも可能なため生じる「署名の一人歩き問題」があるが，我々の提案する新しいリング署名方式によってこの問題を解決することができる．指定検証者リング署名は，通常のリング署名としても使うことができるだけでなく，リング署名を持っている人なら署名者に限らず誰でも，それを特定の人にしか検証できないものに変換できる機能を持つ．この機能により，指名者が意図する人にのみ署名を検証させることが可能となる．さらに，我々は指定検証者リング署名の具体的な方式も提案した．

- 墨塗り署名に関する研究を行った．墨塗り署名とは，墨塗り者と呼ばれる第三者が，署名者から文書とその文書に対する署名を受け取ったとき，文書の一部を墨塗りし，さらにそれに対する署名を生成できる署名方式である．このとき，墨塗りされた部分からは，墨を塗られる前の文書に関する情報は得られない．墨塗り署名は，個人情報のように開示すべきでない情報を除いた部分開示を行う場合

などに利用される．我々は，秘密情報を用いた墨塗り署名に注目し，そのモデルと安全性を定式化した．また，そのモデルのもとで安全な墨塗り署名方式を提案した．この方式は gap co-Diffie-Hellman group の存在を仮定することで安全性が証明されている．さらに，これまでに提案されている多くの方式と我々の方式について比較，整理を行った．

- 3 人モデルにおける，効率の良いパスワード認証付き鍵交換プロトコルを提案した．Abdalla，Fouque，Pointcheval は，3 人モデルにおけるパスワード認証付き鍵交換プロトコルの一般的な構成方法を提案した．彼らのプロトコルは自然で有用であるが，安全性を示すには多くの仮定が必要である．具体的には，2 人モデルのパスワード認証付き鍵交換プロトコル，3 人モデルの鍵配布，MAC の存在と，desional Diffie-Hellman problem の困難性を仮定する必要がある．さらに，このプロトコルは多くのラウンド数を必要とする．我々は，一般的な構成方法ではないものの，少ない仮定のもとで安全な 3 人モデルにおけるパスワード認証付き鍵交換プロトコルを提案した．我々のプロトコルは，desional Diffie-Hellman problem の困難性のみを仮定すれば，ランダムオラクルモデルのもとで安全である．さらに，我々のプロトコルは 4 ラウンドで終了するため，非常に効率がよいものとなっている．

- Computational Bilinear Diffie-Hellman 問題に基づく複数キーワード検索つき公開鍵暗号方式を提案した．Park，Kim，Lee は複数キーワード検索つき公開鍵暗号方式 (PECK) を提案した．彼らは具体的な方式を 2 つ提案しており，それらは Decisional Bilinear Diffie-Hellman problem の困難性に基づいて安全性が証明されている．我々は彼らの方式を拡張した新たな方式を提案した．この方式は Park らの仮定よりも弱い仮定である Computational Bilinear Diffie-Hellman problem の困難性を仮定することで安全性を証明することができる方式である．

- Cramer-Shoup の構成法による平方剰余問題と関連する暗号方式を提案した．Eurocrypt '02 において Cramer と Shoup は適応的選択暗号文攻撃に対して安全な公開鍵暗号の一般的構成法を提案した．我々はこの構成法を用いて新たに具体的に適応的選択暗号文攻撃に対し安全な公開鍵暗号を提案した．彼らは安全性が平方剰余判定問題に依存する公開鍵暗号を具体的に提案していたが，この暗号は離散対数問題，n 次剰余判定問題に安全性が基づく暗号よりも効率が悪かった．我々は平方剰余判定問題と関係を持つ問題を提案し，その問題に安全性が基づく公開鍵暗号を提案した．この暗号は Cramer と Shoup が提案した平方剰余判定問題に基づく暗号よりも効率的である．

- 指定検証者署名への変換が可能な Aggregate Signature　も提案した．二人以上の署名を一つにまとめる aggregate signature と呼ばれる署名がある．本論文では，署名の所有者に，任意の指定された検証者への署名を指定させる機能を追加した aggregate signature を提案した．この機能により，指定された検証者以外は署名を検証できないので，他の人の手に渡った署名は，誰もが検証できる形で送信することができない．

- Groth，古川によるプロトコルのような，honest verifier ゼロ知識証明であるシャッフルに対する証明方式を提案した．古川，佐古，Groth や古川によって提案された以前の方式とは異なり，我々の方式は，メッセージの部分に加法準同型性を持つ Paillier の暗号系によって暗号化された要素のシャッフルとして使う事ができる．以前の方式で使われた ElGamal 暗号方式はこの性質は持っていない．

4.3　組み合わせ問題を基礎とした暗号方式

組み合わせ問題を基礎とした暗号方式に関して，次のような研究を行った．

まず，ナップザック問題に基づいた量子計算署名に関する研究を行った．これまでに，いくつかのナップザック問題ベースの公開鍵暗号方式が提案されている．しかしながら，ナップザック問題

ベースの署名方式はほとんど提案されていない．Shamir の署名方式は線形変換に基づいているが，量子計算機を使うことなくその安全性が破られている．岡本，田中，内山は，量子計算署名の定義を提案した．そして，早稲田，双紙，宮地は，岡本らの定義に基づいたナップザック問題ベースの量子計算署名を提案した．彼らの方式は，符号付きナップザック問題に基づいている．我々は，早稲田，双紙，宮地による方式の詳細な解析を行った．その結果，攻撃者が署名者の秘密鍵を手に入れることができることがわかり，早稲田らの方式は安全ではないことがわかった．さらに我々は，この解析をふまえた上で，ナップザック問題に基づいた量子計算署名を構成することの可能性について議論した．

次に，格子暗号の複数ビット化に関する研究を行った．現在，安全性証明がある格子暗号は1ビット暗号しか知られていない．一方，現在までに知られている効率の良い格子暗号は安全性の証明がない. そこで我々は，よく知られている 4 つの 1 ビット格子暗号 (Ajtai-Dwork 暗号，Regev03 暗号，Regev05 暗号，Ajtai 暗号) を対象に，共通の手法を導入し，公開鍵・秘密鍵・暗号文空間のサイズを変えることなく平文空間を複数ビット化した. 具体的には，セキュリティパラメータを n とした際に，平文のビット数を $O(\log n)$ とすることができる. また，複数ビット化した格子暗号も，元の 1 ビット格子暗号と同様に安全性を証明することができる．その際，格子暗号中で使われているガウス分布と安全性の基となる格子問題の解析を行い，平文のビット数・復号エラーの確率と安全性の基となる格子問題の間にトレードオフがあることが分かった．また，我々は “擬似準同型性” という概念を導入した．通常の暗号の準同型性は，2 つの暗号文の和または積が暗号文になるという性質である．一方，擬似準同型性は，2 つの暗号文の和が暗号文にはなるとは限らないが，無視できる確率を除いて正しく復号できるという性質である．複数ビット化した格子暗号は，ガウス分布の再生性により擬似準同型性を持つ．ただし，復号エラーを抑えるために，和の回数はある程度制限される．さらに，先と同様の手法により，その方式の安全性も証明した.

4.4 暗号プロトコルのモデルと方式に関する研究

- 認証付き鍵交換プロトコルにおける non-malleability に基づく安全性について考察した．ここでは，パスワードに基づいた認証付き鍵交換 (AKE) プロトコルを扱った．2000 年に Bellare，Pointcheval，Rogaway によって AKE の厳密なモデルが提案された．我々は，セッションキーの non-malleability 性に基づいた AKE の新しい安全性を定義し，次にこの安全性が Bellare，Poincheval，Rogaway によって提案されたものと等価であることを示した．さらに，この新しい安全性を用いて，ランダムオラクルモデルでは安全であるが，衝突困難性に基づくハッシュ関数を用いたモデルでは安全でなくなるプロトコルがあることを示した.

- ランダムオラクルモデルを用いたプロトコルの指標と方式について考察した．ランダムオラクルモデルの研究では，ランダムオラクルをつかった方式と，ランダムオラクルの部分を，ある関数の集合からランダムに選んだ関数に置き換えた方式との gap に関する研究が注目されている．我々はランダムオラクルモデルにおける方式の研究の異なる方向性を考える．我々は，ランダムオラクルに対する全ての質問と答えを表現するのに必要な表のサイズに注目し，ランダムオラクルモデルでの公開鍵秘匿通信方式や署名方式における表のサイズの減らし方を示した．さらに，この考えを PSS-R と OAEP に応用した方式を提案し，その安全性を証明した.

- 中程度の難しさをもつ関数のモデルと方式について考察した．moderately-hard function は様々なアプリケーションを持ち，関連する論文も数多く発表されている．しかしながら，moderately-hard function の厳密なモデルは提案されていなかった．本論文では，まず moderately-hard function の厳密なモデルを提案する．ここでは，計算モデルを構成し，moderately-hard function に必要とされる性質を調査した．さらに，moderately-hard function として利用できるいくつかの関数を

提案した．この関数は，$p^r q$ の素因数分解の困難性と primitive function の連続計算という二つのアイデアに基づいている．

- 多対 1 モデルでの公平な署名交換に関する研究を行った．2004 年，Chen，Kudla，Paterson は，concurrent signature の概念を提案した．この署名を用いると，利用する状況はある程度制限されるものの，信用できる第 3 者を仮定したり，多くの通信を必要とすることなく，公平に署名を交換することができる．彼らのモデルでは 1 対 1 での公平な署名交換を扱っていたが，我々は多対 1 での公平な署名交換を考える．我々は多対 1 モデルにおける concurrent signature のモデルと安全性を定式化するとともに，具体的な方式を提案した．我々の方式は，離散対数問題の困難性を仮定すると，honest-but-curious セッティングかつ random permutation model のもとで安全である．

- secret handshake と呼ばれる認証プロトコルに関する研究も行った．近年，Balfanz, Durfee, Shankar, Smetters, Staddon, Wong は，プライバシーを考慮した相互認証のひとつである secret handshake のモデルを提案した．secret handshake を用いると，認証を行う 2 人が同じグループのメンバーならば，お互いが同じグループに所属しているということを納得できる．一方で，違うグループに属している場合は，自分が所属しているグループの情報を相手に漏らすことはない．このモデルにおける具体的な方式は，Xu，Young により初めて提案されている．Balfanz らのモデルでは，認証の際に対象とするグループはひとつだけであった．我々は，複数グループにおける secret handshake のモデルと，具体的な方式を提案した．このモデルでは，メンバーがあるグループに加入したり，グループから離脱しても，それ以外のグループの所属情報を変更したり，再構築する必要がない．

4.5 公開鍵暗号における乱数漏洩を考慮した安全性

公開鍵暗号の分野では，さまざまな安全性が定式化されている．標準的なものとしては，暗号文から平文を完全に復元することができないという安全性（一方向性），2 つの平文とそのいずれかの暗号文をうけとり，その暗号文がどちらの平文から作られたのかを判別することができないという安全性（判別不可能性）などがある．

これらの安全性を考える際，乱数は正しく選ばれ（すなわち，乱数空間から一様かつランダムに選ばれ），その情報は攻撃者に（明示的に）渡されることはない．しかしながら，公開鍵暗号を使用している状況によっては，乱数に関する情報が攻撃者に漏れてしまうといった状況も想定できる．例えば，暗号化に使用された乱数が，安全でない記憶領域に残っており，そこに攻撃者がアクセスすることで乱数情報を得られるかもしれない．または，使用している疑似乱数生成器がうまく動作せず，生成される乱数に偏りが生じたり，ランダムな出力をしないかもしれない．

このような乱数情報が漏れた場合の安全性についてはしばしば議論が行われてきたが，その安全性の定式化は行われていなかった．そのため，乱数情報が漏れた状況で，公開鍵暗号の安全性がどの程度低下するのか，あるいは，乱数情報が漏れたとしても，ある程度の安全性は保たれているのか，といった詳細な議論は，これまで行われてこなかった．

このような状況をふまえ，我々はまず，公開鍵暗号における乱数漏洩を考慮した安全性の定式化を行った．今回は，最もシンプルな安全性の定式化として，攻撃者に暗号化に使用した乱数そのものを与えるという定式化を行った．安全性のゴールとしては，上述の一方向性や判別不可能性などが考えられるが，乱数を攻撃者に与えた場合，攻撃者は必ず判別不可能性を破ることができてしまうことがわかった．そこで今回は，攻撃者に乱数情報を与えた場合の一方向性を定式化した．

定式化した安全性について，もう少し詳しく説明する．まず，鍵生成アルゴリズムによって公開鍵と秘密鍵のペア (pk, sk) が生成される．次に，平文 m と乱数 r がそれぞれランダムに選ばれ，これを用いて暗号文 $c = E_{pk}(m; r)$ が生成される．

攻撃者は，公開鍵 pk，暗号文 c に加えて，乱数 r を受け取り，出力 m' を返す．$m' = m$ ならば攻撃者の勝ちである．攻撃者がこのゲームにほとんど勝つことができないとき，その暗号方式は乱数漏洩を考慮した場合の一方向性 (one-wayness with the randomness revealed, OWR) をみたすと定義する．

さらに，定式化は OWR-CPA，OWR-PCA，OWR-CCA の 3 種類が存在し，それぞれは攻撃者がアクセスできるオラクルによって違いがある．まず，OWR-CPA は 攻撃者に与えられるオラクルは存在しない．つまり，上で説明したようなゲームで攻撃者が勝てないとき，その暗号方式は OWR-CPA をみたすと定義する．OWR-PCA は，攻撃者にチェックオラクルというものが与えられ，攻撃者は上で説明したゲーム中にそれを使うことができる．チェックオラクルとは，平文と暗号文のペアをオラクルに質問すると，それが正しいペア（つまり，暗号文を復号すると，その平文になる）であるか，そうでないかを答えてくれるオラクルである．最後に，OWR-CCA は，攻撃者に復号オラクルが与えられる．すなわち，攻撃者は好きな暗号文を復号してもらうことができる（ただし，チャレンジする暗号文 c だけは質問できない.）．攻撃者にとって有利なほど，安全性としては強力になるので，OWR-CPA が最も弱い安全性，OWR-CCA が最も強い安全性ということになる．

これらの定式化のもとで，我々は既存の方式が提案する安全性をみたすかどうかについて議論した．まず，これまでに提案され，乱数漏洩がない状況では安全性が証明されている多くの方式が，我々の定式化した安全性のうち，最も弱いもの (OW-CPA) すらみたさないことを示した．具体的には，ElGamal 暗号，Paillier 暗号，Cramer-Shoup 暗号，Fujisaki-Okamoto 変換による暗号，REACT，RSA-OAEP などがある．

次に，2 つの方式が，我々が提案する安全性をみたすことを証明した．具体的には，Coron, Handschuh, Joye, Paillier, Pointcheval, Tymen によって提案された GEM と，Phan, Pointcheval によって提案された 3-round OAEP である．

1 つめの GEM は，弱い安全性をみたす暗号方式を用意し，それをつかってより強い安全性をみたす暗号方式をつくることができる汎用変換方式である．我々は，GEM を用いれば，OWR-PCA をみたす暗号方式を用意することで，OWR-CCA をみたす暗号方式を構成できることを示した．

2 つめの 3-round OAEP は，公開鍵暗号の安全性として最も標準的である IND-CCA をみたす暗号方式である．証明のための仮定は，暗号方式で用いられている関数が partial one-way trap-door permutation であることである．我々は，同じ仮定の下で，3-round OAEP が OWR-CCA をみたすことを証明した．

4.6 複数ユーザーを考慮したトークンつき公開鍵暗号

トークンつき公開鍵暗号とは，Baek, Safavi-Naini, Susilo によって提案された概念である．

トークンつき公開鍵暗号では，暗号化を行う際，暗号文とともにトークンと呼ばれる補助情報を生成する．このとき，暗号文だけでは，秘密鍵をもっている人ですら復号を行うことができない．しかしながら，ひとたびトークンが公開されれば，秘密鍵をもっている人のみがその暗号文を復号することができる．このとき，秘密鍵をもっていない人は，暗号文とトークンの両方を手に入れても復号することができないようになっている．

つまり，トークンつき公開鍵暗号は，暗号文を事前に生成してそのデータを配布しておき，暗号文を復号させたいと思った時点でトークンを公開し，秘密鍵をもっている人だけに復号させるといった状況に適している．

トークンつき公開鍵暗号の安全性として，Baek らは 3 つの安全性を定式化した．これらは大きく 2 つに分けられる．ひとつは，秘密鍵をもっていてもトークンなしでは暗号文を復号できないという安全性 (IS-CPA) であり，もうひとつは，秘密鍵をもっていない人は（トークンが公開されても）暗号文を復号できないという安全性 (T1-CCA, T2-CCA) である．その後，Galindo, Herranz は，ある暗号文とトークンのペアに対して，そのトークンを別のものに置き換えることで，それがはじめに意図したものと異なる平文に復号されてしまうことがないという安全性 (SETUF) を定式化している．すなわち，この安全性はトークンつき公開

鍵暗号に対する改ざん不可能性をとらえている．

トークンつき公開鍵暗号の利用例としては，前に述べたように，暗号文を事前に生成してそのデータを配布しておき，暗号文を復号させたいと思った時点でトークンを公開し，秘密鍵をもっている人だけに復号させるといったものが考えられる．このような利用を考えた場合，トークンつき公開鍵暗号は，同じトークンを複数ユーザーで使えることが望ましい．すなわち，同じトークンを用いて複数ユーザーに複数の暗号文を送信し，あとでそのトークンを公開するといった使い方ができれば，使用するトークンがひとつだけですむため，効率の向上が期待できる．しかしながら，その場合の安全性については，現在の安全性の定式化ではとらえられておらず，新たに定式化を行う必要がある．

これをふまえて，我々はまず，複数ユーザーを考慮したトークンつき公開鍵暗号の安全性を提案した．安全性は 4 種類あり，M-IS-CPA, M-T1-CCA, M-T2-CCA, M-SETUF と呼ばれ，それぞれが Baek らおよび Galindo らが提案した安全性の複数ユーザー版となっている．これらの安全性は，単に複数ユーザーに拡張しただけではなく，Boldyreva, Micali のアイディアを用いて，より強力な攻撃者を考慮したものとなっている．すなわち，単に複数ユーザーに拡張したものに比べてより強い安全性を定式化したことになる．

次に，我々が提案した 4 つの複数ユーザー版の安全性と，過去に提案された単一ユーザー版の安全性の関係の一部を証明した．その結果は図 1に示されている．この図からわかるように，M-T2-CCA と M-SETUF については，対応する単一ユーザー版の安全性を証明すれば十分である．一方で，M-IS-CPA および M-T1-CCA については，対応する単一ユーザー版の安全性だけで十分であるかはわからない．

さらに，我々は，過去に提案されている Galindo, Herranz の方式が，提案した複数ユーザー版の安全性をみたすことを証明した．Galindo らは，彼らの方式が IS-CPA, T2-CCA, SETUF をみたすことを証明している．よって，我々が示した安全性間の関係（図 1）より，あとは M-IS-CPA を証明すれば，複数ユーザー版の全ての安全性をみたすことがわかる．我々は

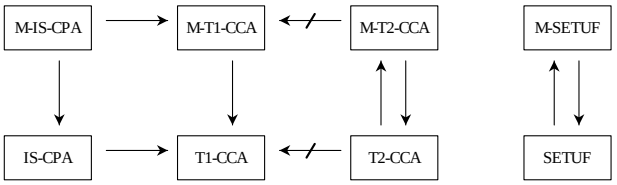

図 1: 安全性の関係．上段が複数ユーザーでの安全性，下段が単一ユーザーでの安全性を表す．

Galindo らの方式がランダムオラクルモデルにおいて M-IS-CPA をみたすことを証明した．なお，M-IS-CPA を証明するときの仮定は，Galindo らが IS-CPA を証明したときと変わっていない．

4.7 格子問題に基づく認証方式と署名方式

格子問題に基づく暗号方式が注目を集めている．その理由は, 暗号方式の安全性を格子問題の最悪時の困難性から保証できることにある．また今のところ格子問題を解く量子アルゴリズムが知られていないことにもある．現在, 公開鍵暗号とハッシュ関数については安全性を格子問題の最悪時の困難性から保証できるものが知られている．

格子問題に基づく署名方式として GGH 署名と NTRU 署名が知られている． しかし, 両者とも安全性証明が付けられておらず, 様々な攻撃を受けてきた．2006 年には NTRU 署名の一モードと GGH 署名について, Nguyen と Regev が公開鍵と数万個の署名から確率的に秘密鍵を求める攻撃を提案している．

次に, 格子問題に関する認証方式について述べる．Micciancio と Vadhan は 2003 年に GapCVP と呼ばれる問題の近似版について統計的なゼロ知識証明を提案している．また林と多田は BNELVP と呼ばれる問題について証拠秘匿性を持つ認証プロトコルを提案している．しかしこれらのプロトコルの安全性は格子問題の平均時の困難性に基づいて証明されている．

以上から分かるように, 認証方式と署名方式については, 安全性を格子問題の最悪時から保証できるものが知られていない．そこで, 我々は安全性の根拠を格子問題の最悪時とする認証方式と署名方式について研究を行った．

まず我々は Regev05 暗号の鍵生成アルゴリズム

を変形した. 変形したRegev05暗号の安全性がある学習問題の最悪時の困難性から保証できる. 鍵生成アルゴリズムの変形により, 公開鍵がq進符号のパリティ検査行列とシンドロームに, 秘密鍵がエラー付の符号語に対応する. 一方, Sternが二進符号のパリティ検査行列とシンドロームからハミング重みが固定されたエラー付符号語を求める問題に関するゼロ知識アーギュメントを提案している. 我々は, Sternのゼロ知識証明をq進版に拡張し, 公開鍵認証方式を得た. またFiat-Shamir変換を施すことで署名方式も得た.

さらに格子問題に基づくハッシュ関数も, ハッシュ関数のインデックスをq進符号のパリティ検査行列に, ハッシュ値をシンドロームに, ハッシュされる文書をエラー付の符号語に対応させることができる. ハッシュされる文書に少し制限を加えることで, 拡張したゼロ知識アーギュメントの枠組みに乗せることができる. したがって, ハッシュ関数のインデックスとハッシュ値を公開鍵に, ハッシュされる文書を秘密鍵とすることで, 公開鍵認証方式を得た. 先と同様に, Fiat-Shamir変換を施すことで署名方式も得た.

認証方式の安全性については以下である. 認証方式のなりすましに成功する敵が存在すると仮定する. このとき, 敵を上手く使うことで, 公開鍵から秘密鍵を得ることができる. 変形されたRegev05暗号を用いた認証方式では, 秘密鍵を得ることで暗号文の解読ができるので, なりすましに成功することは暗号の安全性が破れることを意味する. 暗号の安全性は, ある学習問題の最悪時に基づいているので, 認証方式の安全性も同じ問題の最悪時の困難性に基づいていることが言える. 一方, ハッシュ関数を用いた認証方式では, 秘密鍵を得ることで, ハッシュ関数の一方向性を破っている. ハッシュ関数の一方向性は格子問題の最悪時に基づいているので, 認証方式の安全性も同じ問題の最悪時に基づいている.

Fiat-Shamir変換を施して得られた署名方式のランダムオラクルモデルでの安全性は, 認証方式の安全性に基づくことがすでに知られている. したがって, 署名方式の安全性はランダムオラクルモデルでは格子問題または学習問題の最悪時に基づいている.

4.8 格子問題に基づく暗号方式の平文知識証明

平文知識証明とは, 公開鍵と暗号文を共通入力としたときに, 証明者が暗号文に対応する平文を知っていることを証明するゼロ知識証明のことである. 数論の問題に基づく暗号方式ではすでに多くの平文知識証明プロトコルが知られている. その暗号方式と平文知識証明を組み合わせることでより強い安全性を持つ暗号方式を得ることができる. また, 他のプロトコルに暗号方式を組み込む際にも使われるなど, 平文知識証明の応用は広い.

格子暗号の分野では, GoldwasserとKharchenkoが, Ajtai-Dwork暗号の暗号文に関する平文知識証明のプロトコルを2005年に提案している. 格子暗号にはAjtai-Dwork暗号以外にもRegev04暗号, Regev05暗号, GGH暗号, NTRU暗号等が知られているが, 平文知識証明プロトコルが提案されているのは, Ajtai-Dwork暗号のみである. そこで, 我々は彼らのプロトコルを応用し，Regev04暗号とRegev05暗号の暗号文に関する平文知識証明を提案した.

GoldwasserとKharchenkoのプロトコルでは, 共通入力である暗号文と公開鍵から, あるベクトルと格子の基底を生成する. 彼らはNguyenとSternがAjtai-Dwork暗号の攻撃に用いた基底の生成方法を採用し, 暗号文から得たベクトルと公開鍵から得た格子の関係を基底の生成方法に基づいて証明している. 具体的には, 基底の生成方法から, 0の暗号文から得たベクトルは公開鍵から得られた格子に近く, 1に復号される暗号文から得たベクトルは公開鍵から得られた格子から遠いということが言える. これと認証方式の関連研究で述べたMicciancioとVadhanのGapCVPに関するゼロ知識証明と疑似準同型性を用いることで, 全体のプロトコルを構成している.

そこで我々はRegev04暗号とRegev05暗号の公開鍵の特性に基づいて, 格子の基底の生成方法を考案し, 同様に暗号文から得たベクトルと公開鍵から得た基底で張られる格子の関係について証明を行った. さらに全体のプロトコルもGoldwasserとKharchenkoと同様に構成し, 証明を行った. 証明の都合上, Regev04暗号とRegev05暗号の安全性の基となる問題の安全性パラメータが悪くなることが分かった. 全体の安全性は格子暗号の安全

性の基となる問題の最悪時の困難性から保証することができる.

我々の結果には別の意味もある. Nguyen と Stern は格子の基底の生成方法を考案することにより, Ajtai-Dwork 暗号の暗号文を識別する問題が GapCVP の問題に関係することを示している. Nguyen と Stern は暗号の安全性パラメータ (格子の次元) が小さければヒューリスティックに 0 と 1 の暗号文を識別することが出来ることを示した. 我々は, Regev04 暗号と Regev05 暗号について, 格子の基底の生成方法を考案し, 暗号文を識別する問題が GapCVP の問題に関係することを本研究中で示した. したがって, Nguyen と Stern の攻撃方法と同様に, 安全性が低い場合の Regev04 暗号と Regev05 暗号も, 安全性パラメータが小さければヒューリスティックに 0 と 1 の暗号文を識別することが出来ることになる.

4.9 Pseudo-Free Group の変形

公開鍵暗号の安全性は，ある種の計算問題が効率的に解くことができないという仮定に依存している．よく知られた問題としては RSA 問題や離散対数問題などがある．これらの問題が効率的に解くことができないということを仮定して安全性が証明できる具体的な暗号方式としては，前者は RSA 暗号系や RSA-OAEP，後者は ElGamal 暗号系や Cramer-Shoup 暗号系などがある．

2004 年に Rivest は多くの暗号的な計算問題が効率的に解けないことが証明できる Pseudo-Free Group と呼ばれる群を提案した．具体的に Pseudo-Free Group においては，上述の RSA 問題や離散対数問題は効率的に解くことができない．この群は，Free Group の方程式に着目して定義されたものである．Free Group は多くの暗号的な問題が解くことができないことが知られている．しかしながら，この群は原始的過ぎて暗号で用いるには使い物にならない．よって，擬似的な Free Group を定義することは暗号学的に有用である．

Pseudo-Free Group は先に述べたように，多くの計算問題が効率的に解くことができないということから，暗号学的にみて強い仮定だと言える．それゆえに，様々な安全性の証明が簡単になると同時に，証明の新しいフレームワークになることが期待できる．さらには，この強い仮定を利用して新たなアプリケーションが構築できるのではないかとも期待できる．

Rivest が Pseudo-Free Group の定義する以前に，Hohenberger によって簡単に概念が提示されていた．そこでは Pseudo-Free Group をさらに強くすることで，Micali と Rivest によって提案された Directed Transitive Signature と呼ばれる特殊な署名方式の構築の十分条件が与えられていた．

Rivest は Pseudo-Free Group のいくつかの性質を述べたのではあるが，肝心な Pseudo-Free Group であるような群が実際にあるかどうかはわかっていなかった．2005 年に Micciancio は RSA 暗号系などで用いられる群 $(\mathbb{Z}/n\mathbb{Z})^{\times}$ が Strong RSA 仮定の下で Pseudo-Free であることを示した．ただし，n は Strong Prime と呼ばれる特殊な 2 つの素数の積である．

今回我々は，Rivest の論文中の証明についての問題点の指摘と，Pseudo-Free Group の変形についてのいくつかの性質を示した．

前者については Pseudo-Free Group において，RSA 問題のような暗号的な計算問題が効率的に解くことはできないということを先に述べたが，このことが疑わしいことがわかった．その理由は Rivest が与えた Pseudo-Free Group の方程式に問題があったためである．具体的には指数部分に変数を持つことが許されないということである．離散対数問題等の多くの暗号的な計算問題は方程式からの立場から述べると，指数の部分に (整数) 変数を持つことが多々ある．それにも関わらず Rivest は許されない方程式の形を使って，離散対数問題等の問題が Pseudo-Free Group では効率的に解けないと述べた．

それゆえ我々は，Rivest が同じ論文中で提案した Pseudo-Free Group の変形である Pseudo-Free Group with Generalized Exponential Expression と，発表で使われたプレゼンテーション資料に記されていた Weakly Pseudo-Free Group という二つの変形を用いて，Pseudo-Free Group の議論を行うことにした．

特に Pseudo-Free Group with Generalized Exponential Expression については紹介程度にとどまっており，我々は定式化を行い，さらにはそのことを用いて，先ほどの Pseudo-Free Group では

成り立つことが疑わしい問題も解決することができた.

次に後者であるが，これは Pseudo-Free Group with Generalized Exponential Expression と Weakly Pseudo-Free Group の関係を中心にいくつか性質を示した.

特に，一つの元 g で生成される群 $\langle g\rangle$ を Pseudo-Free Group with Generalized Exponential Expression としたとき，適当に選んだ元 h を加えた二つの元で生成される群 $\langle g, h\rangle$ は Weakly Pseudo-Free Group となることを示した．一般的には，$\langle g\rangle$ の暗号的な強さが $\langle g, h\rangle$ になると弱まってしまう場合があることが知られている．この定理は，例えば $\langle g\rangle$ を使って離散対数問題ベースの暗号系を構成したときに，群を $\langle g\rangle$ のように拡張しても安全性が保証できることを述べてもいる．このことは，Pseudo-Free Group with Generalized Exponential Expression と Weakly Pseudo-Free Group においてどちらの群ともに離散対数問題が効率的に解くことができないことから言える.

5 グラフアルゴリズムに関するミニ研究集会 (2005 年)

戸田が世話役となり，Chordal graph に関する計算問題ならびにアルゴリズムを中心に，研究成果の発表と新たな課題探求に向けた討論を行った.

日時： 2005 年 3 月 19 日 (土)　午前 10 時 ~ 午後 6 時
場所： 日本大学文理学部 8 号館レクチャーホール
参加者数： 19 名
研究発表：

(1) 10:00~11:20，Computing automorphism groups of chordal graphs whose simplicial components are of small size，戸田誠之助（日大文理）
（概要）小さなサイズの単体成分へと分解可能な任意の chordal graph に対して，その自己同型群が多項式時間計算可能であることを示した.

(2) 11:30~12:30，2-リンクパズルの多項式時間解法，牧野 格三（東工大）
（概要）ナンバーリンクパズルを「k-リンクパズル」と呼ばれるグラフ論的な計算問題へと一般化し，3 × (偶数) や 4 × (偶数) といった格子グラフに関する 2-リンクパズルに対して多項式時間アルゴリズムを示すとともに，一般の格子グラフに関する予想を述べた．さらに，参加者を交えた討論を経て新たな研究課題が見出された.

(3) 13:30~15:00，On the Laminar Structure of Ptolemaic and Distance Hereditary Graphs，上原 隆平 (JAIST)，宇野裕之 (大阪府立大学)
（概要）Chordal graph（のクラス）と distance hereditary graph（のクラス）の共通部分として特徴付けられている Ptolemaic graph（のクラス）に対して，ある種の木表現モデルが存在すること，その木表現モデルが各 Ptolemaic graph に対して一意的に定まること，ならびに，その木表現モデルを線形時間で構築できることを示した．さらに，この結果をもとに，Ptolemaic graph（のクラス）に対する認識問題や同型性判定問題が線形時間計算可能であることを示した．また，この研究の発展的可能性として，distance hereditary graph に対する同様の木表現モデルの存在性に関する予想を述べた.

(4) 15:15~16:45，On precoloring extension problem，名古屋孝幸（東京電機大学）
（概要）グラフの precoloring extension problem (PREXT と略す) に対して，一般のグラフに対しては NP 完全であることや，クリーク数を制限した chordal graph に対して多項式時間計算可能であることを紹介した．また，PREXT を制限した 1-PREXT 問題に対して，chordal graph に対するネットワークフローを用いた多項式時間アルゴリズムを紹介した.

研究発表終了後，午後 6 時頃まで討論を行った．討論の間に，グラフ自己同型群問題の応用研究として，河内亮周氏（東工大）に次の成果を発表して頂いた.

(5) Computational Distinguishability between Quantum States and Its Applications，A.

Kawachi, T. Koshiba, H. Nishimura and T. Yamakami

（概要）確率分布に対する判別問題の自然な一般化として，二つの量子状態を判別する問題（QSCDff）を新たに定義し，その問題が落とし戸関数の性質を有すること，その最悪計算量と平均計算量が等価であること，さらに，その最悪計算量がグラフ自己同型群問題の最悪計算量と同等以上であることを示した．

各地から多くの参加者を得て活発な討論が行われ，発展的研究課題を見出すこともできて，とても充実した研究集会であった．

6 暗号理論に関するミニ研究集会 (2006年)

総括班の櫻井の呼びかけをきっかけに，本特定領域研究における暗号理論の研究者：

太田 和夫 (電気通信大学)
國廣 昇 (電気通信大学)
櫻井 幸一 (九州大学)
高木 剛 (はこだて未来大学)
田中 圭介 (東京工業大学)

とそれぞれの研究グループの研究者を中心にミニ研究集会を開催した．はこだて未来大学の高木が会場世話人となり，田中がプログラムのとりまとめをした．

当日の参加者は講演者を含めて約 20 名だった．講演は下記の概要の通りであるが，1, 3 番目の講演は，各自の研究成果に関する内容が中心であり，2, 4, 5 番目の講演は，研究分野のサーベイに関する内容が中心であった．

参加者が少ないこともことも手伝って自由に質問できる雰囲気があった．実際，発表の最中にも質問がでるなど活発な質疑や討論が行われ，それぞれの専門分野に関する理解を深めることができた．ただ，本研究集会は，参加者の都合により，半日で開催することになったが，そのため，発表および質疑応答の時間が十分だとはいえなかった．

研究集会後に開いた懇親会では，通常の学会主催の研究会では得られない貴重な集まりだったという意見が多く，次年度以降も継続してこのような暗号理論の研究集会を開催したいという意見も多かった．

日時　2006 年 2 月 16 日 (木) 13:00-17:30

場所　はこだて未来大学 小講義室 585 （〒 041-8655 北海道函館市亀田中野町 116 番地 2）

プログラム

1. 13:00-13:30
   Privacy-preserving Text Mining in Distributed Environment
   ○ Chunhua Su, Kouichi Sakurai (九州大学)

2. 13:30-14:00
   Pairing Implementation using Hyperelliptic Curves
   Colm O hEigeartaigh (Dublin City University)

3. 14:15-15:00
   A Survey about Side Channel Attacks on XTR
   ○ Dong-Guk Han, Tsuyoshi Takagi (はこだて未来大学)

4. 15:00-15:45
   オフライン検証性を満たす追跡不可能な量子現金
   國廣 昇 (電気通信大学)

5. 16:00-16:45
   離散対数問題系に基づく安全で効率的な署名方式
   太田 和夫 (電気通信大学)

6. 16:45-17:30
   匿名性をもつ公開鍵暗号
   ○林 良太郎, 田中 圭介 (東京工業大学)

各発表の概要

1. Privacy-preserving Text Mining in Distributed Environment
   ○ Chunhua Su, Kouichi Sakurai (九州大学)
   概要：プライバシーを考慮したデータマイニングに対する研究のサーベイと今回，テキス

トデータをとくに扱ったものに関する著者の提案法方式の紹介．キーワードを用いた質疑プロトコルを利用する際に，紛失通信という暗号技術を利用している．

2. Pairing Implementation using Hyperelliptic Curves
   Colm O hEigeartaigh (Dublin City University)
   概要：ID ベース暗号の実現で注目されている楕円曲線ペアリングを，超楕円曲線の場合に適用した場合のサーベイと著者による最新の実装データを報告した．標数が 2,3 の Duursma-Lee 法を改良した η ペアリングは，現在のところ最も高速にペアリング暗号を実装するアルゴリズムである．1024 ビットのセキュリティを持つ埋込み次数 12 の超特異な超楕円曲線を用いて，Pentium 4 + SSE2 において 1.8ms を達成した．

3. A Survey about Side Channel Attacks on XTR
   ○ Dong-Guk Han, Tsuyoshi Takagi (はこだて未来大学)
   概要：拡大次数 6 の有限体上の離散対数問題を利用した XTR という公開鍵暗号系に対する実装攻撃のサーベイ．発表者 (昨年度は九大で博士課程在籍，今年度は未来大でポスドク) を中心とするここ数年の解読法と防御法に関する研究を紹介した．著者等が提案したユークリッド互助法を応用した防御法は，固定パターン持つ耐 SPA 性クラスの中で最速な方式である．この領域は，未だに「攻撃→防御→攻撃」の繰り返しで研究が進行しているのが現状である．

4. オフライン検証性を満たす追跡不可能な量子現金
   國廣 昇 (電気通信大学)
   概要：これまでに提案されている量子現金方式は，オフライン検証性または追跡不可能性のどちらか一方を満たす方式であったが，今回はこの 2 つの性質を同時に満足する量子現金の提案を行った．さらに，提案した量子現金を，古典の電子現金の世界だけで見てみた場合の対応付けを考察し，量子現金方式の安全性評価への方向付けを示した．

5. 離散対数問題系に基づく安全で効率的な署名方式
   太田 和夫 (電気通信大学)
   概要：Schnorr 署名にはじまり，CRYPTO 2005 で発表された最新の Chevallier 署名にいたる離散対数問題系に基づく電子署名の安全性と効率に関するサーベイ．安全性の根拠として，離散対数問題，計算 Deffie-Hellmann 問題，判定 Deffie-Hellmann 問題の困難性を仮定した場合の，署名生成の実現手段，困難な問題を署名偽造に帰着するための帰着効率，計算効率などを比較している．困難な問題の制約を強めると，帰着効率や計算効率が向上していることが，具体例によって確認できた．

6. 匿名性をもつ公開鍵暗号
   ○林 良太郎, 田中 圭介 (東京工業大学)
   概要：暗号文を見ても，それが誰の公開鍵で暗号化されたのかがわからない，という暗号文の受信者の匿名性に関する研究．2001 年ごろ概念が提起・定式化され匿名通信路の実現・電子入札などへの応用をもつ．著者らの開発した技術を含む，4 つの実現テクニックを，RSA 暗号とエルガマル暗号の場合に分けて，比較考察している．今後の課題としては，ランダムオラクルモデルに依存しない標準モデルの場合の考察・匿名性を満たす ID ベース方式の実現などがある．

7 暗号理論に関するミニ研究集会 (2007 年)

2006 年に続き、特定領域研究「新世代の計算限界」暗号関係ミニ研究集会を開催した．本研究集会は，本特定領域研究における暗号理論の研究者：

太田 和夫 (電気通信大学)
國廣 昇 (電気通信大学)
櫻井 幸一 (九州大学)
高木 剛 (はこだて未来大学)
田中 圭介 (東京工業大学)

とそれぞれの研究グループの研究者を中心に開催された．電気通信大学の國廣が会場世話人とプログラムのとりまとめを行った．

2006 年は函館での開催，期間は 1 日であったが，2007 年は東京での開催，期間は 2 日だった．参加者は，2006 年は約 20 名だったが，2007 年は 1 日目が約 40 名，2 日目が約 30 名と増加した．また 2006 年と異なり，企業の研究所からも多くの参加者がいた．

講演は下記の概要の通りであるが，1，10 番目の講演は，研究分野のサーベイに関する内容が中心であり，残りの講演は各自の研究成果に関する内容が中心であった．

参加者は少なくなかったものの自由に質問できる雰囲気が常にあった．実際に，講演の最中にも質問がでたり，講演直後の決められた時間以外にも活発な討論がされたりと，それぞれの専門分野に関する理解を深めることができた．

研究集会 1 日目の後の懇親会では，通常の学会主催の研究会では得られない貴重な集まりだったという意見や，次年度以降も継続してこのような暗号理論の研究集会を開催したいという意見が多く聞かれた．他にも研究集会に関して具体的に，一件あたりの発表および質疑応答の時間をもっと長くとりたい，チュートリアル講演を主体としたスクール的な研究集会をもちたいなどといった意見も聞かれた．

日時　2007 年 3 月 2 日 (金) 13:30–17:30, 3 日 (土) 9:30–15:45

場所　電気通信大学 総合研究棟 601 会議室 (〒182-8585 東京都調布市調布ヶ丘 1-5-1)

プログラム

1. 3 月 2 日 (金) 13:30–14:30
   証明可能安全性理論に向けて
   太田 和夫 (電気通信大学)

2. 14:45–15:15
   耐タンパ性を備えたユニークデバイスに基づく暗号認証基盤の検討
   今本 健二 (九州大学) (発表者: 蘇 春華 (九州大学))

3. 15:15–16:00
   ペアリング暗号の安全な高速実装について
   高木 剛 (はこだて未来大学)

4. 16:15–16:45
   指定検証者署名の定式化，および，送信者と受信者の匿名性について
   大山 千尋 (東京工業大学)

5. 16:45–17:30
   Concurrently Secure Password-based Authenticated Key Exchange without Random Oracles or Setup Assumptions
   米山 一樹 (電気通信大学)

6. 3 月 3 日 (土) 9:30–10:30
   スタンダードモデル PA の基礎に関して
   寺西 勇 (NEC)

7. 10:45–11:30
   Non-Malleability Definitions Reconsidered
   宮川 聡 (電気通信大学)

8. 11:30–12:15
   Collusion-resistant Private Association Rules Mining in Distributed Environment
   蘇 春華 (九州大学)

9. 13:30–14:15
   Revisiting Zero-Knowledgeness of an On the Fly Authentication Scheme
   Bagus Santoso (電気通信大学)

10. 14:15–15:45
    格子問題をベースとした暗号について
    草川 恵太 (東京工業大学)

各発表の概要

1. 証明可能安全性理論に向けて
   太田 和夫 (電気通信大学)
   概要: 実用的な暗号技術として，安全性が理論的に証明できる（証明可能安全な）方式が期待されている．公開鍵暗号の発明後しばらくの間『ある攻撃に対して安全な方式は，別の攻撃に対しては安全性証明がつかない』と信じられていた (Folklore)．本解説では,「folklore」の呪縛から逃れ,「安全性証

明」への道筋を示した Goldwasser, Micali, Rivest による記念碑的な論文を紹介することで，本研究集会の導入とする．安全性定理に込められた「ココロ」，呪縛からの解放の「アイデア」などを解説した．

2. 耐タンパ性を備えたユニークデバイスに基づく暗号認証基盤の検討
今本 健二 (九州大学)
概要：従来，公開鍵証明書を用いた公開鍵基盤（PKI）や ID ベース暗号を利用した暗号化システムにおいては，数学アルゴリズムや第三者機関の利用など，様々な仮定に基づいた設計が行われている．本論文では，深谷らが提案したデバイス固有値を用いた対称暗号技術による ID ベース暗号化方式（IST 方式）に基づいた手法を検討し，本方式を用いることで認証を行う方式（3way 認証方式）を提案し，既存の認証方式との比較を行う．

3. ペアリング暗号の安全な高速実装について
高木 剛 (公立はこだて未来大学)
概要：ペアリング暗号の安全な高速実装について考察を行う．高速実装するにあたっては，ペアリングに関する演算の理論的改良，ペアリングをプログラミングコードで実装する際の種々の工夫を行っている．理論的改良については，３乗根を求めることなく EtaT ペアリングを演算する方法，および，トーラスを用いた最終的な結果を得るための指数演算の方法の２つを主に提案した．プログラミングコードで実装する際の種々の工夫に関しては，Java, C, BREW, FPGA の４つのコードにおいて高速実装を行った．さらには，ペアリングに関するサイドチャネル攻撃についても考察した．

4. 指定検証者署名の定式化，および，送信者と受信者の匿名性について大山 千尋 (東京工業大学)
概要：本研究では，指定検証者署名における「受信者（指定検証者）の匿名性」という新しい安全性の概念を提案する．指定検証者署名を用いると，署名者が，特定の人にだけ検証が可能であるような署名を生成することができる．受信者の匿名性とは，攻撃者が署名を盗聴しても，その署名がだれに向けて指定されたのかが判別できないという性質である．我々は，この受信者の匿名性という概念を定式化するとともに，この性質をみたす方式を２つ提案する．

5. Concurrently Secure Password-based Authenticated Key Exchange without Random Oracles or Setup Assumptions
米山 一樹 (電気通信大学)
概要：本発表では，plain model におけるパスワード認証つき鍵交換の一般的な構成法を提案する．ここで plain model とは，その方式がランダムオラクル，あるいは，trusted setup assumption を必要としないという意味である．さらに，我々の方式は複数のインスタンスが同時にプロトコルを実行したとしても（concurrent でも）安全である．我々の方式は plain model で concurrent な安全性を達成する初めての方式である．

6. スタンダードモデル PA の基礎に関して
寺西 勇 (NEC)
概要：plaintext awareness という安全性の概念についての考察を行った．plaintext awareness とは，公開鍵暗号の安全性についての概念であり，暗号文を作れる人はいうその平文を知っているはずであるという性質である．plaintext awareness は，もともとはランダムオラクルモデルという強い仮定の下で定義されていたが，近年はスタンダードモデルでの定義も提案されている．本発表では，現在の定義の問題点などを指摘するとともに，他の安全性の概念との関連性を示した．

7. Non-Malleability Definitions Reconsidered
宮川 聡 (電気通信大学)
概要：公開鍵暗号方式が 頑健性 (NM) を満たすとは，攻撃者が，暗号文から，対応する平文を改ざんした新たな暗号文を作成できないことをいう．この NM の概念を定式化するためには，攻撃者が作成すべき「新たな暗号文」に条件を付加する必要がある． この条件は２種類にわけられ，攻撃者は新たな暗号文に不正な暗号文を含めることはできないといった定義 (定義 1) と，攻撃者は新たな暗号

文に不正な暗号文を含めることはできるが，含めた場合には実験に失敗するといった定義 (定義 2) がある．本研究では，NM に関する 3 種類の定義 (SNM, CNM, IND-P) について，SNM および CNM においては，定義 1 と定義 2 の間には攻撃者の能力の観点からすると差がないことを示した．また，IND-P においては，定義 2 のような方法では条件を付加することは不可能であることも示した．

8. Collusion-resistant Private Association Rules Mining in Distributed Environment
蘇 春華 (九州大学)
概要：相関ルールマイニングはデータベースに蓄積された大量のデータから，頻繁に同時に生起する事象同士を相関の強い事象の関係，すなわち相関ルールとして抽出する技術である．本論文では，相関ルールのプライバシー保護問題に着目し，結託を防止した安全なプライベート相関ルールマイニング手法を提案した．従来の提案では準同型性暗号の暗号を用いており，鍵の管理と生成，計算量と通信量はかなり大きいものだった．今回の我々のの提案では，分散ネットワークにおける n 個のパーティーがデータベースのプラバシーを保ったままで，共同の相関ルールマイニングを算出するシナリオを想定する．我々は，Han による Apriori algorithm の効率を大きく改善するアルゴリズムを使って，結託を防止できる効率のよい手法を提案した．

9. Revisiting Zero-Knowledgeness of an On the Fly Authentication Scheme
Bagus Santoso (電気通信大学)
概要：on-the-fly の認証方式である GPS のなりすましに対する安全性は，ゼロ知識性に依存して証明されているが，実際に使用した場合の安全性についての詳細な考察は行われていなかった．我々は，GPS に対して，正当な証明者と検証者の間での通信履歴を集めるだけで，秘密鍵の先頭ビットを計算することができることを示した．

10. 格子問題をベースとした暗号について
草川 恵太 (東京工業大学)
概要：格子問題に基づく暗号方式が注目を集めている．その理由は，暗号方式の安全性を格子問題の最悪時の困難性から保証できることにある．また今のところ格子問題を解く量子アルゴリズムが知られていないことも格子問題に基づく暗号方式が注目を集める理由のひとつである．現在，公開鍵暗号とハッシュ関数については安全性を格子問題の最悪時の困難性から保証できるものが知られている．本発表では，ハッシュ関数を攻撃することが，組合せ問題の最悪時の困難性と結びつくことを詳細に解説した．さらに，未解決問題についても解説を行った．

研究業績一覧

著書

1. 金森敬文，畑埜晃平，渡辺治:
“ブースティング — 学習アルゴリズムの設計技法”, 森北出版, 2006 年.
概要: ブースティング技法について，その入門的な解説を述べ，著者らが行ってきた理論的な研究を紹介した本．ブースティング技法の背景にある PAC 学習の話から始め，ブースティングによる学習アルゴリズムの基礎を解説する．その後で，著者らの研究の中で，とくにブースティングを応用してみたい人が直面するだろう疑問点に対し，我々が理論的に見出した解決法を紹介する形で解説した．

学術論文

1. T. Onodera and K. Tanaka:
“Shuffle for Paillier’s Encryption Scheme”, IEICE Transactions on Fundamentals, Special Section on Discrete Mathematics and Its Applications, （掲載予定）.
概要: In this paper, we propose a proof scheme of shuffle, which is an honest verifier zero-knowledge proof of knowledge such as the protocols by Groth and Furukawa. Unlike the previous schemes proposed by Furukawa-Sako, Groth and Furukawa, our

scheme can be used as the shuffle of the elements encrypted by Paillier's encryption scheme, which has an additive homomorphic property in the message part. The ElGamal encryption scheme used in the previous schemes does not have this property.

2. O. Watanabe:
"Randomized algorithms for 3-SAT", Theory of Computing Systems, (掲載予定).
概要: SAT 問題に対して，最悪時時間計算量の改善を行った．具体的には，まず，3SAT 問題に対し，これまでの変数数 n に対する最悪時計算時間 $O(1.333^n)$ の乱択アルゴリズムに対し，最悪時計算時間が $O(1.330^n)$ のアルゴリズムを設計した．一方，一般の SAT 問題に対しては，決定性アルゴリズムを考え，これまでの最悪時計算時間 $O(1.239^m)$ のアルゴリズム（ただし m は論理式の節数）に対し，$O(1.234^m)$ のアルゴリズムを提案した．

3. M. Yamamoto:
"Generating instances for MAX2SAT with optimal solutions", Theory of Computing Systems, (掲載予定).
概要: MAX-SAT 問題の難しさの平均的な解析をする際，問題例の分布に対する確率モデルが必要である．これまで，そのような確率モデルとして妥当なものがなかったが，我々は，MAX-2SAT 問題に対して，まず，テスト例題生成，という観点から問題例生成の手法を提案した．さらに，それを単純化して，MAX-2SAT 問題の問題例に対する自然な確率分布を提案することができた．

4. Masahito Hayashi, Akinori Kawachi, and Hirotada Kobayashi:
"Quantum Measurements for Hidden Subgroup Problems with Optimal Sample Complexity", Quantum Information and Computation Journal, (掲載予定).
概要: One of the central issues in the hidden subgroup problem is to bound the sample complexity, i.e., the number of identical samples of coset states sufficient and necessary to solve the problem. In this paper, we present general bounds for the sample complexity of the identification and decision versions of the hidden subgroup problem. As a consequence of the bounds, we show that the sample complexity for both of the decision and identification versions is $\Theta(\log H \log p)$ for a candidate set H of hidden subgroups in the case where the candidate nontrivial subgroups have the same prime order p, which implies that the decision version is at least as hard as the identification version in this case. In particular, it does so for the important cases such as the dihedral and the symmetric hidden subgroup problems. Moreover, the upper bound of the identification is attained by a variant of the pretty good measurement. This implies that the concept of the pretty good measurement is quite useful for identification of hidden subgroups over an arbitrary group with optimal sample complexity.

5. J. Cai and O. Watanabe:
"Relativized collapsing between BPP and PH under stringent oracle access.", Information Processing Letters, 90(3), 147-154, May, 2004.
概要: We propose a new model of stringent oracle access defined for a general complexity class. For example, when comparing the power of two machine models relative to some oracle set X, we restrict that machines of both types ask queries from the same segment of the set X. In particular, for investigating polynomial-time (or polynomial-size) computability, we propose polynomial stringency, bounding query length to any fixed polynomial of input length. Under such stringent oracle access, we show an oracle G such that $\mathrm{BPP}^G = \mathrm{PH}^G$.

6. J. Cai and O. Watanabe.:
"On proving circuit lower bounds against the polynomial-time hierarchy", SIAM

Journal on Computing, 33(4), 984-1009, 2004.

概要: We consider the problem of proving circuit lower bounds against the polynomial-time hierarchy. We give both positive and negative results. For the positive side, for any fixed integer $k > 0$, we give an explicit SIGptwo language, acceptable by a SIGptwo-machine with running time $O(n^{k^2+k})$, that requires circuit size $> n^k$. This provides a constructive version of an existence theorem of Kannan. Our main theorem is on the negative side. We give evidence that it is infeasible to give relativizable proofs that any single language in the polynomial-time hierarchy requires super polynomial circuit size. Our proof techniques are based on the decision tree version of the Switching Lemma for constant depth circuits and Nisan-Wigderson pseudorandom generator. We also take this opportunity to publish some unpublshed older results of the first author on constant depth circuits, both straight lower bounds and inapproximability results based on decision tree type Switching Lemmas.

7. R. Uehara, S. Toda, T. Nagoya:
"Graph Isomorphism Completeness for Chordal Bipartite Graphs and Strongly Chordal Graphs", Discrete Applied Mathematics, 145(3), 479–482, January, 2005.
概要: This paper deals with the graph isomorphism (GI) problem for two graph classes: chordal bipartite graphs and strongly chordal graphs. It is known that GI problem is GI complete even for some special graph classes including regular graphs, bipartite graphs, chordal graphs, comparability graphs, split graphs, and k-trees with unbounded k. On the other hand, the relative complexity of the GI problem for the above classes was unknown. We prove that deciding isomorphism of the classes are GI complete.

8. Akinori Kawachi, Hirotada Kobayashi, Takeshi Koshiba, and Raymond H. Putra:
"Universal Test for Quantum One-Way Permutations", Theoretical Computer Science, 345(2-3), 370-385, 2005.
概要: The next bit test was introduced by Blum and Micali and proved by Yao to be a universal test for cryptographic pseudorandom generators. On the other hand, no universal test for the cryptographic one-wayness of functions (or permutations) is known, although the existence of cryptographic pseudorandom generators is equivalent to that of cryptographic one-way functions. In the quantum computation model, Kashefi, Nishimura and Vedral gave a sufficient condition of (cryptographic) quantum one-way permutations and conjectured that the condition would be necessary. In this paper, we affirmatively settle their conjecture and complete a necessary and sufficient condition for quantum one-way permutations. The necessary and sufficient condition can be regarded as a universal test for quantum one-way permutations, since the condition is described as a collection of stepwise tests similar to the next bit test for pseudorandom generators.

9. Kazuo Iwama, Akinori Kawachi, and Shigeru Yamashita:
"Quantum Biased Oracles", IPSJ Journal, 46(10), 2400-2408, 2005.
概要: This paper reviews researches on quantum oracle computations when oracles are not perfect, i.e., they may return wrong answers. We call such oracles biased oracles, and discuss the formal model of them. Then we provide an intuitive explanation how quantum search with biased oracles by Høyer, et al. (2003) works. We also review the method, by Buhrman, et al. (2005), to obtain all the answers of a quantum biased oracle without any overhead compared to the perfect oracle case. Moreover, we dis-

cuss two special cases of quantum biased oracles and their interesting properties, which are not found in the classical corresponding cases. Our discussion implies that the model of quantum biased oracle adopted by the existing researches is natural.

10. Kazuo Iwama, Akinori Kawachi, and Shigeru Yamashita:
"Quantum Sampling for Balanced Allocations", IEICE transactions on Information and Systems, E88-D(1), 47-52, 2005.
概要: It is known that the original Grover Search (GS) can be modified to use a general value for the phase θ of the diffusion transform. Then, if the number of answers is relatively large, this modified GS can find one of the answers with probability one in a single iteration. However, such a quick and error-free GS can only be possible if we can initially adjust the value of θ correctly against the number of answers, and this seems very hard in usual occasions. A natural question now arises: Can we enjoy a merit even if GS is used without such an adjustment? In this paper, we give a positive answer using the balls-and-bins game in which the random sampling of bins is replaced by the quantum sampling, i.e., a single round of modified GS. It is shown that by using the quantum sampling: (i) The maximum load can be improved quadratically for the static model of the game and this improvement is optimal. (ii) That is also improved to $O(1)$ for the continuous model if we have a certain knowledge about the total number of balls in the bins after the system becomes stable.

11. Kazuo Iwama and Akinori Kawachi:
"Compact Routing with Stretch Factor of Less Than Three", IEICE transactions on Information and Systems, E88-D(1), 39-46, 2005.
概要: Cowen gave a universal compact routing algorithm with a stretch factor of three and table-size of $O(n^{2/3}\log^{4/3} n)$ based on a simple and practical model. (The table-size is later improved to $O(n^{1/2}\log^{3/2} n)$.) This paper considers, using the same model, how the necessary table-size differs if the stretch factor must be *less than* three. It is shown that: (i) There is a routing algorithm with a stretch factor of two whose table-size is $(n-\sqrt{n}+2)\log n$. (ii) There is a network for which any routing algorithm that follows the model and with a stretch factor of less than three needs a table-size of $(n-2\sqrt{n})\log n$ in at least one node. Thus, we can only reduce roughly an *additive* $\sqrt{n}\log n$ (i.e., $\sqrt{n}$ table-entries) from the trivial table-size of $n\log n$ which obviously enables shortest-path routing. Furthermore it turns out that we can reduce only an additive $\log n$ (i.e., only one table-entry) from the trivial $n\log n$ if we have to achieve a stretch factor of less than *two*. Thus the algorithm (i) is (roughly) tight both in its stretch factor and in its table-size.

12. S. Balaji, H.M. Mahmoud, and O. Watanabe:
"Distributions in the Ehrenfest process", Statistics and Probability Letters, Vol. 76, 666-674, 2006.
概要: We introduce a tenable class of urns that generalize the classical Ehrenfest model, and analyze the Ehrenfest process obtained by embedding the discrete evolution in real time. We show that lurking under the Ehrenfest process is a limiting binomial distribution, whose number of trials is an integer invariant property of the process.

13. J.Y. Cai and O. Watanabe:
"Random access to advice strings and collapsing result", Algorithmica, Vol. 45, 43-

57, 2006.

概要: We propose a model of computation where a Turing machine is given random access to an advice string. With random access, an advice string of exponential length becomes meaningful for polynomially bounded complexity classes. We compare the power of complexity classes under this model. It gives a more stringent notion than the usual model of computation with relativization. Under this model of random access, we prove that there exist advice strings such that the Polynomial-time Hierarchy PH and Parity Polynomial-time all collapse to P.

14. Akinori Kawachi and Takeshi Koshiba:
"Progress in Quantum Computational Cryptography", Journal of Universal Computer Science, Vol. 12, No. 6, 691-709, 2006.

概要: Shor's algorithms can be regarded as a negative effect of the quantum mechanism on public-key cryptography. From the computational point of view, his algorithms illustrate that quantum computation could be more powerful. It is natural to consider that the power of quantum computation could be exploited to withstand even quantum adversary. Over the last decade, quantum cryptography has been discussed and developed even from the complexity-theoretic point of view. In this paper, we will survey the investigation on quantum computational cryptography.

15. R. Hayashi and K. Tanaka:
"Schemes for Encryption with Anonymity and Ring Signature", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security, Vol. E89-A, No. 1, 66-73, January, 2006.

概要: In this paper, we present previously unproposed schemes with the anonymity property for encryption and ring signature by applying two techniques. That is, we construct a key-privacy encryption scheme by using N-ary representation, and a ring signature scheme by using the repetition of evaluation of functions. We analyze precisely the properties of these schemes and show their advantage and disadvantage.

16. H. Hiwatari and K. Tanaka:
"A Cramer-Shoup Variant Related to the Quadratic Residuosity Problem", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security, Vol. E89-A, No. 1, 203-205, January, 2006.

概要: At Eurocrypt '02, Cramer and Shoup proposed a general paradigm to construct practical public-key encryption schemes secure against the adaptive chosen ciphertext attack as well as several concrete examples. One of these example is the scheme based on the quadratic residuosity (QR) problem. However this scheme is less efficient than the other examples. In this paper, we construct a new variant of the Cramer-Shoup encryption scheme which is related to the QR problem. Our variant is more efficient than the scheme based on the QR problem.

17. Akinori Kawachi and Koshiba Takeshi:
"Progress in Quantum Computational Cryptography", Journal of Universal Computer Science, 12(6), 691-709, 2006.

概要: Shor's algorithms for the integer factorization and the discrete logarithm problems can be regarded as a negative effect of the quantum mechanism on publickey cryptography. From the computational point of view, his algorithms illustrate that quantum computation could be more powerful. It is natural to consider that the power of

quantum computation could be exploited to withstand even quantum adversaries. Over the last decade, quantum cryptography has been discussed and developed even from the computational complexity- theoretic point of view. In this paper, we will survey what has been studied in quantum computational cryptography.

18. Akinori Kawachi, and Takeshi Koshiba:
"Quantum Computational Cryptography", Topics in Applied Physics, Vol.102, 167-184, 2006.
概要: As computational approaches to classical cryptography have succeeded in the establishment of the foundation of the network security, computational approaches even to quantum cryptography are promising, since quantum computational cryptography could offer richer applications than the quantum key distribution. Our project focused especially on the quantum one-wayness and quantum public-key cryptosystems. The one-wayness of functions (or permutations) is one of the most important notions in computational cryptography. First, we give an algorithmic characterization of quantum one-way permutations. In other words, we show a necessary and sufficient condition for quantum one-way permutations in terms of reflection operators. Second, we introduce a problem of distinguishing between two quantum states as a new underlying problem that is harder to solve than the graph automorphism problem. The new problem is a natural generalization of the distinguishability problem between two probability distributions, which are commonly used in computational cryptography. We show that the problem has several cryptographic properties and they enable us to construct a quantum public-key cryptosystem, which is likely to withstand any attack of a quantum adversary.

19. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, and Shigeru Yamashita,:
"Quantum Identification of Boolean Oracles", Topics in Applied Physics, 102, 3-18, 2006.
概要: We introduce the Oracle Identification Problem (OIP), which includes many problems in oracle computation such as those of Grover search and Bernstein-Vazirani as its special cases. We give general upper and lower bounds on the number of oracle queries of OIP. Thus, our results provide general frameworks for analyzing the quantum query complexity of oracle computation. Our results are also related to exact learning in the computational learning theory.

20. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, and Shigeru Yamashita:
"Improved Algorithms for Quantum Identification of Boolean Oracles", Theoretical Computer Science, 378(1), 41-53, 2007.
概要: The oracle identification problem (OIP) was introduced by Ambainis et al. [A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R.H. Putra, S. Yamashita, Quantum identification of boolean oracles, in: Proc. of STACS'04, in: LNCS, vol. 2996, 2004, pp. 105-116]. It is given as a set S of M oracles and a blackbox oracle f. Our task is to figure out which oracle in S is equal to the blackbox f by making queries to f. OIP includes several problems such as the Grover Search as special cases. In this paper, we improve the algorithms in [A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R.H. Putra, S. Yamashita, Quantum identification of boolean oracles, in: Proc. of STACS'04, in: LNCS, vol. 2996, 2004, pp. 105-116] by providing a mostly optimal upper bound of query complexity for this problem: (i) For any or-

acle set S such that $|S| \leq 2^{N^d}$ $(d < 1)$, we design an algorithm whose query complexity is O(NlogM/ logN), matching the lower bound proved in [A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R.H. Putra, S. Yamashita, Quantum identification of boolean oracles, in: Proc. of STACS'04, in: LNCS, vol. 2996, 2004, pp. 105-116]. (ii) Our algorithm also works for the range between 2^{N^d} and $2^{N^{\log N}}$ (where the bound becomes $O(N)$), but the gap between the upper and lower bounds worsens gradually. (iii) Our algorithm is robust, namely, it exhibits the same performance (up to a constant factor) against noisy oracles as also shown in the literature [M. Adcock, R. Cleve, A quantum Goldreich-Levin theorem with cryptographic applications, in: Proc. of STACS'02, in: LNCS, vol. 2285, 2002, pp. 323-334; H. Buhrman, I. Newman, H. Rohrig, R. deWolf, Robust quantum algorithms and polynomials, in: Proc. of STACS'05, in: LNCS, vol. 3404, 2005, pp. 593-604; P. Hoyer, M. Mosca, R. de Wolf, Quantum search on bounded- error inputs, in: Proc. of ICALP'03, in: LNCS, vol. 2719, 2003, pp. 291-299] for special cases of OIP.

21. 河内 亮周:
"量子計算における整数格子問題へのアプローチ", 招待解説論文, 電子情報通信学会論文誌 A, J90-A(5), 376-384, 2007.
概要: 今まで計算困難と思われていた素因数分解・離散対数問題が量子計算機を使うと効率良く解けるというのは今となっては良く知られた事実である．一方，多くの研究者は NP 困難問題はさすがに量子計算でも効率良く解くことはできない，と予想しているようである．それでは，素因数分解・離散対数問題以外（特に数論的な問題以外）で，NP 困難ではなさそうで P（あるいは BPP）に入ることも知られていない問題に対して量子計算は有効であるのか？というのは自然な疑問であろう．本稿ではその代表として整数格子にまつわるいくつかの問題に関して量子計算の分野でどのような進展があるのか，アルゴリズム，暗号，計算量理論の観点から解説したい．

22. T. Hofmeister, U. Schoening, R. Schuler, and O. Watanabe:
"Randomized algorithms for 3-SAT", Theory of Comput. Systems, 40, 249-262, 2007.
概要: SAT 問題に対して，最悪時時間計算量の改善を行った．具体的には，まず，3-SAT 問題に対し，これまでの変数数 n に対する最悪時計算時間 $O(1.333^n)$ の乱択アルゴリズムに対し，最悪時計算時間が $O(1.330^n)$ のアルゴリズムを設計した．一方，一般の SAT 問題に対しては，決定性アルゴリズムを考え，これまでの最悪時計算時間 $O(1.239^m)$ のアルゴリズム（ただし m は論理式の節数）に対し，$O(1.234^m)$ のアルゴリズムを提案した．

研究会等

1. K. Hatano and O. Watanabe:
"Learning r-of-k functions by boosting", 15th International Conference on Algorithmic Learning Theory (ALT 2004), Lecture Notes in Computer Science 3244, 114-126, 2004.
概要: We investigate further improvement of boosting in the case that the target concept belongs to the class of r-of-k threshold Boolean functions, which answers "+1" if at least r of k relevant variables are positive, and answers "−1" otherwise. Given m examples of a r-of-k function and literals as base hypotheses, popular boosting algorithms (e.g., AdaBoost) construct a consistent final hypothesis in $O(k^2 \log m)$ iterations. While this convergence speed is tight in general, we show that a modification of AdaBoost (confidence-rated AdaBoost or InfoBoost) can make use of the property of r-of-k functions that make less error on one-side to find a consistent final hypothesis in $O(kr \log m)$ iterations. Our

result extends the previous investigation by Hatano and Warmuth and gives more general examples where confidence-rated AdaBoost or InfoBoost has an advantage over AdaBoost.

2. J.Y. Cai and O. Watanabe:
"Random access to advice strings and collapsing results", Proceedings of the Fifteenth International Symposium on Algorithms and Computation (ISAAC 2004), Lecture Notes in Computer Science 3341, 209-220, 2004.
概要: We propose a model of computation where a Turing machine is given random access to an advice string. With random access, an advice string of exponential length becomes meaningful for polynomially bounded complexity classes. We compare the power of complexity classes under this model. It gives a more stringent notion than the usual model of computation with relativization. Under this model of random access, we prove that there exist advice strings such that the Polynomial-time Hierarchy PH and Parity Polynomial-time parityP all collapse to the class P. Our main proof technique uses the decision tree lower bounds for constant depth circuits of Hastad etal and the algebraic machinery of Razborov and Smolensky.

3. Kazuo Iwama and Akinori Kawachi:
"Approximated Two Choices in Randomized Load Balancing", Proceedings of the Fifteenth International Symposium on Algorithms and Computation (ISAAC 2004), Lecture Notes in Computer Science 3341, 545-557, 2004.
概要: This paper studies the maximum load in the *approximated d-* choice balls-and-bins game where the current load of each bin is available only approximately. In the model of this game, we have r thresholds $T_1, ..., T_r$ $(0 < T_1 < \cdots < T_r)$ for an integer r (≥ 1). For each ball, we select d bins and put the ball into the bin of the lowest range, i.e., the bin of load i such that $T_k \leq i \leq T_{k+1} - 1$ and no other selected bin has height less than T_k. If there are two or more bins in the lowest range (i.e., their height is between T_k and $T_{k+1} - 1$), then we assume that those bins cannot be distinguished and so one of them is selected uniformly at random. We then estimate the maximum load for n balls and n bins in this game. In particular, when we put the r thresholds at a regular interval of an appropriate Δ, i.e., $T_r - T_{r-1} = \cdots = T_2 - T_1 = T_1 = \Delta$, the maximum load $L(r)$ is given as $(r + O(1)) \sqrt[r+1]{\frac{r+1}{(d-1)^r} \ln n / \ln\left(\frac{r+1}{(d-1)^r} \ln n\right)}$. The bound is also described as $L(\Delta) \leq \{(1+o(1)) \ln\ln n + O(1)\}\Delta / \ln((d-1)\Delta)$ using parameter Δ. Thus, if Δ is a constant, this bound matches the (tight) bound in the original d-choice model given by Azar et al., within a constant factor. The bound is also tight within a constant factor when $r = 1$.

4. Akinori Kawachi, Hirotada Kobayashi, Takeshi Koshiba, and Raymond H. Putra:
"Universal Test for Quantum One-Way Permutations", Proceedings of the Twenty-Ninth International Symposium on Mathematical Foundations of Computer Science (MFCS 2004), Lecture Notes in Computer Science 3153, 839-850, 2004.
概要: The next bit test was introduced by Blum and Micali and proved by Yao to be a universal test for cryptographic pseudorandom generators. On the other hand, no universal test for the cryptographic one-wayness of functions (or permutations) is known, though the existence of cryptographic pseudorandom generators is equivalent to that of cryptographic one-way functions. In the quantum computation model, Kashefi, Nishimura and Vedral gave a sufficient condition of (cryptographic) quantum

one-way permutations and conjectured that the condition would be necessary. In this paper, we relax their sufficient condition and give a new condition that is necessary and sufficient for quantum one-way permutations. Our condition can be regarded as a universal test for quantum one-way permutations, since our condition is described as a collection of stepwise tests similar to the next bit test for pseudorandom generators.

5. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Hiroyuki Masuda, Raymond H. Putra, and Shigeru Yamashita:
"Quantum Identification of Boolean Oracles", Proceedings of the Twenty-First Symposium on Theoretical Aspects of Computer Science (STACS 2004), Lecture Notes in Computer Science 2996, 105-116, 2004.
概要: The oracle identification problem (OIP) is, given a set S of M Boolean oracles out of 2^N ones, to determine which oracle in S is the current black-box oracle. We can exploit the information that candidates of the current oracle is restricted to S. The OIP contains several concrete problems such as the original Grover search and the Bernstein-Vazirani problem. Our interest is in the quantum query complexity, for which we present several upper bounds. They are quite general and mostly optimal: (i) The query complexity of OIP is $O(\sqrt{N \log M \log N} \log\log M)$ for *any* S such that $M = |S|N$, which is better than the obvious bound N if $M < 2^{N/\log^3 N}$. (ii) It is $O(\sqrt{N})$ for *any* S if $|S| = N$, which includes the upper bound for the Grover search as a special case. (iii) For a wide range of oracles ($|S| = N$) such as random oracles and balanced oracles, the query complexity is $O(\sqrt{N/K})$, where K is a simple parameter determined by S.

6. O. Watanabe:
"Pseudo expectation: A tool for analyzing local search algorithms", Statistical Physics of Disordered Systems and its Applications (SPDSA2004), July, 2004.
概要: Watanabe et. al. proposed pseudo expectation for analyzing relatively simple Markov processes, which would be often seen as simple execution models of local search algorithms. In this paper, we first explain how it is used, and then investigate the approximation error bound of pseudo expectations.

7. 新倉 康明, J. Schneider, 渡辺 治.:
"単純な規則で表されるマルコフ過程の近似解析手法", アルゴリズム研, 情処研報 AL94, 73-80, 2004.
概要: 本稿では，単純で比較的状態数の大きなマルコフ過程のモデルを設定し，その平均的な状態遷移を，簡単な計算 (これを疑似平均と呼ぶことにする) で近似する手法を提案する．乱択アルゴリズムの動きは，マルコフ過程のモデルで近似することができる場合がある．しかし，マルコフ過程としても状態空間が大きくなるために，その平均的な振る舞いの解析が非常に困難になる場合が多い．そのような解析を簡単な計算で行うための道具が疑似平均である．本稿では，幾つかの実験と解析を通して，疑似平均の近似性能について考察する．

8. R. Hayashi and K. Tanaka:
"The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity", PKC 2005—The 8th International Workshop on Practice and Theory in Public Key Cryptography, Lecture Notes in Computer Science 3386, 216-233, January, 2005.
概要: We say that an encryption scheme or a signature scheme provides anonymity when it is infeasible to determine which user generated a ciphertext or a signature. To construct the schemes with anonymity,

it is necessary that the space of ciphertexts or signatures is common to each user. In this paper, we focus on the techniques which can be used to obtain this anonymity property, and propose a new technique for obtaining the anonymity property on RSA-based cryptosystem, which we call "sampling twice." It generates the uniform distribution over $[0, 2^k)$ by sampling the two elements from $\mathbb{Z}_N$ where $|N| = k$. Then, by applying the sampling twice technique, we construct the schemes for encryption, undeniable and confirmer signature, and ring signature, which have some advantage to the previous schemes.

9. 鈴木学, 田中圭介:
"ランダムオラクルモデルを用いたプロトコルの指標と方式", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 1, 151-156, 2005 年 1 月.
概要: A study of the random oracle model seems to be concentrated to showing the gap between the schemes in the random oracle model and the schemes whose random oracles are replaced with functions chosen at random from some function ensembles. We consider a different direction on the study of the schemes in the random oracle model. We focus on the size of the tables necessary to describe all of the entries to be potentially queried in the random oracle model. We show how to reduce the table sizes of the schemes for encryption and signature in the random oracle model. In particular, we apply this idea to PSS-R and OAEP and show the security of our schemes.

10. 金内志津, 田中圭介:
"Computational Bilinear Diffie-Hellman 問題に基づく複数キーワード検索つき公開鍵暗号方式", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 1, 343-348, 2005 年 1 月.
概要: Park, Kim, and Lee proposed a public-key encryption with conjunctive field keyword search (PECK). They proposed two constructions for PECK based on the Decisional Bilinear Diffie-Hellman problem. We construct a variant of one of their schemes based on the Computational Bilinear Diffie-Hellman problem.

11. 樋渡玄良, 田中圭介:
"Cramer-Shoup の構成法による平方剰余問題と関連する暗号方式", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 2, 481-486, 2005 年 1 月.
概要: At Eurocrypt '02 Cramer and Shoup proposed a general paradigm to construct practical public-key cryptosystems secure against the adaptive chosen ciphertext attack as well as several concrete examples. Using the construction, we present a new variant of the Cramer-Shoup encryption scheme, secure against the adaptive chosen ciphertext attack. Our variant is based on the problem related to the quadratic residuosity (QR). They also proposed the encryption scheme based on the QR, but this scheme is less efficient than those based on the decision Diffie-Hellman problem or the decision composite residuosity. In this paper, we define the new assumptions related to the QR assumption and propose a new public-key encryption scheme whose security is based on the new assumption. Our scheme is more efficient than the QR-based scheme proposed by Cramer and Shoup.

12. 小野寺貴男, 田中圭介:
"中程度の難しさをもつ関数のモデルと方式", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 2, 799-804, 2005 年 1 月.
概要: Moderately-hard functions are useful for many applications and there are quite many papers concerning on moderately-hard functions. However, the formal model for moderately-hard functions have not

been proposed. In this paper, first, we propose the formal model for moderatelyhard functions. For this purpose, we construct the computational model and investigate the properties desired for moderately-hard functions. Then, we propose that some particular functions can be used as moderately-hard functions. These functions are based on two ideas: the difficulty of factoring $p^r q$ and sequential computation of primitive functions.

13. 羽田大樹, 田中圭介:
"認証付き鍵交換プロトコルにおける non-malleability に基づく安全性", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 3, 1087-1092, 2005 年 1 月.
概要: This paper continues the study of password-based protocols for authenticated key exchange (AKE). In 2000, Bellare, Pointcheval, and Rogaway proposed the formal model on AKE. In this paper, we propose the new security notions on AKE, based on the non-malleability of session keys. Then we prove that this security notion is equivalent to that proposed by Bellare, Pointcheval, and Rogaway. Furthermore, we show that there is a protocol secure in the random oracle model not always secure in the standard model with collision-resistant hash functions.

14. 林良太郎, 田中圭介:
"ElGamal 暗号と Cramer-Shoup 暗号をもとにした匿名性を持つ暗号方式", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 3, 1315-1320, 2005 年 1 月.
概要: In this paper, we have proposed new variants of the ElGamal and the Cramer-Shoup encryption schemes. Our schemes have the anonymity property even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime. More precisely, our ElGamal variants provide anonymity against the chosen-plaintext attack, and our Cramer-Shoup variants provide anonymity against the adaptive chosen-ciphertext attack. These anonymity properties are proved under a slightly weaker assumption than the DDH assumption. Furthermore, our ElGamal variants are secure in the sense of IND-CPA, and our Cramer-Shoup variants are secure in the sense of IND-CCA2.

15. 林良太郎, 田中圭介:
"匿名性をもつ RSA 暗号方式のための Sampling Twice テクニック", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 3, 1321-1326, 2005 年 1 月.
概要: We say that an encryption scheme or a signature scheme provides anonymity when it is infeasible to determine which user generated a ciphertext or a signature. To construct the schemes with anonymity, it is necessary that the space of ciphertexts or signatures is common to each user. In this paper, we focus on the techniques which can be used to obtain this anonymity property, and propose a new technique for obtaining the anonymity property on RSA-based cryptosystem, which we call "sampling twice." It generates the uniform distribution over $[0, 2^k)$ by sampling the two elements from $\mathbb{Z}_N$ where $|N| = k$. Then, by applying the sampling twice technique, we construct the schemes for encryption, undeniable and confirmer signature, and ring signature, which have some advantages to the previous schemes.

16. 三原章裕, 田中圭介:
"指定検証者署名への変換が可能な Aggregate Signature", 2005 年 暗号と情報セキュリティシンポジウム (SCIS2005), 3, 1453-1458, 2005 年 1 月.
概要: There is a signature scheme which can aggregate two or more persons ' signatures to one, called an aggregate signature. In this paper, we propose a scheme

of an aggregate signature which has additional functionality allowing any holder of a signature to designate the signature to any desired designated-verifier. By this functionality, no one other than the designated-verifier can verify the signature, so the signature passed to other persons would not appear where the signer does not intend to send it in the form which anyone can verify.

17. A. Kawachi, T. Koshiba, H. Nishimura, T. Yamakami:
"Computational Indistinguishability between Quantum States and Its Applications", Advances in Cryptography – Eurocrypt 2005, Lecture Notes in Computer Science 3494, 268-284, May, 2005.
概要: ある二つの量子状態の識別問題が (i) 落とし戸を持つ，(ii) 平均時の困難性が最悪時の困難性と等価である，(iii) 最悪時の困難性が少なくともグラフ自己同型性判定問題の最悪時困難性と同等かそれ以上である，という三つの暗号論的性質を満たすことを証明した．さらに，この識別問題をもとにして，量子公開鍵暗号系を提案した．この公開鍵暗号系における暗号の解読は少なくともグラフ自己同型性判定問題を解くことと同等かそれ以上に難しいことが証明可能であるため，現在知られている量子計算機上のアルゴリズムでは解読困難であるといえる．

18. H. Hada and K. Tanaka:
"Security for Authenticated Key Exchange Based on Non-Malleability", International Conference on Information Technology and Applications (ICITA 2005), vol. 2, 508-513, July, 2005.
概要: This paper continues the study of password-based protocols for authenticated key exchange (AKE). In 2000, Bellare, Pointcheval, and Rogaway proposed the formal model on AKE. In this paper, we propose new security notions on AKE, based on the non-malleability of session keys. Then we prove that those security notion are equivalent to that proposed by Bellare, Pointcheval, and Rogaway. Furthermore, we show that there is a protocol secure in the random oracle model, not always secure in the standard model with collision-resistant hash functions.

19. A. Mihara and K. Tanaka:
"Universal Designated-Verifier Signature with Aggregation", International Conference on Information Technology and Applications (ICITA 2005), vol. 2, 514-519, July, 2005.
概要: There is a signature scheme which can aggregate two or more persons' signatures to one, called an aggregate signature. In this paper, we propose a scheme of an aggregate signature which has additional functionality allowing any holder of a signature to designate the signature to any desired designated-verifier. By this functionality, no one other than the designated-verifier can verify the signature, so the signature passed to other persons would not appear where the signer does not intend to send it in the form which anyone can verify.

20. T. Isshiki and K. Tanaka:
"An $(n-t)$-out-of-n Threshold Ring Signature Scheme", Information Security and Privacy – 10th Australasian Conference (ACISP 2005), Lecture Notes in Computer Science 3574, 406-416, July, 2005.
概要: In CRYPTO2002, Bresson, Stern, and Szydlo proposed a threshold ring signature scheme. Their scheme uses the notion of fair partition and is provably secure in the random oracle model. Their scheme is efficient when the number t of signers is small compared with the number n of group members, i.e., $t = O(\log n)$ (we call this scheme BSS scheme). However, it is inefficient when t is $\omega(\log n)$. In this paper, we propose a new threshold ring signature scheme which is efficient when the number

of signers is large compared with the number n of group members, i.e., when the number t of non-signers in the group members is small compared with n. This scheme is very efficient when $t = O(\log n)$. This scheme has a kind of dual structure of BSS scheme which is inefficient when the number of signers is large compared with the number of group members. In order to construct our scheme, we modify the trap-door one-way permutations in the ring signature scheme, and use the combinatorial notion of fair partition. This scheme is provably secure in the random oracle model.

21. R. Hayashi and K. Tanaka:
"Universally Anonymizable Public-Key Encryption", Advances in Cryptology – ASIACRYPT 2005, Lecture Notes in Computer Science 3788, 293-312, December, 2005.
概要: We first propose the notion of universally anonymizable public-key encryption. Suppose that we have the encrypted data made with the same security parameter, and that these data do not satisfy the anonymity property. Consider the situation that we would like to transform these encrypted data to those with the anonymity property without decrypting these encrypted data. In this paper, in order to formalize this situation, we propose a new property for public-key encryption called universal anonymizability. If we use a universally anonymizable public-key encryption scheme, not only the person who made the ciphertexts, but also anyone can anonymize the encrypted data without using the corresponding secret key. We then propose universally anonymizable public-key encryption schemes based on the ElGamal encryption scheme, the Cramer-Shoup encryption scheme, and RSA-OAEP, and prove their security.

22. O. Watanabe:
"Some heuristic analysis of local search algorithms for SAT problems", 3rd International Symposium on Stochastic Algorithms, Foundations and Applications (SAGA 2005), Lecture Notes in Computer Science 3777, 14-24, October, 2005.
概要: SAT 問題群（一般の SAT 問題とその変形版）に対する局所探索法に関しては，様々な実験的な研究が行われているが，理論的な解析は少ない．我々は，アルゴリズムの「平均的なよさ」を解析するために，アルゴリズムの「平均的な実行」を追う手法を研究してきたが，その手法を SAT 問題群の局所探索法に応用した．その結果，(i) 局所探索法が成功する場合の理由を準理論的に示すことができた．さらに，(ii) SAT 問題群の中でも，局所探索法に対する相性に差があること，(iii) タブー探索の効果，なども明らかにすることができた．

23. M. Yamamoto:
"An improved $\widetilde{\mathcal{O}}(1.234^m)$-time deterministic algorithm for SAT", 16th International Symposium on Algorithms and Computation (ISAAC'05), Lecture Notes in Computer Science 3827, 644-653, December, 2005.
概要: SAT 問題に対して，最悪時時間計算量の改善を行った．具体的には，まず，3SAT 問題に対し，これまでの変数数 n に対する最悪時計算時間 $O(1.333^n)$ の乱択アルゴリズムに対し，最悪時計算時間が $O(1.330^n)$ のアルゴリズムを設計した．一方，一般の SAT 問題に対しては，決定性アルゴリズムを考え，これまでの最悪時計算時間 $O(1.239^m)$ のアルゴリズム（ただし m は論理式の節数）に対し，$O(1.234^m)$ のアルゴリズムを提案した．

24. S. Toda:
"Computing Automorphism Groups of Chordal Graphs Whose Simplicial Components Are Of Small Size", 電子情報通信学会コンピュテーション研究会, IEICE Technical Report, Vol. 105, No.144, COMP2005-24,

37–42, June, 2005.

概要: It is known that any chordal graph can be uniquely decomposed into simplicial components. Based on this fact, it is shown that for a given chordal graph, its automorphism group can be computed in $O((c! \cdot n)^{O(1)})$ time, where c denotes the maximum size of simplicial components and n denotes the number of nodes. It is also shown that isomorphism of those chordal graphs can be decided within the same time bound. From the viewpoint of polynomial-time computability, our result strictly strengthens the previous ones respecting the clique number.

25. M. Yamamoto:
"An improved $\widetilde{\mathcal{O}}(1.234^m)$-time deterministic algorithm for SAT", 電子情報通信学会 コンピュテーション研究会, 信学技報, Vol. 105, No. 499, COMP2005-54, 37–42, December, 2005.

概要: SAT 問題に対して，最悪時時間計算量の改善を行った．具体的には，まず，3SAT 問題に対し，これまでの変数数 n に対する最悪時計算時間 $O(1.333^n)$ の乱択アルゴリズムに対し，最悪時計算時間が $O(1.330^n)$ のアルゴリズムを設計した．一方，一般の SAT 問題に対しては，決定性アルゴリズムを考え，これまでの最悪時計算時間 $O(1.239^m)$ のアルゴリズム（ただし m は論理式の節数）に対し，$O(1.234^m)$ のアルゴリズムを提案した．

26. M. Halldorsson, O. Watanabe, and M. Yamamoto:
"An improved upper bound for the three domatic number problems", 第 7 回情報科学技術フォーラム, 情報処理学会・電気情報通信学会, 2006.

概要: In this paper we consider the domatic number problem. For this problem, Tiege, etal [RRSY06] recently proposed a deterministic algorithm solving this problem, and they proved that it runs in $O(2.6949^n)$-time for any graph with n vertices. Here we give a better bound $O(2.6834^n)$ for the same algorithm.

27. 林良太郎, 田中圭介:
"Relationships between Data-Privacy and Key-Privacy", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 1A2-1, 2006 年 1 月.

概要: The classical security requirement of public-key encryption schemes is that it provides privacy of the encrypted data. Popular formalizations such as one-wayness (OW) or indistinguishability (IND) are directed at capturing various data-privacy requirements. Bellare, Boldyreva, Desai, and Pointcheval proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity" (IK, which means "indistinguishability of keys."). It asks that an encryption scheme provides privacy of the key under which the encryption was performed. That is, if an encryption scheme provides the key-privacy, then the receiver is anonymous from the point of view of the adversary. Related to this security notion, Halevi provided a simple sufficient condition (which we denote IKR) and he showed IND $\wedge$ IKR implies IK. Hayashi and Tanaka modified the definition by Bellare, Boldyreva, Desai, and Pointcheval, and proposed a new definition of the anonymity property, which we call the strong anonymity (sIK). In this paper, we show the relationships between data-privacy (IND, OW) and key-privacy (IK, IKR, sIK). For example, we show that wIK does not imply OW, but sIK implies not only OW but IND. We also show that sIK is equivalent to IND $\wedge$ IKR, while IK is weaker than IND $\wedge$ IKR.

28. 林良太郎, 田中圭介:
"Generic Conversion for the Anonymity against the Adaptive Chosen Ciphertext Attack", 2006 年 暗号と情報セキュリティシ

ンポジウム (SCIS2006), 1F3-1, 2006年1月.
概要: Bellare, Boldyreva, Desai, and Pointcheval proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity." It asks that an encryption scheme provides privacy of the key under which the encryption was performed. That is, if an encryption scheme provides the key-privacy, then the receiver is anonymous from the point of view of the adversary. They formalized the property of anonymity, and this can be considered under either the chosen plaintext attack or the adaptive chosen ciphertext attack, yielding two notions of security, IK-CPA and IK-CCA. In this paper, we propose the notion of plaintext awareness in the two-key setting, called PA2. We say that the public-key encryption scheme is secure in the sense of PA2 if the scheme is secure in the sense of IK-CPA and there exists a knowledge extractor for PA2. There are some differences between the definition of knowledge extractor for PA and that for PA2. We also prove that if a public-key encryption scheme is secure in the sense of PA2, then it is also secure in the sense of IK-CCA. Since it looks much easier to prove that a public-key encryption scheme is secure in the sense of PA2 than to prove directly it is secure in the sense of IK-CCA, the notion of PA2 is useful to prove the anonymity property of public-key encryption schemes. We also propose the first generic conversion for the anonymity, that is, we prove that the Fujisaki- Okamoto conversion, where basic public-key encryption scheme is secure in the sense of IK-CPA, is secure in the sense of IK-CCA in the random oracle model.

29. 林良太郎, 田中圭介:
"Universally Anonymizable Public-Key Encryption", 2006年 暗号と情報セキュリティシンポジウム (SCIS2006), 1F3-2, 2006年1月.
概要: We first propose the notion of universally anonymizable public-key encryption. Suppose that we have the encrypted data made with the same security parameter, and that these data do not satisfy the anonymity property. Consider the situation that we would like to transform these encrypted data to those with the anonymity property without decrypting these encrypted data. In this paper, in order to formalize this situation, we propose a new property for public-key encryption called universal anonymizability. If we use a universally anonymizable public-key encryption scheme, not only the person who made the ciphertexts, but also anyone can anonymize the encrypted data without using the corresponding secret key. We then propose universally anonymizable public-key encryption schemes based on the ElGamal encryption scheme, the Cramer-Shoup encryption scheme, and RSA-OAEP, and prove their security.

30. 金内志津, 田中圭介:
"Signcryption with Batch Verification", 2006年 暗号と情報セキュリティシンポジウム (SCIS2006), 2A3-4, 2006年1月.
概要: Signcryption is a public-key cryptographic method that performs encryption and signature in a single logical step. It is more efficient than running the sign algorithm and the encryption algorithm separately. In this paper, we propose the signcryption with batch verification. Using batch verification in the de-signcryption algorithm of the signcryption, we improve the efficiency of the verification of the plural signcrypted messages. We also give the proofs of the security property: the chosen ciphertext security against insider attack, the unforgeability against chosen-message attack, and the ciphertext anonymity.

31. 草川恵太，河内亮周，田中圭介:
"Multi-Bit Cryptosystems based on Lattice Problems", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 2A4-4, 2006 年 1 月.
概要: We propose multi-bit versions of several single-bit cryptosystems based on lattice problems, Ajtai and Dwork Cryptosystem [STOC '97] and its error-free version (Goldreich, Goldwasser, and Halevi [CRYPTO '97]), Regev Cryptosystems [STOC 2003] and [STOC 2005], and Ajtai Cryptosystem [STOC 2005]. By analyzing trade-offs between hardness of their underlying lattice problems and probability of decryption errors, it is shown that our cryptosystems encrypt $O(\log n)$-bit plaintexts into ciphertexts of the same length as the original ones with reasonable sacrifices of the hardness of the underlying lattice problems.

32. 八代正俊，田中圭介:
"Analysis of the Waseda-Soshi-Miyaji scheme and on Quantum Computation Signature", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 3C2-1, 2006 年 1 月.
概要: Several knapsack-based public-key encryption schemes were proposed, however the knapsack-based signature schemes are few. Shamir scheme is based on linear transformation. This scheme is broken without the quantum computer. Okamoto, Tanaka and Uchiyama proposed the definition of a quantum computation digital signature scheme. Waseda, Soshi and Miyaji proposed a knapsack-based quantum computation digital signature scheme based on the OTU. Their scheme is based on the signed knapsack problem. In this paper, we analyse the Waseda-Soshi-Miyaji scheme, they claimed that there scheme is secure. In fact, the forger can determine the signer's private key. Therefore we discuss on the possibillity of the construction for quantum computation digital signature scheme based on the knapsak problems.

33. 大山千尋，田中圭介:
"Universal Designated-Verifier Ring Signature", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 3A3-2, 2006 年 1 月.
概要: In this paper, we propose new variant of ring signature called universal designatedverifier ring signature (UDVRS). Like universal designated-verifier signature (UDVS), UDVRS has special functionality that allows any holder of a ring signature, who is not necessarily the signer, to designate the signature to any desired designated-verifier, using the verifier's public key. Only the designated-verifier can verify the signature and be convinced that the signature was signed by one of the ring members: he cannot transfer any conviction to the third party. The purpose of our UDVRS scheme is to allow only a specified entity to verify the ring signature, which keeps the signature from being used beyond the signer's aim.

34. 羽田大樹，田中圭介:
"A Password-Based Authenticated Key Exchange Protocol in the Three Party Setting", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 3D3-2, 2006 年 1 月.
概要: In this paper, we continue the study of password-based authenticated key exchange in the three-party setting. Abdalla, Fouque, and Pointcheval contributed the model in the three-party and a generic construction of the protocol. Their protocol is very generic and natural, but assumes twoparty password-based authenticated key exchange, three-party key distribution, message authentication code (MAC), and the decisional Diffie-Hellman problem. Moreover it needs many rounds.

We present a specific protocol in their setting which needs only four rounds, and assume the decisional Diffie-Hellman problem in the random oracle model.

35. 樋渡玄良，田中圭介:
"Fair Exchange of Signatures in the Many-to-One Model", 2006年 暗号と情報セキュリティシンポジウム (SCIS2006), 3A4-4, 2006年1月.
概要: In 2004, Chen, Kudla, and Paterson introduced the concept of concurrent signature. The concurrent signature scheme falls just short of providing a full solution to the problem of fair exchange of signatures, however their schemes require neither a trusted third party nor a high degree of interaction between parties, so this is useful in some situations. They also proposed a protocol only for the one-to-one model. We extend this scheme to the many-to-one model. Consider the situation that a single party A wants to get the all signatures of three parties, B, C, and D, participated in the protocol, while these parties want to get only the signature of the party A. We propose a security model for the concurrent signature scheme applied to the many-to-one model. We also propose a concrete scheme which is secure. By putting an assumption that one party is honest-but-curious, we prove the security in the random permutation model under the discrete logarithm assumption. Our proposed scheme can be applied to the above situation.

36. 鈴木学，一色寿幸，田中圭介:
"Sanitizable Signature with Secret Information", 2006年 暗号と情報セキュリティシンポジウム (SCIS2006), 4A1-2, 2006年1月.
概要: A sanitizable signature scheme is a signature scheme that allows the sanitizer to sanitize certain portions of the document and to generate the valid signature of the resulting document with no interaction with the signer. There exist many models and schemes for sanitizable signature. In this paper, we precisely formalize the algorithms and the security requirements of sanitizable signature with secret information. We propose a sanitizable signature scheme based on the gap co-Diffie-Hellman groups and prove that our scheme satisfies these security requirements. Furthermore, we discuss various models of sanitizable signature and classify the previously proposed schemes and our scheme.

37. 山下直之，田中圭介:
"Secret Handshake with Multiple Groups", 2006年 暗号と情報セキュリティシンポジウム (SCIS2006), 4D2-3, 2006年1月.
概要: Recently, a privacy-preserving authentication model called secret handshake was introduced by Balfanz, Durfee, Shankar, Smetters, Staddon, and Wong. It allows two members of a same group to authenticate each other whether they belong to a same group or not secretly, in the sense that each party reveals his affiliation to the other only if the other party is also a group member. Xu and Young constructed the first scheme that achieved this property. Previous works focus on the models which each participant authenticates himself as a member of one group. In our study, we present a new secret handshake model. In our model, two users authenticate each other if and only if each one's memberships of the groups are equal. In this paper, we present a definition of this model. We call this model secret handshake with multiple groups and produce a concrete scheme. Furthermore, our scheme can deal with one's change of memberships. Even if a member is added to a new group, or is deleted from the one that he belongs to, there is no need to change his other memberships. Our scheme does not satisfy the unlinkability, but that can be achieved by modifying

our scheme.

38. 渡辺治，山本真基:
“A message passing algorithm for MAX2SAT”，電子情報通信学会全国大会, COMP-NHC 学生シンポジウム, DS-1-6, March, 2006.
概要: MAX-SAT 問題の難しさの平均的な解析をする際，問題例の分布に対する確率モデルが必要である．これまで，そのような確率モデルとして妥当なものがなかったが，我々は，MAX-2SAT 問題に対して，まず，テスト例題生成，という観点から問題例生成の手法を提案した．さらに，それを単純化して，MAX-2SAT 問題の問題例に対する自然な確率分布を提案することができた．さらに，上記の分布のもとでの MAX-2SAT 問題の難しさの解析を目的とし，我々は，その分布に対して比較的よい性能を持ち，線形時間のアルゴリズムを考案した．これは，人工知能の研究で開発された「信念伝播法」という手法にヒントを得て，それを非常に単純化したアルゴリズムである．このアルゴリズムが，上記の分布の元で，MAX-2SAT 問題を高い確率で解くことを証明した．

39. Ryotaro Hayashi and Keisuke Tanaka:
“PA in the Two-Key Setting and a Generic Conversion for Encryption with Anonymity”, Information Security and Privacy - 11th Australasian Conference, ACISP 2006, Lecture Notes in Computer Science 4058, 271-282, July, 2006.
概要: We propose the notion of plaintext awareness in the two-key setting, called PATK. We also prove that if a public-key encryption scheme is secure in the sense of PATK, then it is also secure in the sense of IK-CCA. Since it looks much easier to prove that a public-key encryption scheme is secure in the sense of PATK than to prove directly that it is secure in the sense of IK-CCA, the notion of PATK is useful to prove the anonymity property of public-key encryption schemes. We also propose the first generic conversion for the anonymity, that is, we prove that the public-key encryption scheme derived from the Fujisaki-Okamoto conversion scheme, where the basic public-key encryption scheme is secure in the sense of IK-CPA, is secure in the sense of IK-CCA in the random oracle model.

40. Akinori Kawachi and Tomoyuki Yamakami:
“Quantum Hardcore Functions by Complexity-Theoretical Quantum List Decoding”, 33rd International Colloquium on Automata, Languages and Programming (ICALP 2006), Lecture Notes in Computer Science 4052, 216-227, 2006.
概要: We present three new quantum hardcore functions for any quantum one-way function. We also give a quantum solution to Damgård's question (CRYPTO'88) on his pseudorandom generator by proving the quantum hardcore property of his generator, which has been unknown to have the classical hardcore property. Our technical tool is quantum list-decoding of “classical” error-correcting codes (rather than “quantum” error-correcting codes), which is defined on the platform of computational complexity theory and cryptography (rather than information theory). In particular, we give a simple but powerful criterion that makes a polynomial-time computable code (seen as a function) a quantum hardcore for any quantum one-way function. On their own interest, we also give quantum list-decoding algorithms for codes whose associated quantum states (called codeword states) are nearly orthogonal using the technique of pretty good measurement.

41. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, and Shigeru Yamashita:
“Improved Algorithms for Quantum Identification of Boolean Oracles”, 10th Scan-

dinavian Workshop on Algorithm Theory (SWAT 2006), Lecture Notes in Computer Science 4059, 280-291, 2006.

概要: The oracle identification problem (OIP) was introduced by Ambainis et al. It is given as a set S of M oracles and a blackbox oracle f. Our task is to figure out which oracle in S is equal to the blackbox f by making queries to f. OIP includes several problems such as the Grover Search as special cases. In this paper, we improve the algorithms of Ambainis et al. by providing a mostly optimal upper bound of query complexity for this problem: (i) For any oracle set S such that $|S| \leq 2^{N^d}$ ($d < 1$), we design an algorithm whose query complexity is $O(\sqrt{N \log M / \log N})$, matching the lower bound proved in 2004. (ii) Our algorithm also works for the range between 2^{N^d} and $2^{N/\log N}$ (where the bound becomes $O(N)$), but the gap between the upper and lower bounds worsens gradually. (iii) Our algorithm is robust, namely, it exhibits the same performance (up to a constant factor) against the noisy oracles as also shown in the literatures for special cases of OIP.

42. J. Cai and O. Watanabe:
"Stringent relativization: a new approach for studying complexity classes", SIGACT News, Vol. 37, Dec. Issue (#140), 2006.

概要: A new notion of relativization—stringent relativization—has been proposed recently for discussing collapsing relations of complexity classes, with which we hope to open a new approach for studying complexity classes. Starting with the motivation of this notion, we discuss the meaning and implication of collapsing relations under the stringent relativization.

43. O. Watanabe and M. Yamamoto:
"Average-case analysis for the MAX-2SAT problem", 9th International Conference on Theorem and Application of Satisfiability Testing (SAT'06), Lecture Notes in Computer Science 4142, 277-282, 2006.

概要: We propose a "planted solution model" for discussing the average-case complexity of the MAX-2SAT problem. We show that for a large range of parameters, the planted solution (more precisely, one of the planted solution pair) is the optimal solution for the generated instance with high probability. We then give a simple linear time algorithm based on a message passing method, and we prove that it solves the MAX-2SAT problem with high probability under our planted solution model.

44. M. Onsjoe and O. Watanabe:
"A simple message passing algorithm for graph partition problem", 17th International Symposium on Algorithms and Computation (ISAAC'06), Lecture Notes in Computer Science 4288, 507-516, 2006.

概要: Motivated by the belief propagation, we propose a simple and deterministic message passing algorithm for the Graph Bisection problem and related problems. The running time of the main algorithm is linear w.r.t. the number of vertices and edges. For evaluating its average-case correctness, planted solution models are used. For the Graph Bisection problem under the standard planted solution model with probability parameters p and r, we prove that our algorithm yields a planted solution with probability $1 - \delta$ if $p - r = \Omega(n^{-1/2} \log(n/\delta))$.

45. 戸田誠之助:
"コーダルグラフに関する同型性判定のための単純なアルゴリズム", コンピュテーション研究会, 信学技報, vol. 106, no. 29, COMP2006-8, 57-62, 2006 年 4 月.

概要: 筆者による以前の研究 (IEICE Technical Report, COMP2005-24; IEICE Transactions on Information and Systems, August 2006) において, コーダルグラフの自己同型群を求めるためのアルゴリズムを設計し, そ

れを利用することによって同型性も判定できることを示した．しかし，そこでは群論的手法を多用しており，複雑で時間量の解析も困難であった．さらに，自己同型群のもとで不変な木表現（s-木）が構成可能であるといった事実以外には，コーダルグラフに関する様々な性質をまったく利用していないものになっていた（注：これは群論的手法を多用しているためである）．そこで，コーダルグラフの性質をうまく利用することによって，より単純なアルゴリズムを設計できるのではないかということが素直な疑問として残されていた．本研究では，この疑問に答えるために，アルゴリズム設計のための指針を与える．

46. Akinori Kawachi, Hirotada Koabashi and Masahito Hayashi:
"Quantum Measurements for Hidden Subgroup Problems with Optimal Sample Complexity", preprint, quant-ph/06041724, 2006.
概要: One of the central issues in the hidden subgroup problem is to bound the sample complexity, i.e., the number of identical samples of coset states sufficient and necessary to solve the problem. In this paper, we present general bounds for the sample complexity of the identification and decision versions of the hidden subgroup problem. As a consequence of the bounds, we show that the sample complexity for both of the decision and identification versions is $\Theta(\log|\mathcal{H}|/\log p)$ for a candidate set $\mathcal{H}$ of hidden subgroups in the case that the candidate subgroups have the same prime order p, which implies that the decision version is at least as hard as the identification version in this case. In particular, it does so for the important instances such as the dihedral and the symmetric hidden subgroup problems. Moreover, the upper bound of the identification is attained by the pretty good measurement, which shows that the pretty good measurements can identify any hidden subgroup of an arbitrary group with at most $O(\log|\mathcal{H}|)$ samples.

47. M. Onsjoe and O. Watanabe:
"Finding Most Likey Solutions", Proc. Computation and Logic in the Real World (CiE 2007), Lecture Notes in Computer Science 3244, 758-767, 2007.
概要: As one simple type of statistical inference problems we consider Most Likely Solution problem, a task of finding a most likely solution (MLS in short) for a given problem instance under some given probability model. Although many MLS problems are NP-hard, we propose, for these problems, to study their average-case complexity under their assumed probablity models. We show three examples of MLS problems, and exmplain that "message passsing algorithms" (e.g., belief propagation) work reasonably well for these problems.

48. E. Hemaspaandra, L. Hemaspaandra, T. Tantau, and O. Watanabe:
"On the Complexity of Kings", Proc. 16th International Symposium on Fundamentals of Computation Theory (FCT'07), Lecture Notes in Computer Science 4639, 328-340, 2007.
概要: A k-king in a directed graph is a node from which each node in the graph can be reached via paths of length at most k. Recently, kings have proven useful in theoretical computer science, in particular in the study of the complexity of reachability problems and semifeasible sets. In this paper, we study the complexity of recognizing k-kings. For each succinctly specified family of tournaments (completely oriented digraphs), the k-king problem is easily seen to belong to Π_2^P. We prove that the complexity of kingship problems is a rich enough vocabulary to pinpoint every nontrivial many-one degree in Π_2^P.

49. Naoyuki Yamashita and Keisuke Tanaka:
"Secret Handshake with Multiple Groups", In Information Security Applications: 7th International Workshop, WISA 2006, Lecture Notes in Computer Science 4298, 339-348, August, 2007.
概要: A privacy-preserving authentication model called secret handshake was introduced by Balfanz, Durfee, Shankar, Smetters, Staddon, and Wong. It allows two members of a same group to authenticate themselves secretly to the other whether they belong to a same group or not, in the sense that each party reveals his affiliation to the other only if the other party is also a same group member. The previous works focus on the models where each participant authenticates himself as a member of one group. In this paper, we consider a secret handshake model with multiple groups. In our model, two users authenticate themselves to the other if and only if each one's memberships of multiple groups are equal. We call this model secret handshake with multiple groups. We also construct its concrete scheme. Our scheme can easily deal with the change of memberships. Even if a member is added to a new group, or deleted from the one that he belongs to, it is not necessary to change the memberships for the other groups that he belongs to.

50. Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa:
"Multi-Bit Cryptosystems Based on Lattice Problems", 10th International Workshop on Theory and Practice in Public Key Cryptography, PKC 2007, Lecture Notes in Computer Science 4450, 315-329, April, 2007.
概要: We propose multi-bit versions of several single-bit cryptosystems based on lattice problems, the error-free version of the Ajtai-Dwork cryptosystem by Goldreich, Goldwasser, and Halevi [CRYPTO '97], the Regev cryptosystems [JACM 2004 and STOC 2005], and the Ajtai cryptosystem [STOC 2005]. We develop a universal technique derived from a general structure behind them for constructing their multi-bit versions without increase in the size of ciphertexts. By evaluating the trade-off between the decryption errors and the hardness of underlying lattice problems, it is shown that our multi-bit versions encrypt $O(\log n)$-bit plaintexts into ciphertexts of the same length as the original ones with reasonable sacrifices of the hardness of the underlying lattice problems. Our technique also reveals an algebraic property, named *pseudo-homomorphism*, of the lattice-based cryptosystems.

51. 伊東利哉, 渡辺 治:
"重みつき乱択最適選好マッチング", 電子情報通信学会 コンピュテーション研究会, 信学技報 COMP, 2007.
概要: We consider a generalized version of the popular matching problem, where applicants are classified into two classes. Mahdian showed that if $m > 1.42n$, where m is the number of items and n is the number of applicnats, then a random instance of the matching problem has a popular matching with high probability. In this paper, we analyze the k weighted matching problems, and we show that for any beta such that $m = \beta n$, (lower bound) if $\beta/n^{1/3} = o(1)$, then a random instance of the 2-weighted matching problems does not have a 2-weighted popular matching with probability $1 - o(1)$; (upper bound) if $n^{1/3}/\beta = o(1)$, then a random instance of the 2-weighted matching problems has a 2-weighted popular matching with probability $1 - o(1)$.

52. O. Watanabe:
"Complexity of finding most likely solutions", 電子情報通信学会 コンピュテーショ

ン研究会, 信学技報 COMP, 2007.

概要: As one simple type of statistical inference problems we consider Most Likely Solution problem, a task of finding a most likely solution (MLS in short) for a given problem instance under some given probability model. Although many MLS problems are NP-hard, we propose, for these problems, to study their average-case complexity under their assumed probablity models. We show three examples of MLS problems, and exmplain that "message passsing algorithms" (e.g., belief propagation) work reasonably well for these problems.

53. 作本紘一, 田中圭介:
"Key-Substitution Attacks on Group Signature", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 1B1-4, 2007 年 1 月.

概要: Group signatures were introduced by Chaum and Van Heyst, and many security requirements for group signatures have been proposed. Bellare, Micciancio, and Warinschi showed that satisfying full-anonymity and full-traceability is sufficient, in the sence that all the above-mentioned requirements are implied by them. Wilson and Menezes introduced a considerable attack against standard signatures, key substitution attack. In this paper, we propose security conditions of group signatures against this attack and show that the security requirements are not sufficient regarding the attack. We also propose a group signature scheme that is secure against key substitution attack, fully-anonymous, and fully-traceable.

54. 草川恵太, 河内亮周, 田中圭介:
"A Lattice-Based Cryptosystem and Proof of Knowledge on Its Secret Key", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 1C1-1, 2007 年 1 月.

概要: We propose a lattice-based cryptosystem by modifying the Regev05 cryptosystem (STOC 2005), and design a proof of secret-key knowledge. Lattice-based public-key identification schemes have already been proposed, however, it is not known that their public keys can be used for the public keys of encryption schemes. Our modification admits the proof of knowledge on its secret key, however, we need a stronger assumption than that required by the original cryptosystem.

55. 草川恵太, 河内亮周, 田中圭介:
"Proof of Plaintext Knowledge for the Regev Cryptosystems", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 1C1-2, 2007 年 1 月.

概要: Goldwasser and Kharchenko (TCC 2006) showed a proof of plaintext knowledge for the Ajtai- Dwork cryptosystem and left the open problem designing a proof of plaintext knowledge for the Regev04 cryptosystem (JACM 2004). In this paper, we show a proof of plaintext knowledge for the Regev04 cryptosystem (JACM 2004) using their technique. Furthermore, we show that it can be applied to the Regev05 cryptosystem (STOC 2005). The key idea is to analyze tradeoffs between the hardness of the underlying lattice problem and the variance of ciphertexts, which given by Kawachi, Tanaka, and Xagawa (SCIS 2006).

56. 林良太郎, 田中圭介:
"The Security with the Randomness Revealed for Public-Key Encryption", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 2C1-4, 2007 年 1 月.

概要: We consider the situation for public-key encryption that the adversary knows the randomness which was used to compute the ciphertext. In some practical scenarios, there is a possibility that the randomness is revealed. For example, the randomness used to make a ciphertext may be

stored in insecure memory, or the pseudo-random generator may be corrupted. We first formalize the security notion on this situation as "the one-wayness with the randomness revealed." In addition to the formalization, we focus on two schemes, the generic chosen-ciphertext secure encryption method (GEM) and 3-round OAEP, and prove that these two schemes satisfy our security notions.

57. 竹部裕俊, 田中圭介:
"Steganographic Signature", 2007年 暗号と情報セキュリティシンポジウム (SCIS2007), 2B2-6, 2007年1月.
概要: Steganography is the science of sending messages hidden in harmless communications over a public channel so that an adversary eavesdropping on the channel even detect the presence of the hidden messages. In this paper, we formalize and propose steganographic signature. We define the security of steganographic signature, steganographic security and unforgeability. We construct a steganographic signature scheme, and we show that our proposed steganographic signature scheme with the extended Schnorr signature scheme is steganographically secure and unforgeable.

58. 八代正俊, 田中圭介:
"Private Approximation of the Set Cover Problem", 2007年 暗号と情報セキュリティシンポジウム (SCIS2007), 2D2-1, 2007年1月.
概要: Private approximation, introduced by Feigenbaum, Ishai, Malkin, Nissim, Strauss, and Wright, allows us to find approximate solutions with disclosing as little information as possible. In STOC 2006, Beimel, Carmi, Nissim, andWeinreb studied the private approximation for both the vertex cover and the max exact 3SAT problems. In this paper, we consider the set cover problem where the costs of all sets are polynomially bounded. We show that there exists neither a deterministic nor a randomized private approximation. We also consider the case that the frequencies of all elements are equal. We show that in this case there exist no deterministic private approximation.

59. 平野貴人, 田中圭介:
"Variations on Pseudo-Free Groups", 2007年 暗号と情報セキュリティシンポジウム (SCIS2007), 2D2-2, 2007年1月.
概要: The notion of the pseudo-free group was informally introduced by Hohenberger [Hoh03], and was formalized by Rivest. Rivest showed that many cryptographic assumptions (e.g. the RSA assumption, the strong RSA assumption, the discrete logarithm problem and so on) hold in pseudo-free groups. In this paper, we point out the fact that in the definition by Rivest, many cryptographic assumptions except for the RSA assumption do not hold. The reason is that the equation in pseudo-free groups contains no integer-valued exponent variables. Rivest probably supposed that we may not need the notion of exponent variables since the adversary can choose himself equations. In this paper, we also study some of the variations introduced by Rivest. Using these variations, we show several properties for pseudo-free groups. In particular, we describe the subgroup of pseudo-free groups.

60. 井上大輔, 田中圭介:
"Constructions for Conditional Oblivious/Converge Transfer/Cast", 2007年 暗号と情報セキュリティシンポジウム (SCIS2007), 2D4-1, 2007年1月.
概要: In this paper, we introduce a new notion of conditional converge cast (CCC), such that we append the conditional property to converge cast. Additionally,

we generalize the three primitives with conditional property, conditional oblivious transfer (COT), conditional oblivious cast (COC), and CCC. CCC is a three-party protocol which involves two sender S_0 and S_1 and a receiver R. S_0 owns a secret x and a message m_0, and S_1 y and m_1. In a CCC protocol for the predicate Q (Q-CCC), S_0 and S_1 send their messages to R in a masked form. R obtains the message depending on the value of $Q(x, y)$, i.e. R obtains m_0 if $Q(x, y) = 0$ and m_1 otherwise. Besides, the secrets x and y cannot be revealed to R or the other sender. We propose a CCC protocol for "equality" predicate with an additively homomorphic encryption scheme. Additionally, we extend 1-out-of-2 COT/COC/CCC to 1-out-of-n COT/COC/CCC. In 1-out-of-2 protocols, a sender or senders send two messages to a receiver or receivers. In 1-out-of-n protocols, a sender or senders send n messages, where $n = 2l$ for some l. We provide the consecutive definitions and the concrete protocols for 1-out-of-n COT/COC/CCC protocols. We prove that our protocols are secure under the security of 1-out-of-2 protocols.

61. 林良太郎, 田中圭介:
"Token-Controlled Public-Key Encryption in the Multi-User Setting", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 3C2-4, 2007 年 1 月.
概要: In this paper, we formalize the security notions for token-controlled public-key encryption in the multi-user setting, by not simply modifying the previous security notions in the single-user setting proposed by Baek, Safavi-Naini, and Susilo, but employing the idea to formalize the attacks in the multi-user setting proposed by Bellare, Boldyreva, and Micali. Our security notions capture the possibility of an adversary seeing encryptions of related messages under the same token and different keys when the choice of the relation can be made by the adversary. We also show that the Galindo.Herranz scheme is secure in the multi-user setting.

62. 大山千尋, 田中圭介:
"Privacy of Verifier's Identity on Designated-Verifier Signature", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 3C4-5, 2007 年 1 月.
概要: In this paper, we propose a new notion of the designated-verifier 's anonymity on designatedverifier signature (DVS), called " the privacy of verifier 's identity ". In DVS schemes, a signer can designate a signature to an intended verifier, that is, a signature generated via a DVS scheme can convince only one intended recipient of the validity or the invalidity of the signature. The privacy of verifier 's identity explains that an eavesdropper who obtains a designated-verifier signature cannot tell to whom the signature was designated, which means that the recipient is anonymous. We define the privacy of verifier 's identity, provide two concrete schemes which satisfies the property, and prove their security.

63. 山下直之, 田中圭介:
"An ID-based Combined Scheme with Encryption and Signature", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 4C2-5, 2007 年 1 月.
概要: The cryptographic protocol known as the combined scheme allows users to decrypt ciphertexts and create signatures using the same key. In this paper, we model ID-based combined schemes. Many ID-based encryption schemes and ID-based signature schemes are proposed. Most of them are based on bilinear maps. Although it seems possible to combine these schemes, there is no security definition for the com-

bination. We propose a model for this combinations, and define the security condition. As an additional property, a definition for the key privacy of encryption schemes is proposed. In the combined scheme, the same private key is used for the decryption and the signing. To protect the owner ' s privacy, both the encryption scheme and the signature scheme must satisfy the key privacy condition. When combining them, the encryption scheme should not degrade the key privacy of the signature scheme, and vice versa. We propose a key privacy condition for ID-based signature schemes. We then modify this notion to ID-based combined schemes. We construct a concrete scheme and prove that this scheme satisfies these security requirements.

64. 河内亮周, Christopher Portmann:
"Quantum Asymmetric-Key Cryptosystem Secure Against A Computationally Unbounded Adversary", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 4C1-5, 2007 年 1 月.
概要: In this paper we propose a quantum asymmetric-key cryptosystem, which does not rely on a computationally hard problem for security, but on uncertainty principles of quantum mechanics, thus obtaining security against a computationally unbounded adversary. We first propose a universally composable security criteria for quantum asymmetrickey cryptosystems by adapting the universally composable security of quantum key distribution by Mayers et al. to the context of quantum asymmetric-key encryption. We then give a specific implementation using this security notion, which improves the quantum asymmetric-key cryptosystem of Kawachi et al. in the sense of information-theoretic security. We prove that the information leak on the decryption key from the multiple copies of the encryption keys released in our scheme is exponentially smaller than that of Kawachi et al., which allows Alice to produce exponentially more encryption keys.

65. 林良太郎, 田中圭介:
"The Semantic Security and the Non-Malleability with the Randomness Revealed for Public-Key Encryption", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 2F1-5, 2008 年 1 月.
概要: 我々は公開鍵暗号において, 暗号文を計算する際に用いられた乱数を敵が知っているという状況を考える. 実用的なシナリオでは、乱数が暴かれるという可能性がある. 例えば, 安全でないメモリーに蓄えられた暗号文に乱数が使われたり, 擬似乱数生成器が操られていたりするケースがある. 我々はこの状況の安全性を "the semantic security with the randomness revealed" および "the non-malleability with the randomness revealed" として定式化した. これにくわえて, 3-round OAEP 方式に着目し, この方式が安全性を満たすことを示した.

66. 和田幸一郎, 平野貴人, 田中圭介:
"Schmidt-Takagi 暗号方式の変形", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 1F1-3, 2008 年 1 月.
概要: 我々は Schmidt-Takagi 方式の法を $n = p^2q$ とした Paillier 暗号方式の変形を提案した. 彼らの方式は, 素因数分解仮定のもとで one-wayness 安全であることや加法的準同型性という良い性質を持つ. 本論文では Schmidt-Takagi 暗号方式の変形について考察した. この変形は素因数分解仮定のもとで OW-CPA 安全であり DCR 仮定のもとで IND-CPA 安全を持つ. さらに, 暗号化関数はメッセージに関してパラメータが条件を満たすときに加法的準同型性を持つことがわかる.

67. 平野貴人, 和田幸一郎, 田中圭介:
"暗号文の単純な分解", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 1F1-5, 2008 年 1 月.
概要: この論文において我々は, 秘密分散

や加法的準同型に関連のある暗号文の分解というモデルを導入する. 受信者の公開鍵を用いることでそれぞれの送信者はメッセージをいくつかの部分に分割し, それらをそれぞれのサーバーに分配したいというものである. 我々は加法的な準同型に関するいくつかの性質をもつ Paillier 暗号方式を変形した方式を考察し, 実際に加法的な準同型性と円分多項式を用いて方式を構築した.

68. 樋渡玄良, 田中圭介:
"公開鍵暗号方式に対する安全性の概念を組み合わせたときの相互関係", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 2F1-2, 2008 年 1 月.
概要: TCC 2004 で Groth は次のことを示した．公開鍵暗号方式が，IND-CCA1 と NM-CPA を同時に満たしたとしても，NM-CCA1 を満たすには十分ではない．本論文では，公開鍵暗号方式に対する安全性の概念を複数組み合わせたときの相互関係についてのさらなる考察を行なう．特に，我々は一方向性について様々な考察を行い，安全性の概念の組み合わせ OW, IND, NM-CPA, CCA1, CCA2 のすべての間の関連性を示す．我々の考察は，現在知られている結果を拡張した内容を含んでいる.

69. 草川恵太, 田中圭介:
"格子問題に基づく高い安全性をもつ認証方式", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 3D3-1, 2008 年 1 月.
概要: Stern 認証方式を一部変更したものが, ある格子問題の最悪時の困難性を仮定することにより, コンカレント攻撃に耐えるという高い安全性を持つことを証明した. 以前提案されていた Micciancio-Vadhan 認証方式よりも, 基にする仮定が弱くなっている. なお, 仮定をイデアル格子問題に変更することで, 鍵サイズが小さい方式も提案した. また, Stern 認証方式を元にアドホック匿名認証方式も構成した. こちらの安全性も, 格子問題の最悪時の困難性を仮定することにより証明した.

70. 草川恵太, 田中圭介:
"イデアル格子問題に基づくコンパクトな署名方式", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 3D3-2, 2008 年 1 月.
概要: 2007 年に Gentry, Peikert, Vaikuntanathan が格子問題に基づくハッシュ関数に落とし戸をつけた. 彼らはそれを元に署名方式, 紛失送信, ID ベース暗号を構成している. 残念ながら, 彼らの署名方式の鍵サイズはセキュリティパラメータを n としたときに $\tilde{O}(n^2)$ と大きく実用的でない. そこでコンパクトなハッシュ関数としてしられているイデアル格子ハッシュ関数に着目し, 鍵サイズを小さくした. 具体的には彼らの鍵生成アルゴリズムとして使われている Ajtai のアルゴリズムを上手く作りかえ, イデアル格子ハッシュ関数に沿うようにした. なお, 安全性はあるイデアル格子問題の最悪時の困難性に基づいている.

71. 西巻陵, 藤崎英一郎, 田中圭介:
"二つのモデルの差を示す新たな暗号の実例", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 2F1-4, 2008 年 1 月.
概要: ランダムオラクルモデルにおいてはゼロ知識性を持つが, 標準モデルでは知識を漏らしてしまうプロトコルを構成した. 詳しくいうと, 証明者と検証者がランダムオラクルにアクセスできる時にはプロトコルはゼロ知識性を持つ. しかし, ランダムオラクルが暗号学的なハッシュ関数に置き換えられた場合には, 知識を漏らしてしまう. このような結果は Canetti, Goldreich, Halevi によって署名方式や暗号方式においては考えられていた. 我々のプロトコルは二つのモデルの新しいギャップを示しているといえる.

72. Portmann Christopher, 河内亮周, 田中圭介:
"量子非対称鍵暗号の最適性について", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 2D1-5, 2008 年 1 月.
概要: 効率のより量子非対称鍵暗号方式を提案した. ここで効率が良いの意味は, 既存方式に比べて指数的なサイズのメッセージを

暗号化出来るという意味である. さらに二つの異なる鍵配送方式のモデル化について研究をおこなった. 一つ目のモデルでは, 敵は量子通信路を自由に制御出来る. このモデルでは, 最適な量子非対称鍵暗号方式はワンタイムパッドに一致する. 従ってこのモデルでは, 非対称鍵暗号は共通鍵暗号に比べて利点が無い. 二つ目のモデルでは, 敵の能力を制限している. このモデルでは敵は一度送られた鍵を改変出来ないものとする. しかし, 鍵の複製を許すものとする. 二つ目のモデルでは, 敵がメッセージの情報を知る確率がセキュリティパラメータに関して無視できる確率であることを示した. したがって情報理論的な安全性を持つといえる.

73. 沼山晃, 一色寿之, 田中圭介:
"ハッシュ関数に対する攻撃を考慮した電子署名の安全性", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 2B2-5, 2008 年 1 月.
概要: 暗号プロトコルの安全性を証明する際に必要となるランダムオラクルモデルの性質を捉えるために, 弱いランダムオラクルモデルを定式化した. つまり, ランダムオラクルモデルに, collision, second-preimage, または first-preimage を返すオラクルを追加したモデルを考えた. さらに, この弱いランダムオラクルモデルにおいて full domain hash 署名とその変形に関する安全性の解析を行った. また, その結果として弱いランダムオラクルモデル間の関係性を示した.

74. 一色寿之, 沼山晃, 田中圭介:
"ハッシュ関数に対する攻撃を考慮した ID ベース暗号の安全性", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 4D2-1, 2008 年 1 月.
概要: ID ベース暗号において, 攻撃者がペアリングやハッシュ関数などのマスタ秘密鍵に依存しないシステムパラメータに関する情報を用いて攻撃対象の ID を選択する新しい安全性を提案する. その上で, ランダムオラクルモデルにそのランダムオラクルの collision resistance を破るオラクルを導入した collision tractable ランダムオラクルモデルにおいて, Boneh-Franklin IBE 方式は既存の selective-ID の安全性を満たすが, 提案する安全性を満たさないことを示す. また, Boneh-Franklin IBE 方式を改良し, 提案する安全性を満たす IBE 方式を提案する.

75. 作本紘一, 田中圭介:
"鍵代用可能署名", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 3F3-5, 2008 年 1 月.
概要: 本論文では電子署名の新しい機能として, 署名生成者のみが他者に代用鍵を生成させることができる電子署名方式を提案する. ここでは, 本来の署名者の公開鍵以外に, ある文書と電子署名の組を受理する公開鍵を代用鍵と呼ぶ. 鍵重複攻撃は, 署名者本人以外が, 署名者の公開情報のみから代用鍵を作る攻撃である. それに対し我々は, 署名者の公開情報のみからでは代用鍵を生成することはできないが, 署名者と対話を行えば代用鍵が生成可能となる方式を提案する. 本研究では, そのような署名方式のアルゴリズムの枠組みと安全性の形式的な定義を与え, さらにそれを満たす具体的な方式の提案と, 安全性証明を行う.

76. 井上大輔, 田中圭介:
"忘却通信に関連するプロトコルの対称性", 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 2E4-5, 2008 年 1 月.
概要: 2006 年に Wolf,Wullschleger が, Oblivious Transfer(OT) の拡張である Chosen 1-out-of-2 OT に対し, その対称性を証明した, 彼らは同様の性質を持つ物として新しいプロトコルを提案したが, 本研究では既知のプロトコルに対しその対称性を考察した. 具体的には OT の拡張である Strong Conditional OT に若干の制限を加えた XOR-, AND-, OR-OT に対し, 効率的で, かつ安全性を全く損なわずにプロトコルの反転が出来ることを証明した.

77. 竹部裕俊, 田中圭介:
"認証つき公開鍵ステガノグラフィー", 2008 年 暗号と情報セキュリティシンポジウム

(SCIS2008), 3F1-5, 2008 年 1 月.

概要: ステガノグラフィーとは，公開通信路内で行われる普通の通信の中で，通信を傍受する敵に気付かれないように密かに他のメッセージを埋め込むという情報秘匿技術である．暗号理論的なステガノグラフィーの研究において，公開鍵をベースとした情報秘匿システムが公開鍵ステガノグラフィーである．公開鍵ステガノグラフィーの研究において，これまでに様々なモデルや方式が提案されているが，我々の知る限りでは，相手認証機能をもった方式は考えられていない．本論文では，相手認証機能を備えた公開鍵ステガノグラフィーのモデルを提案し，この方式における安全性を定式化する．また，認証つき公開鍵ステガノグラフィーの具体的な方式を，公開鍵暗号方式と電子署名方式を組み合わせて構成し，この方式の安全性の証明を行う．

78. Mario Larangeira, 田中圭介:
“ペアリングを用いた署名方式と Strong Diffie-Hellman 問題の関係”, 2008 年 暗号と情報セキュリティシンポジウム (SCIS2008), 3F2-1, 2008 年 1 月.

概要: Boneh と Boyen は, Strong Diffie-Hellman (SDH) 仮定の下で安全性が証明可能な署名方式を提案した．そこでは, 署名を偽造するアルゴリズムが存在すれば SDH 問題を解くアルゴリズムが存在することを示すことで, 安全性の証明がなされている．本研究では, 離散対数問題を解くことが困難であるという仮定の下では, SDH 問題を解くアルゴリズムを用いても Boneh-Boyen 署名方式について署名を偽造することは困難であるということを generic model の上で証明する．

文部科学省科学研究費補助金 特定領域研究 (課題番号 16092215)

B03: 量子論理回路の最適化に関する研究

通常のコンピュータにおいては, 計算時間の短縮のために, 計算の途中で計算結果の一部をメモリ内に一時的に保存しておくことがある．量子コンピュータの回路設計においては，補助量子ビットがそのようなワークビットとして用いられるが，補助量子ビットは厳密に定義がなされているわけではない．本研究ではどのような補助量子ビットにゲート数削減の効果があるのかを検証するために，補助量子ビットの分類と定式化を行った．そして，量子回路のゲート数とビット数の関係について考察した．さらに本研究では, 回路計算量の下界を導出するための証明手法として, Nielsen によって提案された, 量子論理回路サイズの下界を求めるための幾何学的手法に着目し研究を進めた. そして, 筆者らによる量子論理回路の深さ最小化に関する結果と, この Nielsen の結果を組み合わせることで新たな知見が得られた.

研究組織

研究代表者：	西野 哲朗	電気通信大学 電気通信学部
研究分担者：	垂井 淳	電気通信大学 電気通信学部
	太田 和夫	電気通信大学 電気通信学部 (平成 17–19 年度)
	國廣 昇	電気通信大学 電気通信学部 (平成 17–19 年度)

交付決定額 (配分額)

平成 16 年度	6,700,000 円
平成 17 年度	6,700,000 円
平成 18 年度	2,000,000 円
平成 19 年度	2,300,000 円
合　計	17,700,000 円

研究成果の概要

- **学術誌**: (1) Yasuhiro Takahashi and Noboru Kunihiro, "A quantum circuit for Shor's factoring algorithm using 2n+2 qubits," Quantum Information and Computation, Vol.6 No.2, pp.184-192, 2006, (2) Yasuhiro Takahashi, Noboru Kunihiro, and Kazuo Ohta, " The Quantum Fourier Transform on a Linear Nearest Neighbor Architechture," Quantum Information and Computation, Vol.7 No.4, pp.383-391, 2007.
- **国際会議**: (1) Yukihide Nakui, Tetsuro Nishino, Seiya Okubo: On the Minimization of the Depth of Certain Quantum Circuits, International Symposium on Energy, Informatics and Cybernetics (EIC 2005), July 10-13, Orlando, Florida, USA (2005), (2) Shin-ichi Hashiba, Seiya Okubo and Tetsuro Nishino: Efficient Quantum Algorithms for Algebraic Problems, International Conference on Computer & Communication Engineering (ICCCE '06), May 9-11, Kuala Lumpur, Malaysia, pp.567-572 (2006).

1 はじめに

1985 年に D. Deutsch が，量子力学に基づく新たな計算モデルとして量子 Turing 機械を提案し，量子計算機のモデル化を行って以来，量子計算に関する研究が活発に行われてきた．例えば，1994 年に P. W. Shor は，整数の因数分解を多項式時間内に高い成功確率で行う量子アルゴリズムを示した．さらに，1996 年には L.K.Grover が，効率的量子探索アルゴリズムを提案した．このように，量子計算は本質的に古典計算よりも強力である可能性がある．

また，一方，幾何学的手法を用いた量子論理回路のサイズの下界に関する研究や，補助量子ビットが回路計算量に及ぼす影響を明らかにする研究が行われている．これらの研究により，通常の計算量理論に，何らかの貢献ができるのではないかと期待されている．

量子計算機の物理的実装の実現には，多くの困難が存在する．例えば，量子もつれ合いを保つことができる時間が短いことや，複雑な量子操作を行なうことは難しい等である．これらの問題の解決のためにも，量子回路サイズは重要である．本研究では，量子回路サイズを評価するよい方法を検討する．特に，C-NOT ゲートに着目し，量子回路計算量と C-NOT ゲート数の関係について，幾つかの定理を示す.

補助量子ビットの効果の検証

量子コンピュータは従来のコンピュータに比べて本質的に計算能力の高い、未来のコンピュータとして期待されている．現在、その物理的実現が盛んに研究されているが、量子コンピュータの実現には多くの困難が伴う．そのうちの一つとして、量子コンピュータは量子重ね合わせ状態という量子力学的にデリケートな状態をとる、ということが挙げられる。そのためサイズの大きい量子コンピュータの複雑な量子重ね合わせ状態を長時間維持することは非常に困難となる．それに加えて，量子コンピュータは扱えるビット数が大きくなるほど実現が困難であることが知られている．すなわち，同じアルゴリズムを実行する場合，量子コンピュータにおいては特に，時間計算量および領域計算量を縮小することが本質的に重要な問題となる．

本研究では，まず最初に, 量子回路のゲート数とビット数の関係について考察する．具体的には，あるアルゴリズムを実行する量子回路に対して，それに補助量子ビットを付加し，回路を再構成することで，ゲートの総数をさらに縮小できるかどうかを検証する．

我々は古典コンピュータを用いてアルゴリズムを実行するときに，計算時間の短縮のために計算の途中で，その計算結果の一部をメモリの別の場所に一時的に保管することをよく行う．量子コンピュータの回路設計においても，補助量子ビットはそのようなワークビットとしてたびたび用いられるが，そこで使われる補助量子ビットは厳密に定義されているわけではない．本研究ではどのような種類の補助量子ビットにゲート数縮小の効果があるのかを検証するために，補助量子ビットの分類，定式化を行った．

量子回路計算量の下界導出に向けて

回路計算量理論は，情報理論の創始者として有名な，C. Shannon の 1949 年の論文から始まったと考えられている．一般に，ある関数を計算する回路としては，種々のものが考えられるが，Shannon は，関数 f を計算する最小回路のサイズによって，その関数 f の複雑さを測ることを提案した．

当時の Shannon の動機は，回路を実現するのに必要な素子数を最小化することであったらしい．彼は，すべての n 入力関数の複雑さに関する上界を証明し，さらにほとんどの関数について，この上界が下界とあまり違わないことを**数え上げ論法**を用いて示した．

回路は，計算能力に関して Turing 機械と密接な関係を持っており，回路サイズに関する十分大きな下界は時間計算量に関する下界をただちに与える．回路モデルは，計算モデルのなかでも特に定義が単純なので，組合せ論的解析をより簡単に行なえる．しかし，現在我々は一般の回路サイズに関しては，非常に弱い下界しか示すことができない．

この回路計算量理論は 1980 年代に，**P = NP ? 問題** [10] に対する有望なアプローチとして注目を集めた [9, 13]. P = NP ? 問題に対する 1 つのアプローチは，計算モデルの能力に制限を加え，

可能なアルゴリズムのクラスを制限して議論を行うことであった．実際，このアプローチにより，いくつかの興味深い結果が証明された．しかし，これらの結果に基づいて，より一般的な計算モデルに対する強い下界を導くことはできていない．

一方, Razborov と Rudich は論文 [18] のなかで，**Natural Proof** という概念を導入し，以下のことを示した. 非一様ブール計算量についてすでに知られている証明手法を用いた，非単調回路モデルに対する下界の証明はすべて，natural であるか，または natural に表現できる．さらに彼らは，ある妥当な仮定のもとで, 一般回路に対する超多項式下界を証明する natural proof は存在しないことを示した．つまり, P = NP ? 問題の解決に向けては, 新たな証明法を開発しなければならないという状況証拠が示されたのだ.

そこで，本研究では，回路計算量の下界を導出するための natural ではない証明手法として, Nielsen によって提案された, 量子論理回路サイズの下界を求めるための幾何学的手法 [15] に着目し研究を進めた．そして, 筆者らによる量子論理回路の深さ最小化に関する結果 [14] と，この Nielsen の結果を組み合わせることで得られた新たな知見が得られた.

2 量子回路

1985 年に，英国人物理学者 David Deutsch は，**量子 Turing 機械**（quantum Turing machine, 以下 QTM と略す）という量子力学的動作原理に基づく新たな計算モデルを提案した．この QTM に基づくコンピュータが，**量子コンピュータ**と呼ばれている.

通常のコンピュータのメモリの一区画には，0 または 1 が保持できるが，QTM のメモリの一区画には，0 と 1 の任意の重ね合わせ状態が保持できる．ここで，重ね合わせ状態とは，0 に対応する状態ベクトル $|0\rangle$ と 1 に対応する状態ベクトル $|1\rangle$ を，それぞれ,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

とするとき，$\alpha|0\rangle + \beta|1\rangle$ の形で表されるベクトルの和のことをいう．ただし，α と β は，条件式 $|\alpha|^2 + |\beta|^2 = 1$ を満たす任意の複素数であり，振幅と呼ばれる．この重ね合わせ状態を観測すると，0 （または 1）が確率 $|\alpha|^2$ （$|\beta|^2$）で読めるものと仮定する.

QTM のテープの一区画が保持できる情報量を **1 量子ビット**（quantum bit, qubit）という．QTM の動作は，量子ビットに対するユニタリ変換と呼ばれる線形変換の適用という形で表現できる．一方，QTM 上で実行されるアルゴリズムを量子アルゴリズムと呼ぶ．そこで以下では，量子アルゴリズムを量子ビットに適用されるユニタリ変換の系列として記述することにする.

1994 年に，AT & T の Peter Shor は，整数の因数分解を小さな誤り確率で高速に行う量子アルゴリズムの設計に成功し，世界的な注目を集めた．というのは，現在広く用いられている RSA などの公開鍵暗号が，因数分解問題の難しさを前提として設計されているからである．この Shor の結果に影響されて，量子コンピュータの物理的実現に関する研究が現在盛んに行われている.

通常の組み合わせ論理回路のアナロジーとして, Deutsch によって導入されたのが, 量子論理回路である．一般に電気回路は，多数の**論理ゲート**から構成されている．通常のコンピュータを実現するのに用いられている論理ゲートとしては, AND, OR, NOT ゲートなどがある．例えば，AND と NOT，または OR と NOT の 2 種類のゲートを用いれば，任意の Turing 機械の計算を模倣する回路を構成することができる.

一方，量子計算は量子ビットに適用されるユニタリ変換の系列で表現される．Deutsch や Yao らの研究によって，QTM の動作は**量子回路**で模倣できることがわかっている．最近，量子回路を実現するための量子論理ゲートについて盛んに研究が行われているが，現在までに，例えば以下のような量子論理ゲートが考案されている．なお，量子論理ゲートの各入出力は，1 つの量子ビットに対応している.

制御 NOT ゲート ... このゲートは 2 入力 2 出力である．最も単純な場合について説明すると，制御 NOT ゲートにおいては，入力の第一ビット x_1 の値が 0 ならば，入力の第 2 ビット x_2 の値がそのまま出力の第 2 ビット y_2 の値となるが，x_1 の値が 1 ならば，x_2 の値が反転された値が y_2

の値となる．すなわち，$x_1 = 1$ のときには，x_2 の否定が y_2 に代入される．なお，いずれの場合においても，$y_1 = x_1$ である．制御 NOT ゲートは，以下のような 4 次の正方行列で表現される，2 量子ビットに対するユニタリ変換を実行する．

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

ここで，この行列の各行各列は，それぞれ順に，$|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ という状態に対応している．例えば，上の行列の第 3 行は $|10\rangle$ という状態に対応し，第 4 列は $|11\rangle$ という状態に対応するが，その第 3 行第 4 列成分が 1 であることは，以下のことを表している．制御 NOT ゲートへの入力が $x_1 = 1$, $x_2 = 0$ である場合には，その出力は $y_1 = 1$, $y_2 = 1$ となる．

ユニタリ変換ゲート ... このゲートは 1 入力 1 出力であり，入力に対して指定されたユニタリ変換 U を行う．ただし，このユニタリ変換 U は，行列式が 1 であるような，2 行 2 列のユニタリ行列で表現されるものである．ユニタリ変換ゲートの具体例としては，以下に示す Hadamard ゲート H を参照されたい．

通常の組み合わせ論理回路の量子アナロジーとして，Deutsch によって導入されたのが，**量子回路**である．これは，フィードバックを持たない古典的回路の量子版である．量子回路を定義するために，ある基本ゲートの集合が **基底**として選ばれるが，ここでの各基本ゲートは，$2^k \times 2^k$ ユニタリ行列によって規定される k-入力 k-出力素子である．

以下では $h = 2^k$ とし，$\mathbf{C}^h$ で h-組の複素数をから構成されるベクトル空間を表す．$u, v \in \mathbf{C}^h$ に対し，**内積**を $< u, v >= \sum_{1 \leq i \leq h} u_i^* v_i$ により定義し，ベクトル u の**長さ**を $(< u, u >)^{1/2}$ で定義する．また，$< u, v >= 0$ が成り立つとき，u と v は**直交する**という．ただひとつの成分のみが 1 で，その他のすべての成分が 0 であるような自然な単位ベクトルは，全部で h 個存在するが，それらは $\{0,1\}^k$ 内の要素と同一視できる．$2^k \times 2^k$ ユニタリ行列 U は，ベクトル $u \in \mathbf{C}^h$ を別のベクトル $u' \in \mathbf{C}^h$ に次のような方法で変換する：入力 $u = \sum_{x \in \{0,1\}^k} c_x x$ に対し，出力は $u' = \sum_{x \in \{0,1\}^k} c_x U_{x,y} y$ によって与えられる．ただし，x と y は $\mathbf{C}^h$ 内の単位ベクトルである．定義より，ユニタリ行列は，互いに直交する単位ベクトルの集合を，互いに直交する単位ベクトルの別の集合に変換することに注意せよ．

量子回路は，通常のブール回路と同様に，基本ゲートを適当な遅延時間を伴ってワイヤで結合することにより構成される．量子回路は，何本かの入力ワイヤと出力ワイヤを持つ．何本かの入力ワイヤには，繰り返しを許して変数の集合 $x_1, x_2, ..., x_n$ が対応し，残りの入力ワイヤには定数 0 と 1 が対応する．一方，出力ワイヤの何本かを，特定の時刻に測定される出力変数 $y_1, y_2, ..., y_m$ に対応させる．すべての m-入力 m-出力量子ゲートの集合を B_m で表す．

Deutsch は，$n \geq 3$ の場合に，n 個のブール変数により定義される $\mathbf{C}^{2^n}$ のすべてのユニタリ変換は，B_3 を基底とする量子回路によって計算できることを示した．回路からフィードバック・ループを無くすには，最初，定数 0 または 1 に設定されており，出力時にはその同じ定数値に戻されているような，補助ワイヤを追加すればよいことが知られている．

量子コンピュータが行う計算は，ユニタリ変換によって定められる．そこでユニタリ変換 U を持つ量子コンピュータを，$\boldsymbol{x}$ を入力としてとり，$U\boldsymbol{x}$ を出力する**量子回路**とみなす．

量子回路を表現するダイアグラムでは，平行した k 本のワイヤはベクトル空間 $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{k}$ を表す．k 本のワイヤに入力される情報は古典コンピュータの k ビット に相当するので，k 本のワイヤで扱える情報を **k 量子ビット**とよぶ．また，k 本のワイヤを **k 量子ビット レジスタ**とよぶ．

任意の量子回路は以降に述べる 2 種類の**量子ゲート**を組み合わせて構成できる．そのため，これらの量子ゲートは**基本ゲート**と呼ばれる．

本研究では量子回路を構成する基本ゲートの数を，量子コンピュータのサイズと考える．

3　補助量子ビットの分類

補助量子ビットには，それを付加する元の回路の入力に無関係な値が入力される．また回路内部では補助量子ビットに自由に値を書き込むことが出来る．すなわち，作業域として使われる．

補助量子ビット問題とは、既存の回路に内部で作業域として利用できる余分な量子ビットレジスタを加えて再構成したとき、その回路の最小サイズが小さくなることがあるか、という問題である。

次に述べる 2 種類が，現在までに厳密に定式化できた補助量子ビットである．

単純補助量子ビット

論理変数 $|x\rangle$ を入力し論理変数 $|x\rangle$ を出力するような補助量子ビットを単純補助量子ビットと呼ぶ。

定数補助量子ビット

論理定数 $|0\rangle$ を入力し、それぞれ $|0\rangle$ を出力するような補助量子ビットを定数補助量子ビットと呼ぶ。

定数補助量子ビットは、実際の回路設計において、ワークビットとしてゲート数削減のために用いられている。

この補助量子ビットの入出力は以下のように書き直すことが出来る．

論理変数 $|a\rangle$ を入力し，$a = 0$ のときに $|a\rangle \otimes U|x\rangle$ を出力し，$a = 1$ のときに $|a\rangle \otimes *|x\rangle$ を出力する．ただし，$*$ は任意のユニタリ変換とする．

ここで、$U \oplus U = I \otimes U$ より、単純補助量子ビット問題は、定数補助量子ビット問題の限定的な場合であることがわかる。

その他の補助量子ビット

このほかにも，論理入力に対して，任意の論理値を出力するような補助量子ビットや，重ね合わせや絡み合い状態を出力して観測結果を確率的にするような補助量子ビットが考えられる．

4　単純補助量子ビットの効果の検証

単純補助量子ビットの効果を検証するに当たって，問題をわかりやすくするために分割回路の概念を導入する．

分割回路

二つの回路を縦に接続し，新たな回路を作ることを考える．得られた回路について，もし元の二つの回路がそれぞれ用いていた量子ビットの間をまたぐ量子ゲートが存在しなければ，その回路を**分割回路**とよぶ．

また，二つの回路が実現するユニタリ変換について，それぞれをテンソル積で結んだ変換を**分割変換**と呼ぶ．

命題 4.1 分割変換

ある分割変換 $U \otimes V$ に対して，それを実現する分割回路が存在する．

証明　自明である．

□

命題 4.2 分割回路

複数の，ワイヤの数が等しい分割回路を横に接続して作られる回路に対して，その回路に等価な分割回路が存在する．

証明

複数の分割回路を接続した回路が実現する変換は，

$$\prod_i (U_i \otimes V_i) \tag{4.1}$$

と書くことが出来る．この式を変形すると，

$$\begin{aligned} &\prod_i (U_i \otimes V_i) \\ &= \left(\prod_i U_i\right) \otimes \left(\prod_i V_i\right) \end{aligned} \tag{4.2}$$

となり，分割変換であることが分かる．

よって命題 1 より，この分割変換を実現する分割回路が存在する．

□

2つの回路をまたぐC-NOTゲートが1個のときの解析

単純補助量子ビットを 1 つ用いて，回路を最適化するに当たって，補助量子ビットにまたがる C-NOT ゲートが 1 つの回路に最適化することは出来ない，ということを証明した．

補題 4.1 *C-NOT* ゲートと等価な分割回路は存在しない．

補題 4.2 *2* つの部分回路をまたぐ *C-NOT* ゲートがただ *1* つの回路は，分割回路でない．

定理 4.1 $U \otimes V$ を実現する最小サイズの回路が，*2* つの部分回路をまたぐ *C-NOT* ゲートをただ *1* つしか含まないとき，そのような回路は U, V を実現する二つの回路は接続することで最適化できない．

定理 1 で，$V = I$ とすると，単純補助量子ビットを用いて，元の回路と補助量子ビットをまたぐ C-NOT ゲートが一つの回路に，最適化することは出来ない，ということが分かる．

補助量子ビットの分類について，単純補助量子ビットと定数補助量子ビットの 2 種類について定式化を行い，定数補助量子ビットは単純補助量子ビットの一般化であることを示した．

さらに，単純補助量子ビットを回路に加えたときに，補助量子ビットにまたがる C-NOT ゲートが 1 つの回路に再構成することはできない，ということを証明した．

今後は，さらに補助量子ビットの分類を進めその効果を検証する．

5 量子回路のサイズとC-NOTゲート数の関係

本節では，量子回路のサイズと C-NOT ゲート数の関係について考察する．

あるユニタリ作用素 U を実現するにあたり，回路サイズが最小になる回路のゲート数を $m_{\mathcal{G}}(U)$ と，また，C-NOT ゲート数が最小となる回路の C-NOT ゲート数を $m_{\mathcal{C}}(U)$ と表記する．

定理 5.1 $m_{\mathcal{C}}(U) = \Omega(n)$ のとき，次の関係が成立する．

$$m_{\mathcal{G}}(U) = \Theta\left(m_{\mathcal{C}}(U)\right)$$

証明

1. $m_{\mathcal{G}}(U) = \Omega\left(m_{\mathcal{C}}(U)\right)$ の証明
   回路サイズが最小となる回路の C-NOT ゲート数を c'，1 qubit ゲートの数を s' とすると，
   $$m_{\mathcal{G}}(U) = c' + s'$$
   が成立する．あきらかに $m_{\mathcal{C}}(U) \leq c'$, $s' \geq 0$ なので，
   $$m_{\mathcal{C}}(U) \leq m_{\mathcal{G}}(U)$$
   が成り立つ．したがって，
   $$m_{\mathcal{G}}(U) = \Omega\left(m_{\mathcal{C}}(U)\right) \tag{5.1}$$
   となる．

2. $m_{\mathcal{G}}(U) = O\left(m_{\mathcal{C}}(U)\right)$ の証明
   C-NOT ゲート数が最小になる回路の回路サイズ g を
   $$g = m_{\mathcal{C}}(U) + s$$
   とする．ここで，s は 1 量子ビットゲートの個数である．同じワイヤー上で隣接する 1 量子ビットゲートは，ひとつの 1 量子ビットゲートにまとめることができる．したがって，量子回路に含まれる 1 量子ビットゲートは，C-NOT ゲートのすぐ右隣に 2 つと，n 本ある各ワイヤーの最も左に 1 つずつあれば十分である．よって，
   $$g \leq 3m_{\mathcal{C}}(U) + n$$
   が成立する．あきらかに，$m_{\mathcal{G}}(U) \leq g$ なので
   $$m_{\mathcal{G}}(U) \leq 3m_{\mathcal{C}}(U) + n$$
   が成り立つ．よって，$m_{\mathcal{C}}(U) \geq O(n)$ のとき
   $$m_{\mathcal{G}}(U) = O\left(m_{\mathcal{C}}(U)\right) \tag{5.2}$$
   となる．

式 (5.1),(5.2) より $m_{\mathcal{C}}(U) = \Theta\left(m_{\mathcal{G}}(U)\right)$ を得る．□

6　ゲートの種類を制限した場合

本節では，使用するゲートの種類を制限した場合における回路サイズについて，考察を行なう．

定理 6.1 C-NOT ゲートのみから構成される量子ビット数 n の量子回路のサイズは，高々 $O(n^2)$ である．

証明 C-NOT ゲートのみを利用した回路においては，第 1 番目から第 n 番目までの，各々のワイヤーから出力される値は，入力 x_i の排他的論理和となる．各ワイヤーからの出力が x_i の排他的論理和の形で与えられたとき，C-NOT ゲートのみを使用した回路を構成するアルゴリズムを示すことで，定理の証明を行なう．

第 i 番目のワイヤーからの出力を $|z_{i,1}x_1 \oplus z_{i,2}x_2 \oplus ... \oplus z_{i,n}x_n\rangle$, $z_{i,j} \in \{0,1\}$ としたとき，すべてのワイヤーからの出力をまとめて，

$$Z = \begin{pmatrix} z_{1,1} & z_{1,2} & \cdots & z_{1,n} \\ z_{2,1} & z_{2,2} & & z_{2,n} \\ \vdots & & & \vdots \\ z_{n,1} & z_{n,2} & \cdots & z_{n,n} \end{pmatrix}$$

のように表現する．行列 Z のランクが n で無い場合，その回路は C-NOT ゲートのみで構成することはできない．

回路構成アルゴリズム

入力：Z

出力：$C-NOT$ ゲートのみを使用した回路

アルゴリズム：

1. ゲートが1つもない（つまりワイヤーのみの）量子回路を書く．
2. 2a から 2b を $i = 1$ から n まで繰り返す．
   (a) もし，$z_{i,i} = 0$ ならば，$z_{j,i} = 1$ である列 j を1つ探し出し，$z_{i,k} := z_{i,k} \oplus z_{j,k}, k \in \{1, ..., n\}$ とする．
   すなわち，第 i 行目と第 j 行目の，それぞれの要素の排他的論理和を，新たな第 i 行目の要素とする．
   第 j 番目のワイヤーを制御ビット，第 i 番目のワイヤーを目標ビットとした C-NOT ゲートを，量子回路の一番左側に置く．
   (b) $j = 1$ から n（ただし $j = i$ は除く）に対して，以下を繰り返す．
      i. $z_{j,i} = 1$ ならば，
      $z_{j,k} := z_{i,k} \oplus z_{j,k}, k \in \{1, ..., n\}$
      とする．
      すなわち，第 i 行目と第 j 行目の，それぞれの要素の排他的論理和を，新たな第 j 行目の要素とする．
      第 i 番目のワイヤーを制御ビット，第 j 番目のワイヤーを目標ビットとした C-NOT ゲートを，量子回路の一番左側に置く．
      ii. $z_{j,i} = 0$ ならば，何もしない．

ステップ 2aにおいて，C-NOT ゲートは高々 1 個，ステップ 2bにおいて，C-NOT ゲートは高々 $n-1$ 個記入される．また，ステップ 2aから 2bは，n 回繰り返されるので，全体として，書き込まれる C-NOT ゲートの個数は，高々 n^2 個である．

定理 6.2 C-NOT ゲートと NOT ゲートのみから構成される量子ビット数 n の量子回路のサイズは，高々 $O(n^2)$ である．

また，C-NOT ゲートと NOT ゲートのみで構成された回路が出力できるパターン数は，C-NOT ゲートのみで構成された回路が出力できるパターン数の，高々 2^n 倍である．

証明

C-NOT ゲートと NOT ゲートのみから構成される回路においては，それぞれのワイヤーからの出力は，リテラルの排他的論理和と否定のみで構成された式となる．

また，排他的論理和と否定のみで構成された式においては，

$$\overline{x \oplus y} = \overline{x} \oplus y = x \oplus \overline{y}$$

が成り立つ．つまり，1つのリテラルの否定は全体の否定と等価である．リテラルが3つ以上含まれる場合でも，1つのリテラルの否定は全体の否定と等価である．したがって，リテラルの排他的論理和と否定のみで構成可能な式は，排他的論理和のみで構成される形の式と，排他的論理和のみの式全体を否定した形の式の，2パターンしかない．

これらのことより，出力に対応する排他的論理和の式中に否定が含まれていた場合，その回路の最後の層に NOT ゲートを置くことで，その層の直前においては，排他的論理和のみの式とすることができる．

排他的論理和のみの式を計算するのに必要な回路サイズは，$O(n^2)$ であり，また，この回路に含まれる NOT ゲートの数は，高々 n 個である．したがって，C-NOT ゲートと NOT ゲートのみを使用して量子回路を組む場合，必要なゲート数は高々 $O(n^2)$ である．

C-NOT ゲートと NOT ゲートのみによって構成される回路は，C-NOT ゲートのみによって構成される回路と比べ，それぞれのワイヤーの最後の層に，NOT ゲートが有るか否かの差しかない．そのため，C-NOT ゲートと NOT ゲートしか使用しない回路が出力できるパターン数は，C-NOT のみの回路が出力できるパターン数の高々 2^n 倍となる．

□

7 Natural Proof

1994 年カナダのモントリオールで開催された，The 26th ACM Symposium on Theory of Computing (STOC'94) において，A. A. Razborov と S. Rudich による "Natural Proofs" という論文 [18] が発表された．本節では，その内容の概略を紹介する．

多くの人々が，P = NP ? 問題を解くことは非常に難しそうだと感じている．そのことを数学的に示すことはできないであろうか？そのためのひとつの方法は，現在知られている証明手法が，P = NP ? 問題を解決するのには弱過ぎることを示すことである．この方針に従った最初の結果を示したのは，Baker, Gill と Solovay [2] であった．彼らは，相対化可能な証明手法では，P = NP ? 問題は解決できないことを示した．相対化可能な証明手法には，対角線論法やシミュレーションといった当時知られていた主要な証明方法が含まれていたため，研究者は路線変更を余儀なくされた．

そこで多くの研究者が回路計算量の研究を始めた．そして，1980 年代に入ると，前節で述べたように，非常に多くの相対化不可能な証明手法が発見され，それらの手法を用いて強い下界が示された．これらの手法では組み合わせ論が巧妙に用いられている．

Razborov と Rudich は [18] のなかで，**Natural Proof** という概念を導入し，以下のことを示した．非一様ブール計算量についてすでに知られている証明手法を用いた，非単調回路モデルに対する下界の証明はすべて natural であるか，または natural に表現できる．さらに彼らは，暗号を破ることの難しさ（f の値は容易に計算できるが，f^{-1} の値の計算が非常に難しいような，一方向性関数 f の存在）を仮定すれば，一般回路に対する超多項式下界を証明する natural proof は存在しないことを示した．

ある特定の関数 $\{g_n\}$ が多項式サイズの回路を持たないという証明は，通常，以下のように展開される．

(1) ブール関数についてのある性質 C_n を提示する．

(2) 任意の $f_n \in C_n$ に対し，f_n を計算する回路のサイズが n に関する超多項式である（すなわち $\{f_n\} \notin P/poly$ である）ことを証明する．言い換えれば，性質 C_n を持つすべてのブール関数は計算することが難しいことを示す．以下では，このような性質 C_n を useful と呼ぶことにする．

(3) 最後に，g_n が性質 C_n を持つことを示し，これにより，$\{g_n\} \notin P/poly$ が導かれる．もし，関数 $\{g_n\}$ が NP に属していれば，以上は P $\neq$ NP の証明になっている．

ここで，$P/poly$ とは，入力の長さごとに一意に定まる，アドバイス列と呼ばれる記号列（ただし，入力サイズに関する多項式長とする）が与えられれば，多項式サイズの回路で認識できるような言語のクラスである．言語 L が $P/poly$ に属する必要十分条件は，$f_n^{-1}(1) = L \cap \{0,1\}^n$ により定義される関数 f_n が，n に関する多項式サイズの回路で計算できることであることが知られている．

以上のことを形式的に述べるために，いくつかの概念を導入する．ブール関数の**組み合わせ論的性質**とは，ブール関数の集合 $\{C_n \subseteq F_n \mid n \in \omega\}$

のことをいう．組み合わせ論的性質 C_n が**自然**（natural）であるとは，それが，次の条件 1, 2 を満たす部分集合 C_n^* を含むときをいう．また，組み合わせ論的性質 C_n は，条件 3 を満たすとき，$P/poly$ に対して **useful** であるという．

1. (Constructivity) 述語 $f_n \in C_n^*$ が P に属する．すなわち，C_n^* は f_n の真理値表の長さ（2^n）に関する多項式時間で計算可能である．
2. (Largeness) $|C_n^*| \geq 2^{-O(n)} \cdot |F_n|$
3. (Usefulness) 任意の関数の列 $f_1, f_2, \ldots, f_n, \ldots$（ただし $f_n \in C_n$）の回路サイズは，超多項式，すなわち $\{f_n\} \notin P/poly$ である．

ある関数が多項式サイズ回路を持たないという証明は，それが，$P/poly$ に対して useful で，かつ自然な組み合わせ論的性質 C_n の定義を明確に含んでいるとき，$P/poly$ **に対して自然**（ natural against $P/poly$ ）であるという．

上で述べた形の証明が，$P/poly$ に対して natural になるためには，証明で使われる性質 C_n それ自身が natural でなければならない．すなわち，C_n は上の条件 1, 2 を満足する部分集合 C_n^* を含まなければならない．条件 2 は，n 変数ブール関数の全体 F_n のうちの，少なくとも（2^n に関する）多項式分の 1 の個数の関数について，C_n^* が真であることを述べている．また，条件 1 は，$f_n \in C_n^*$ の真偽が，Turing 機械によって関数 f_n の真理表の長さ（すなわち 2^n）に関する多項式時間で決定できることを要求している．

制限された非単調回路モデルに対する下界の証明で，現在までに知られているものはすべて，上で述べたように行われていることがわかる．実際，Razborov と Rudich は，Furst, Saxe と Sipser による $PARITY \notin AC_0$ の証明などがすべて natural である（あるいは natural proof に書き直すことができる）ことを示した．

一方，単調回路モデルに対する下界の証明においては，constructive な組み合わせ論的性質は用いられているが，largeness 条件に対する形式的なアナロジーは存在しない．(特に，random 単調関数の useful な定義は明かではない.）しかし，単調回路計算量の指数下界を示す際に Razborov が用いた近似法は，一般回路に適用してもほとんど効果を発揮しないことが，Razborov 自身によってすでに示されている [17].

Razborov と Rudich は，Natural Proof が，下界の証明においてある意味の限界を持っていることを示した．その基本的アイディアは以下の通りである．まず，SAT $\notin P/Poly$ の natural proof が存在したとすると，その proof に対応したある種のアルゴリズムが存在する．その proof は SAT と pseudo-random function を区別しなければならないから，その proof に対応したアルゴリズムもそれらを区別できなければならない．したがって，そのアルゴリズムは pseudo-random generator を破るのに用いることができる．

以上のことを，もう少し形式的に述べてみよう．pseudo-random generator $G_n : \{0,1\}^n \to \{0,1\}^{2n}$ の hardness $H(G_n)$ とは，以下の条件を満足する S の最小値である．

サイズ S 以下の回路 C のなかに，次の関係式を満たすものが存在する：

$$| \mathbf{Pr}[C(G_n(\mathbf{x})) = 1] - \mathbf{Pr}[C(\mathbf{y}) = 1] | \geq \frac{1}{S}$$

ただし，通常のように，$\mathbf{x}$ は $\{0,1\}^n$ からランダムに選ばれ，また，$\mathbf{y}$ は $\{0,1\}^{2n}$ からランダムに選ばれるものとする．

上の定義の意味を考えてみる．$H(G_n)$ の定義から，サイズが $S < H(G_n)$ であるすべての回路 C に対し，次の関係式が成り立つ：

$$| \mathbf{Pr}[C(G_n(\mathbf{x})) = 1] - \mathbf{Pr}[C(\mathbf{y}) = 1] | < \frac{1}{S}$$

この関係式の右辺は，n が限りなく大きくなるとき 0 に限りなく近づく．したがって，この関係式は,（漸近的には）サイズ S の回路 C には G_n が生成した pseudo-random 列 $\mathbf{y}$ と，真に random な列 $\mathbf{x}$ との区別がつかなくなることを示している．つまり，$\mathbf{y}$ の pseudo random 性の判定は，サイズ $S < H(G_n)$ の回路には，難し過ぎて行えないことを示している．Razborov と Rudich は以下の定理を示した．

定理 7.1 (Razborov & Rudich) $P/poly$ に対して $P/poly$-*natural* な下界の証明が存在したとする．このとき，すべての多項式時間計算可能な

$G_n : \{0,1\}^k \to \{0,1\}^{2k}$ に対し，以下が成り立つ．

$$H(G_k) \leq 2^{k^{o(1)}}$$

言い換えれば，もし 2^{n^ε}-*hard* 関数が存在すれば，$P/poly$ に対する $P/poly$-*natural* な証明は存在しない． □

P = NP ? 問題の解決には，従来の証明手法はおそらく適用できず，また，この問題を解くことは暗号を解くのと同じくらい難しいであろうということは，従来から多くの研究者が抱いてきた直観ではないだろうか？Razborov と Rudich の結果は，まさにそれらのことを数学的に正確に述べている．STOC'94 での講演のなかで，Rudich は次のように述べた．「Baker, Gill と Solovay の仕事によって，ある種の手法は P ≠ NP を証明するには弱過ぎることがわかった．そして我々の今回の結果によって，それ以後開発された手法が P ≠ NP を証明するには強過ぎることがわかった．今後，我々が進むべき道は，それらの中間に位置する強さの証明手法を開発することである．」

そのような natural ではない中間的強さの証明手法を, どのようにして発見するのかについては, 未だ明確な指針が得られているわけではないが, 筆者は, 量子論理回路サイズの下界を証明するための幾何学的アプローチが有望ではないかと考えている．そこで, 以下では, その幾何学的アプローチについて紹介していくことにする．

8 万能基底

通常のブール回路においては，AND, OR, NOT の 3 種類のゲートがあれば（実際は AND と NOT，または OR と NOT の 2 種類で十分），任意のブール関数を計算する回路を構成することができる．このような性質があるため，ゲートの集合 { AND, OR, NOT } は**万能基底**と呼ばれる．量子回路に対しては，次のような万能基底が知られている [6].

無限基底 ... 制御 NOT ゲートと，すべての 1 量子ビットユニタリ変換ゲートから成るゲートの**無限集合** G_U は万能基底である．任意の k 量子ビット ユニタリ作用素を，G_U に属する $O(4^k k)$ 個のゲートを用いて正確に模倣できることが知られている [6]．したがって，G_U から，局所的ユニタリ変換ゲートから成る別の万能基底（3 量子ビット ゲート全体の集合など）に切り替えても，対応する回路サイズは定数倍にしか増加しない．

有限基底 ... 任意の 2 量子ビット ゲートは，Hadamard ゲート

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

と，2 量子ビット ゲートである制御 V ゲート，ただし，

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

を，合計で $O(\log^c(1/\varepsilon))$ (c : 定数) 個用いて，与えられた近似率 ε 以内で近似できることが知られている．したがって，これら 2 つのゲートを含む集合は，任意のゲートを近似できるという意味において万能基底である．

入力が $x_1, x_2, \ldots, x_n$, 出力が $y_1, y_2, \ldots, y_m$ である量子回路 K は, 各入力 $x \in \{0,1\}^n$ に対し, $\{0,1\}^m$ 上の確率分布 p_x を対応させる．n 入力量子回路 K が QTM M を (n,t)-**模倣する**とは, K によって生成される確率分布 p_x の族が, 入力 x に対する t ステップの M の様相の確率分布と等しいときをいう．ただし, M の様相とは, テープセル $-t$ から t までに含まれるテープ記号のリストと, 状態およびヘッド位置を 2 進列として符号化したものとする．

定理 8.1 (Yao) M を QTM とし, n, t を正整数とする．このとき, M を (n,t)-模倣するような, サイズ $poly(n,t)$ の量子回路 K が存在する．

定理 8.2 (Yao) $L \in P$ ならば, L_n を受理する量子回路の最小サイズは $O(n^k)$ である．ただし, L_n は L に属する長さ n の記号列の集合とする． □

L_n に対する量子回路サイズの超多項式下界が得られれば，この定理 8.2 からただちに，$L \notin P$ が導かれる．このことは，量子回路計算量からの P = NP ? 問題に対する新たなアプローチの可能性を示唆している．

9 量子論理回路の深さ最小化

n 変数論理関数 $f:\{0,1\}^n \to \{0,1\}$ の値は, 演算の可逆性のために直接的には量子回路上では計算できない. しかし,

$$U_{f\text{-C-NOT}}|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \tag{9.1}$$

で定義される ***f*-C-NOT 回路**(f-Controlled-NOT 回路) で実質的に計算することができる. [12]

定義 9.1 (量子論理回路) 本稿では, これ以降, この $U_{f\text{-}C\text{-}NOT}$ を計算する回路 *(f-C-NOT 回路)* のことを**量子論理回路**と呼ぶことにする.

この作用素の入力は,

$$|x\rangle = |x_1\rangle|x_2\rangle|x_3\rangle\cdots|x_n\rangle \tag{9.2}$$

の形で n 量子ビットで構成される制御レジスタ x で保持される. そして出力は 1 量子ビットから成るレジスタ y を通して与えられる.

式 (9.1) における f-C-NOT 回路は, 最小項に対応するユニタリ変換である**最小項ゲート**で簡単に構成されうる. どの最小項ゲート M_y^x も

$$M_y^x \equiv \left(\prod N_{x_i}\right) T_y^x \left(\prod N_{x_i}\right) \tag{9.3}$$

のように NOT ゲートで挟まれた 1 つの $(n+1)$ ビット Toffoli ゲートによって実現されうる. ここで N_{x_i} と T_y^x は, それぞれ, 制御レジスタの第 i 量子ビットの状態だけを反転する NOT ゲートと, n 個の制御ビット x と 1 個のターゲットビット y を持つ $(n+1)$ ビット Toffoli ゲートを表す. その積 ($\prod$) は, 0 を持つような x のすべてのビットに関するものである. どの最小項ゲートも, 入力の 1 つの状態だけに対して動作する. また, 最小項ゲートの積の順序は, 可換である.

そして, f-C-NOT 回路は,

$$U_{f\text{-C-NOT}} = \prod M_y^x \tag{9.4}$$

のように, その最小項ゲートすべての積で得られる. ここで, この積は, $f(x)=1$ を満たす x に関するものである. 筆者らは, 以下の定理を示した。

定理 9.1 (Nakui et al.) 最小項ゲートの乗算は, 対応する論理表現においては, その最小項の排他的論理和 *(EXOR)* で表すことができる.

証明 最小項ゲートの定義, あるいは, Toffoli ゲートの定義から容易に示すことができる.

Toffoli ゲート T_y^x は, 次のように定義される.

$$\begin{aligned}
&\forall x_1,\ldots,x_n,y \in \{0,1\},\\
&T_y^x|x_1,\ldots,x_n,y\rangle\\
&\equiv \begin{cases} |x_1,\ldots,x_n\rangle \otimes N|y\rangle, & \text{if} \quad x_1\wedge\cdots\wedge x_n = 1\\ |x_1,\ldots,x_n,y\rangle, & \text{if} \quad x_1\wedge\cdots\wedge x_n = 0 \end{cases}
\end{aligned} \tag{9.5}$$

ここで, $a\wedge b$ は a,b の論理積を表し, $N=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ である. これは, また,

$$\begin{aligned}
&\forall x_1,\ldots,x_n,y \in \{0,1\},\\
&T_y^x|x_1,\cdots,x_n\rangle|y\rangle\\
&= |x_1,\ldots,x_n\rangle|y \oplus (x_1\wedge\cdots\wedge x_n)\rangle
\end{aligned} \tag{9.6}$$

と書くことができる. すなわち, これは, 作用前のターゲットビットの状態 y に論理積 $x_1\wedge\cdots\wedge x_n$ が EXOR で足しこまれることを意味する.

最小項ゲートの定義から, 最小項ゲートは, Toffoli ゲートにおける N が有効になる制御ビットの状態を (NOT ゲートを用いて) 最小項表現に一致するように変えただけである. したがって, 最小項ゲートを作用させるということは, 作用前のターゲットビットの状態にその最小項が EXOR で足し込まれることを意味する. □

定義 9.2 (積項ゲート) 各変数に対して高々*1* つのリテラル *($x,\bar{x}$)* を論理積で結合した式を**積項**と呼ぶことにする. *Toffoli* ゲートを *NOT* ゲートで挟み, この積項に対応する状態で制御されるようにしたゲートを**積項ゲート**と呼ぶことにする.

また, この積項ゲートについても次のことがいえる.

定理 9.2 (Nakui et al.) 積項ゲートの乗算は, 対応する論理表現においては, その積項の排他的論理和 *(EXOR)* で表すことができる. □

文献 [12] では, f-C-NOT 回路の簡単化のルールが 3 つ述べられている:

ルール 1 $m \le n$ に対して, 2 つの $(m+1)$ ビット積項ゲートの制御ビットの論理表現が, 1 つ

のビットの状態を除いて同じで, かつ, それらの 2 つのゲートが連続してあるならば, それらは, 1 つの m ビット積項ゲートによって置き換えられうる.

ルール 2 2 つの $(m+1)$ ビットの積項ゲートが連続してあり, かつ, それらの制御ビットの論理表現が 2 つのビットの状態を除いて同じならば, 1 つの m ビット積項ゲートと 2 つの C-NOT ゲートによって置き換えられうる.

ルール 3 f-C-NOT 回路に積項ゲートの偶数回のべき乗をかけても不変である.

定義 9.3 (ESOP) 任意の積項を排他的論理和で結合した *AND-EXOR* 論理式を ***ESOP(Exclucive-or Sum Of Product)*** と呼ぶ. また, 論理関数 f を *ESOP* で表現したときに積項数が最小になる *ESOP* を論理関数 f の **最小 *ESOP*** と呼ぶ.

以上のことから, 次の量子論理回路の深さ最小化定理が導かれる.

定理 9.3 (Nakui et al.) 論理関数 f の最小 *ESOP* は, *f-C-NOT* 回路に対する深さ最小の量子回路を与える.

証明 これまでに示した定理 9.1, 9.2, および, 積項ゲートの定義より, f-C-NOT 回路を構成する積項ゲートの数は, 論理関数 f の ESOP の積項数と一致し, ESOP から直接的に f-C-NOT 回路が構成できることがわかる.

また, 積項ゲートは, NOT ゲートで挟まれた Toffoli ゲートであるのでこれは, 高々深さ 3, すなわち, 定数オーダ深さ O(1) で構成されることになる.

したがって, f-C-NOT 回路全体の深さを浅くするためには, それの構成要素である積項ゲートの数を少なくすればよいことになる.

最小 ESOP は積項数が最小になるものであるから最小 ESOP が深さ最小の f-C-NOT 回路を与えることになる.

また, 逆に深さ最小の f-C-NOT 回路が与えられた場合, そこから, 最小 ESOP を求めることは, 容易である. □

10 量子回路計算量の下界導出に向けて

Nielsen は, 最近の論文 [15] において, 量子計算論において特徴的な幾何学的性質を利用して, 量子論理回路のサイズの下界を求める方法論を提案し, 以下の定理を示した. なお, Nieisen が示したこの証明法は, natural proof の範疇には入らないものである.

定理 10.1 (Nielsen) G を $SU(2^n)$ 上の万能量子基底とし, F を $SU(2^n)$ 上のある条件を満たす計量とするとき, $SU(2^n)$ に属する任意の U に対して, 以下が成り立つ.

$$d_F(I,U) \leq m_G(U)$$

ただし, $d_F(I,U)$ は, F を計量とする可微分多様体上における n 量子ビット恒等変換 I と U との距離, $m_G(U)$ は, ユニタリ変換 U を実現する G を基底とする量子回路の最小サイズとする. □

この定理と, 前節で示した定理 4.3 から, 以下の定理が導かれた.

定理 10.2 G を $SU(2^n)$ 上の万能量子基底とし, F を $SU(2^n)$ 上のある条件を満たす計量とするとき, 任意の $n-1$ 変数ブール関数に対応するユニタリ変換 U に対して, 以下が成り立つ.

$$d_F(I,U) \leq m_G(U) \leq n \cdot l_G(U) \leq n \cdot ESOP(U)$$

ただし, $l_G(U)$ は, ユニタリ変換 U を実現する G を基底とする量子回路で, 前述の条件を満たすものの最小深さとし, $ESOP(U)$ は, U に対応する $n-1$ 変数ブール関数の最小 *ESOP* の積項数とする. □

このような結果を足がかりとして, 今後, 具体的なブール関数に対する量子回路計算量の下界を示して行くためには, 以下のような問題が, まず最初に解決されなければならない.

1. 特定のブール関数に対応する U について, $d_F(I,U)$ の強い下界を求めること. Nielsen の結果は, 一般のユニタリ変換 U に関するものなので, 通常の計算量理論で議論されて

いるようなブール関数や, 特定の NP 完全問題に対応する U についての議論を展開し, $d_F(I,U)$ に対する強い下界を導き出して行く必要がある. 当然, Nielsen の論文では, 変換 U の一様性も成立していないが, 計算量理論を展開するためには, 変換 U の一様性についても考慮しなければならない.

2. 補助量子ビットが, 量子回路計算量に及ぼす影響を明らかにすること. Nielsen の論文では, 補助量子ビットの存在は仮定しない枠組みで, 結果が導かれている. しかし, 具体的な計算を行う通常の量子論理回路の設計においては, 補助量子ビットは頻繁に用いられるので, 補助量子ビットの存在が, 量子回路計算量の下界の導出にどのような影響を与えるのかを明らかにして行く必要がある. ちなみに, 前節で示した筆者らの結果においては, 補助量子ビットを用いない量子論理回路を取り扱っている.

以上のような問題を解決して行くことで, 量子論理回路を用いた回路計算量の下界導出に関する研究を推進していく計画である.

11 おわりに

本研究では, 量子回路計算量と制御 NOT ゲート数の関係について考察を行ない, さらに, 量子回路計算量の下界導出手法について研究を進めた. これまでの議論により, 量子回路計算量の評価においては, C-NOT ゲート数が本質的であることがわかったが, 一方, C-NOT ゲートや NOT ゲートのみでは, 単純な回路しか構成できないことも判明した. 今後の課題としては, C-NOT ゲートとある特定の 1 量子ビットゲートのみからなる回路のサイズを評価することなどがあげられる.

参考文献

[1] K. Amano, and A. Maruoka, "Potential of the approximation method", In *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, pp.431-440, 1996.

[2] T. P. Baker, J. Gill, and R. Solovay, "Relativizations of the P = NP question", *SIAM Journal on Computing*, Vol. 4, pp.431-442 (1975).

[3] A. Barenco, *et al.*: "Elementary gates for quantum computation", *Physical Review*, Vol. A 52 pp. 3457-3467, 1995.

[4] R. Beals, T. Nishino and K. Tanaka : "On the Complexity of Negation-limited Boolean Networks", *SIAM Journal on Computing*, Vol. 27, pp. 1334-1347 (1998).

[5] E. Bernstein and U. V. Vazirani, "Quantum Complexity Theory", *SIAM Journal on Computing*, Vol.26, No.5, pp.1411-1473, 1997. (An earlier version appeared in *Proc. 25th Annual ACM Symposium on Theory of Computing*, pp.11-20, 1993.)

[6] R. Cleve, "An Introduction to Quantum Complexity Theory", preprint quant-ph/9906111, 1999.

[7] D. Deutsch, "Quantum Theory,the Church-Turing Principle and the Universal Quantum Computer", *Proc. R. Soc. Lond.*, Vol. A 400, pp.97-117 (1985).

[8] D. Deutsch, "Quantum Computational Networks", *Proc. R. Soc. Lond.*, Vol. A 425, pp.73-90 (1989).

[9] P. E. Dunne, *The Complexity of Boolean Networks*, Academic Press (1988).

[10] M.R.Garey and D.S.Johnson: "COMPUTERS AND INTRACTABILITY A Guide to the Theory of NP-Completeness", Freeman, San Fransisco, 1979.

[11] 上坂吉則: 「量子コンピュータの基礎数理」, コロナ社, 2000.

[12] Jae-Seung Lee, Yongwook Chung, Jaehyun Kim, and Soonchil Lee: "A Practical Method of Constructing Quantum Combinational Logic Circuits", Department of

Physics, Korea Advanced Institute of Science and Technology, 1999. LANL quant-ph/9911053

[13] J. van Leeuwen (Ed.), *Handbook of Theoretical Computer Science, Vol. A, Algorithms and Complexity*, The MIT Press / Elsevier (1990) （邦訳：「コンピュータ基礎理論ハンドブック I」, 丸善, 第 14 章「有限関数の複雑さ」, by R. B. Boppana and M. Sipser, 西野哲朗訳）.

[14] Yukihide Nakui, Tetsuro Nishino and Seiya Okubo: On the Minimization of the Depth of Certain Quantum Circuits, International Symposium on Energy, Informatics and Cybernetics (EIC 2005), July 10-13, Orlando, Florida, USA (2005).

[15] M. A. Nielsen, "A geometric approach to quantum circuit lower bounds", quant-ph/0502070, Feb. 2005.

[16] 西野哲朗 :「量子コンピュータ入門」, 東京電機大学出版局, 1997.

[17] A. A. Razborov, "On the Method of Approximations", In *Proceedings of the 21st ACM Symposium on Theory of Computing*, pp.167-176, 1989.

[18] A. A. Razborov, and S. Rudich, "Natural Proofs", In *Proceedings of the 26th ACM Symposium on Theory of Computing*, pp.204-213, 1994.

[19] A. Yao, "Quantum Circuit Complexity", *Proc. 34th Annual IEEE Symposium on Foundations of Computer Science*, pp.352-361, 1993.

研究業績一覧

著書

1. 太田和夫，國廣昇:
"ほんとうに安全？現代の暗号（岩波科学ライブラリー）", 岩波書店, 2005.
概要: 今日のネット社会は暗号なしには成立しない。したがって、情報セキュリティの研究において暗号が大変重要となる。特に、公開鍵暗号と呼ばれる暗号は、見知らぬ人との通信を可能にしてくれる大変便利なものである。公開鍵暗号の多くは、素因数分解などの数学的問題の難しさを安全性の根拠としている。素因数分解は、一見簡単そうに見えるが、実は現在のコンピュータにとっては非常に難しい問題である。この素因数分解を高速に行う研究には、量子コンピュータも登場する。本書では、そのような暗号技術に関する最先端の話題を、易しく紹介して行く。まず、開発のエピソードをまじえながら、現在主流といなっている公開鍵暗号について解説する。素因数分解などの簡単な数学を用いて、暗号のしくみを実感する知的刺激に満ちた入門書である。さらに暗号解読の最新の研究も紹介しながら、暗号はどこまで安全か？量子コンピュータが実現したら暗号はどうなるのか？などの問題についても解説する。

学術論文

1. Yasuhiro Takahashi and Noboru Kunihiro: "A fast quantum circuit for addition with few qubits", Quantum Information and Computation, (2008, to appear).
概要: n 量子ビットので表現される 2 つの自然数値の和を $O(n/\log n)$ 個の補助量子ビットを用いて実現する回路を構成した。回路の深さは、$O(\log n)$ である。

2. Yasuhiro Takahashi, Noboru Kunihiro, and Kazuo Ohta:
"The Quantum Fourier Transform on a Linear Nearest Neighbor Architechture", Quantum Information and Computation, Vol.7, No.4, pp. 383–391, 2007.
概要: 量子アルゴリズムの物理的実現を考えた場合、隣接した量子ビットのみに演算を制限した回路を構成する必要がある。本論文では、隣接した量子ビットのみを用いた効率的な量子フーリエ変換を構成した。

3. J. Tarui:
"On the Minimum Number of Completely 3-Scrambling Permutations", Discrete Mathematics, published online Nov 2007, DOI:10.1016/j.disc.2007.07.069.
概要: 集合 $[n] = \{1, ..., n\}$ の置換の族 P は次の条件を満たすとき k-completely scrambling [Spencer 1972; Furedi 1996] と呼ばれる：任意の異なる $x_1, ..., x_k \in [n]$ に対して、置換 $\pi \in P$ により $\pi(x_1), ..., \pi(x_k)$ に関する $k!$ 個すべての順序が作られる。このような族の最小サイズを $N(n, k)$ とする。本論文では $k = 3$ にフォーカスする。シンプルな構成的方法により次の上界を与える： $N(n, 3) \leq (2 + o(1))log_2 n$. さらに $lim_{n\to\infty} N(n, 3)/(log_2 n) = c_3$ が存在することを示す。c_3 の値を決定することと $k \geq 4$ について $limN(n, k)/(log_2 n) = c_k$ の存在を示すことは未解決問題として残る。

4. K. Iwama, H. Morizumi, and J. Tarui:
"Negation-Limited Complexity of Parity and Inverters", Algorithmica, published online Dec 2007, DOI:10.1007/s00453-007-9135-1.
概要: 否定数限定計算量理論は, された個数の否定ゲートからなる回路の計算パワーを分析するものである. パリティ関数とインバーター関数を計算する否定限定回路のサイズに対する改良した下界を与える：(a) $n = 2^r - 1$ に対して, ゲート $r - 1$ 個を用いてパリティを計算する回路のサイズは $6n - \log_2(n + 1) - O(1)$ 以上である. (b) $n = 2^r - 1$ に対して, ゲート r 個を用いたインバーターのサイズは $8n - log_2(n+1) - O(1)$ 以上である.

5. Yu SASAKI, Yusuke NAITO, Noboru KUNIHIRO and Kazuo OHTA:
"Improved Collision Attacks on MD4 and MD5", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp.36-47, 2007.
概要: At Eurocrypt'05, Wang et al. presented efficient collision attacks on MD5 and MD4 hash functions. They found a collision of MD5 with a complexity of less than 2^37 MD5 hash operations, and a collision of MD4 with complexity less than 28 MD4 hash operations. In their attack, the procedure to generate a collision is divided into 4 steps. First, they determine the message differential and output differentials of chaining variables in each step, which generates a collision with small complexity. Second, they construct sufficient conditions that guarantee that the desired differential is always calculated. Third, they find a message modification that can satisfy the sufficient conditions with high probability. Finally, they search for a message that satisfies all sufficient conditions. In this paper, we focus on the message modification of MD5 and MD4, and propose a new message modification. Using our message modification, a collision of MD5 can be found with complexity less than 229 MD5 hash operations, and a collision of MD4 can be found with complexity less than 3 MD4 hash operations. To improve the complexity from previous attacks, we mainly use two ideas. The first idea is to use message modification that can satisfy more sufficient conditions in the second round than in previous attacks. The second idea is to use message modification that can enable us to search for a collision starting from an intermediate step.

6. Yuichi KOMANO, Kazuo OHTA, Atsushi SHIMBO and Shinichi KAWAMURA:
"Toward the Fair Anonymous Signatures: Deniable Ring Signatures", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp.54-64, 2007.
概要: Ring signature scheme enables a signer to sign a message anonymously. In the ring signature scheme, the signer who

wants to sign a document anonymously first chooses some public keys of entities (signers) and then generates a signature which ensures that one of the signer or entities signs the document. In some situations, however, the ring signature scheme allows the signer to shift the blame to victims because of the anonymity. The group signature scheme may be a solution for the problem; however, it needs an electronic big brother, called a group manager, who can violate the signer anonymity by himself, and a complicated key setting. This paper introduces a new notion of a signature scheme with signer anonymity, a deniable ring signature scheme (DRS), in which no group manager exists, and the signer should be involved in opening the signer anonymity. We also propose a concrete scheme proven to be secure under the assumption of the DDH (decision Diffie Hellman) problem in the random oracle model.

7. Haruki OTA, Kazuki YONEYAMA, Shinsaku KIYOMOTO, Toshiaki TANAKA and Kazuo OHTA:
"Universally Composable Hierarchical Hybrid Authenticated Key Exchange", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp. 139-151, 2007.
概要: Password-based authenticated key exchange protocols are more convenient and practical, since users employ human-memorable passwords that are simpler to remember than cryptographic secret keys or public/private keys. Abdalla, Fouque, and Pointcheval proposed the password-based authenticated key exchange protocol in a 3-party model (GPAKE) in which clients trying to establish a secret do not share a password between themselves but only with a trusted server. On the other hand, Canetti presented a general framework, which is called universally composable (UC) framework, for representing cryptographic protocols and analyzing their security. In this framework, the security of protocols is maintained under a general protocol composition operation called universal composition. Canetti also proved a UC composition theorem, which states that the definition of UC-security achieves the goal of concurrent general composition. A server must manage all the passwords of clients when the 3-party password-based authenticated key exchange protocols are realized in large-scale networks. In order to resolve this problem, we propose a hierarchical hybrid authenticated key exchange protocol (H2AKE). In H2AKE, forwarding servers are located between each client and a distribution server, and the distribution server sends the client an authentication key via the forwarding servers. In H2AKE, public/private keys are used between servers, while passwords are also used between clients and forwarding servers. Thus, in H2AKE, the load on the distribution server can be distributed to the forwarding servers concerning password management. In this paper, we define hierarchical hybrid authenticated key exchange functionality. H2AKE is the universal form of the hierarchical (hybrid) authenticated key exchange protocol, which includes a 3-party model, and it has the characteristic that the construction of the protocol can flexibly change according to the situation. We also prove that H2AKE is secure in the UC framework with the security-preserving composition property.

8. Yasuhiro Takahashi, Noboru Kunihiro, and Kazuo Ohta:
"The Quantum Fourier Transform on a Linear Nearest Neighbor Architecture", Quantum Information and Computation, Vol.7 No.4, pp.383-391, 2007.
概要: We show how to construct an efficient quantum circuit for computing a good ap-

proximation of the quantum Fourier transform on a linear nearest neighbor architecture. The constructed circuit uses no ancillary qubits and its depth and size are $O(n)$ and $O(nlogn)$, respectively, where n is the length of the input. The circuit is useful for decreasing the size of Fowler et al.'s quantum circuit for Shor's factoring algorithm on a linear nearest neighbor architecture.

9. Yoshikazu Hanatani, Yuichi Komano, Kazuo Ohta and Noboru Kunihiro:
"Provably Secure Untraceable Electronic Cash against Insider Attacks", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.5, (2007).
概要: Although a great deal of research has been done on electronic cash schemes with blind multisignatures to prevent an insider attack, there is no discussion of a formal security model in the literature. Firstly we discussed the security model of ecash schemes based on the blind multisignature scheme against a (restricted) attack model and proposed a concrete scheme proven to be secure in the model [1]; however, this attack model disallows an attacker from corrupting an issuing bank and shops in the forgery game. In this paper, first, we reconsider the security model to remove the restriction of the attack model. Second, we propose a new untraceable e-cash scheme with a blind multisignature scheme and prove that the proposed scheme is secure against the (non-restricted) attacks under the DDH assumption in the random oracle model.

10. Takashi Nishide and Kazuo Ohta:
"Constant-Round Multiparty Computation for Interval Test, Equality Test, and Comparison", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.5, (2007).
概要: We propose constant-round protocols for interval tests, equality tests, and comparisons where shared secret inputs are not given bitwise. In [9]. Damgard et al. presented a novel protocol called the bit-decomposition, which can convert a polynomial sharing of an element in prime field Z_p into sharings of bits. Though, by using the bit-decomposition protocol, those protocols can be constructed with constant round complexities theoretically, it involves expensive computation, leading to relatively high round and communication complexities. In this paper, we construct more efficient protocols for those protocols without relying on the bit-decomposition protocol. In the interval test protocol, checking whether a shared secret exists in the known interval is reduced to checking whether a bitwiseshared random secret exists in the appropriate interval. In the comparison protocol, comparing two shared secrets is reduced to comparing the two secrets via $p/2$ indirectly where p is an odd prime for an underlying linear secret sharing scheme. In the equality test protocol, checking whether two shared secrets are equal is reduced to checking whether the difference of the two secrets is zero and furthermore checking whether the difference is a zero is reduced to checking quadratice residuosity of a random secret in a probabilistic way.

11. Yasuhiro Takahashi and Noboru Kunihiro:
"A quantum circuit for Shor's factoring algorithm using $2n + 2$ qubits", Quantum Information and Computation, Vol.6 No.2, pp.184-192, 2006.
概要: We construct a quantum circuit for Shor's factoring algorithm that uses $2n + 2$ qubits, where n is the length of the number to be factored. The depth and size of the circuit are $O(n^3)$ and $O(n^3 logn)$, respectively. The number of qubits used in

the circuit is less than that in any other quantum circuit ever construted for Shor's factoring algorithm. Moreover, the size of the circuit is about half the size of Beauregard's quantum circuit for Shor's factoring algorithm, which uses $2n + 3$ qubits.

12. Yuichi Komano and Kazuo Ohta:
"Taxonomical Security Consideration of OAEP Variants", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp.1233-1245, 2006.
概要: We first model the variants of OAEP and SAEP by changing a construction and position of a redundancy, and establish a universal proof technique in the random oracle model, the comprehensive event dividing tree. We then make a taxonomical security consideration of the variants of OAEP and SAEP, based on the assumptions of one- wayness and partial-domain one-wayness of the encryption permutation, by applying the tree. Furthermore, we demonstrate the concrete attack procedures against all insecure schemes; we insist that the security proof failure leads to some attacks. From the security consideration, we find that one of the variants leads to a scheme without the redundancy; the scheme is not PA (plaintext aware) but IND-CCA2 secure. Finally, we conclude that some of them are practical in terms of security tightness and short bandwidth.

13. Mitsugu Iwamoto, Lei Wang, Kazuki Yoneyama, Noboru Kunihiro and Kazuo Ohta:
"Visual Secret Sharing Schemes for Multiple Secret Images Allowing the Rotation of Shares", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp.1382-1395, 2006.
概要: In this paper, a method is proposed to construct a visual secret sharing (VSS) scheme for multiple secret images in which each share can be rotated with 180 degrees in decryption. The proposed VSS scheme can encrypt more number of secret images compared with the normal VSS schemes. Furthermore, the proposed technique can be applied to the VSS scheme that allows to turn over some shares in decryption. From the theoretical point of view, it is interesting to note that such VSS schemes cannot be obtained from so-called basis matrices straightforwardly.

14. N. Kunihiro W. Abe and K. Ohta:
"Maurer-Yacobi ID based Key Distribution Revisited", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp.1421-1424, 2006.
概要: Maurer and Yacobi proposed an ID-Based key distribution scheme in 1991. In this scheme, the private key for each user is generated by solving discrete logarithm problem. We examine the realizability of this scheme. We show that this scheme can be practical by appropriate parameter setting.

15. 伊豆哲也，國廣昇，太田和夫，武仲正彦:
"双線形写像を用いた墨塗り署名方式の安全性について", 情報処理学会論文誌, Vol. 47, No. 7, pp.2409-2416, 2006.
概要: 部分情報がマスキング（墨塗り）された電子文書において，開示部分の完全性と非開示部分の秘匿を両立させる暗号要素技術として墨塗り署名が注目を集めている．2005年1月に宮崎・花岡・今井が提案した双線形写像を用いた墨塗り署名方式（本稿ではSUMI-6と呼ぶ）は上の性質に加え，墨塗り箇所数の秘匿と墨塗り者による開示条件のコントロールが可能という特徴を持っている．しかしアルゴリズムや技術が不十分であったり，条件の妥当性の議論に欠けたりするという問題があった．本稿はさらなる安全性解析を目的と

して SUMI-6 を詳細検討し，条件によっては可能となるいくつかの問題点を指摘する．また SUMI-6 の改良墨塗り署名方式 SUMI-6' を提案し，その安全性を議論する．さらに，宮崎らが別に提案した墨塗り署名方式 SUMI-5 に対して，双線形写像を用いて改良を施した墨塗り署名方式 SUMI-5' の提案・検討を行う．

16. Yasuhiro Takahashi and Noboru Kunihiro : "A quantum circuit for Shor's factoring algorithm using 2n+2 qubits", Quantum Information and Computation, Vol.6 No.2, pp. 184–192, 2006.
概要: We construct a quantum circuit for Shor's factoring algorithm that uses $2n + 2$ qubits, where n is the length of the number to be factored. The depth and size of the circuit are $O(n^3)$ and $O(n^3 \log n)$, respectively. The number of qubits used in the circuit is less than that in any other quantum circuit ever constructed for Shor's factoring algorithm. Moreover, the size of the circuit is about half the size of Beauregard's quantum circuit for Shor's factoring algorithm, which uses $2n + 3$ qubits.

17. Yasuhiro Takahashi and Noboru Kunihiro : "A Linear-Size Quantum Circuit For Addition With No Ancillary Qubits", Quantum Information and Computation, Vol.5 No.6, pp. 440–448, 2005.
概要: We construct a quantum circuit for addition of two n-bit binary numbers that uses no ancillary qubits. The circuit is based on the ripple-carry approach. The depth and size of the circuit are $O(n)$. This is an affirmative answer to the question of Kutin as to whether a linear-depth quantum circuit for addition can be constructed without ancillary qubits using the ripple-carry approach. We also construct quantum circuits for addition modulo 2^n, subtraction, and comparison that use no ancillary qubits by modifying the circuit for addition.

18. 大久保誠也, 西野哲朗, 太田和夫, 國廣昇: "物理的実現可能性に優れた NMR 量子探索アルゴリズム", 情報処理学会論文誌, Vol.46 No.06, pp. 1416–1425, 2005.
概要: 本論では，測定誤差が $\varepsilon < 1$ である NMR（Nuclear Magnetic Resonance）量子計算機（NMRQC と略記）上で動作する，新しい量子探索アルゴリズムを提案する．具体的には，解が複数個存在する探索問題に対する，新しい NMR 量子探索アルゴリズムを提案する．探索問題の解空間のサイズを N とするとき，このアルゴリズムは， $\varepsilon N + \min\{n, \log \varepsilon\}$ 回のオラクル呼び出しを行うことにより，成功確率 1 で解を発見する．通常の量子計算機上で成功確率 1 で解探索を行うためには，N 回のオラクル呼び出しが必要であることが知られているので，提案アルゴリズムの方がより高速に動作する．そして，量子オラクルを作り替えることができるような問題に対しては，提案アルゴリズムの実行において必要となる量子ビット数を節約できることを示す．さらに，提案アルゴリズムは，量子重ね合わせ状態を維持しなければならない時間が短いので，物理的実現可能性が非常に高い．

19. 大久保誠也, 西野哲朗, 太田和夫, 國廣昇: "Bulk 量子計算モデル上における Grover のアルゴリズムの繰り返し回数について", 情報処理学会論文誌:数理モデル化と応用, Vol.46, No.SIG 17, pp. 10–19, 2005.
概要: 本論文では，NMR 量子計算機をモデル化した，Bulk 量子計算モデル上で動作する，Grover のアルゴリズムの繰り返し回数について考察する．最初に，Bulk 量子計算モデル上で Grover のアルゴリズムを用いて論理式の充足可能性判定問題 (SAT) を解くのに必要となる繰り返し回数について議論する．次に，解がただ一つのみ存在する探索問題に対する量子アルゴリズムを提案する．また，この探索アルゴリズムの秘密鍵探索問題に対する応用についても述べる．さらに，解が複数存在する探索問題に対する量子アルゴリズムも提案する．以上の考察から，本論で提案する Bulk 量子計算モデルは，通常の量子計

算モデルよりも Grover のアルゴリズムを高速に実行できる場合があることがわかる.

研究会等

1. Wang and Kazuo Ohta and Noboru Kunihiro:
   "New Key Recovery Attack on HMAC/NMAC-MD4 and NMAC-MD5", Eurocrypt2008, (2008, to appear).
   概要: ハッシュ関数に基づくメッセージ認証方式である HMAC および NMAC の安全性に関して考察した。特に、HMAC-MD4, NMAC-MD4, NMAC-MD5 に対して、従来よりも効率的な攻撃を提案した。

2. Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro:
   "Security of MD5 Challenge and Response: Extension of APOP Password Recovery Attack", CT-RSA2008, (2008, to appear).
   概要: MD5 を用いたチェレンジ&レスポンス認証方式の脆弱性を指摘した。特に、メールの認証でよく使われている APOP 方式は、途中にルータをはさむなどの実現可能な攻撃に対して破られることを明らかにした。

3. Kouichi Itoh and Noboru Kunihiro and Kaoru Kurosawa:
   "Small Secret Key Attack on a variant of RSA (due to Takagi)", CT-RSA2008, (2008, to appear).
   概要: RSA 暗号の一つの変型判である、Takagi's RSA の秘密鍵が小さい場合には、解読されることを示した。特に、秘密鍵が、RSA の法である N に対して、$N^{0.595/(r+1)}$ 以下である場合には、多項式時間で破られることを示した。

4. J. Tarui:
   "Finding a Duplicate and a Missing Item in a Stream", TAMC07-LNCS: Lecture Notes in Computer Science: Proceedings of TAMC07: The 4th Annual Conference on Theory and Applications of Models of Computation, May 22-25, 2007, （to appear）.
   概要: 次のストリーム計算問題を考える. 入力は $a = \langle a_1, ..., a_m \rangle$, ただし各 $a_i \in \{1, ..., n\}$ で $m > n$. 入力の中の duplicate, すなわち, ある $d = a_i = a_l$, $i < l$ を s ビットのメモリーと r 回のパスによって見つけたい. アルゴリズムは1回のパスで入力を $a_1, ..., a_m$ の順に読む. 鳩の巣原理により duplicate は存在する. 次の下界を示す：$s = O(logn)$ であれば $r = \Omega(logn/loglogn)$.

5. Noboru Kunihiro and Kaoru Kurosawa:
   "Deterministic Polynomial Time Equivalence between Factoring and Key-Recovery Attack on Takagi's RSA", in Proc. of PKC2007, LNCS4450, pp.412-425, 2007.
   概要: RSA 暗号の一つの変型判である、Takagi's RSA の秘密鍵を求める問題と素因数分解問題が、決定性の意味で等価であることを示した。具体的には、秘密鍵が与えられたときに、素因数分解を行う決定性多項式時間アルゴリズムを構成した。

6. Seiya Okubo, Teruhito Aoki, and Tetsuro Nishino:
   "Quantum Circuit Complexity and the Number of Controlled-NOT Gates", ICT Triangle Forum 2007, Sept. 18-20, 2007, Beijing, China, 2007.
   概要: In this paper, we discuss relationships between quantum circuit complexity and the number of controlled NOT gates (C-NOT gates). First, we show that the order of the size of a quantum circuit is equal to the order of the minimum number of C-NOT gates which are necessary to construct the circuit. Next, we show that the size of the quantum circuit constructed by both of C-NOT gates and NOT gates is also $O(n^2)$ Furthermore, the number of possible patterns of the output generated by circuits constructed by both of C-NOT gates and NOT gates is at most 2^n times the number of the patterns of the output generated by circuits constructed by only C-NOT gates.

7. Seiya Okubo and Tetsuro Nishino:
"NMR Quantum Algorithms and Information Security", International Symposium on Advanced ICT (AICT) 2006, pp.289-297, August, 2006.
概要: In this paper, we propose the bulk quantum Turing machine (BQTM for short) which is a mathematical model of the NMR (Nuclear Magnetic Resonance) quantum computer (NMRQC for short) and two efficient quantum algorithms on BQTM to solve some problems which are closely related to some security problems. Namely, we discuss the computational complexity of the searching problem and the minimum finding problem on NMR quantum computers with the measurement accuracy ε. Since our proposed algorithm is more efficient than ordinary quantum algorithms on ordinary quantum computers, we can conclude that NMRQCs are more effective to security problems.

8. Shin-ichi Hashiba, Seiya Okubo and Tetsuro Nishino:
"Efficient Quantum Algorithms for Algebraic Problems", International Conference on Computer & Communication Engineering (ICCCE '06), pp.567-572, May 9-11, 2006.
概要: In this paper, we deal with so called counting problems. For these problems efficient classical or quantum algorithms are not known. But, these problems are very important in some practical applications. So, in this paper, we show how to efficiently compute the permanent of a matrix by using NMR quantum computation.

9. J. Tarui:
"On the Minimum Number of Completely 3-Scrambling Permutations", DMTCS-EuroComb05: DMTCS-Proceedigns of EuroComb05: European Conference on Combinatorics, Graph Theory and Applications (Berlin, Germanay, Sep05–09, 2005), pp. 351–356, 2005.
概要: A family $\mathcal{P} = \{\pi_1, \ldots, \pi_q\}$ of permutations of $[n] = \{1, \ldots, n\}$ is *completely k-scrambling* [Spencer, 1972; F̈uredi, 1996] if for any distinct k points $x_1, \ldots, x_k \in [n]$, permutations π_i's in $\mathcal{P}$ produce all $k!$ possible orders on $\pi_i(x_1), \ldots, \pi_i(x_k)$. Let $N^*(n,k)$ be the minimum size of such a family. This paper focuses on the case $k = 3$. By a simple explicit construction, we show the following upper bound, which we express together with the lower bound due to F̈uredi for comparison.

$$\frac{2}{\log_2 e} \log_2 n \leq N^*(n,3) \leq$$

$$2\log_2 n + (1 + o(1)) \log_2 \log_2 n.$$

We also prove the existence of $\lim_{n\to\infty} N^*(n,3)/\log_2 n = c_3$. Determining the value c_3 and proving the existence of $\lim_{n\to\infty} N^*(n,k)/\log_2 n = c_k$ for $k \geq 4$ remain open.

10. K. Amano and J. Tarui:
"Monotone Boolean Functions with s Zeros Farthest from Threshold Functions", DMTCS-EuroComb05: DMTCS-Proceedigns of EuroComb05: European Conference on Combinatorics, Graph Theory and Applications (Berlin, Germanay, Sep05–09, 2005), pp. 11–16, 2005.
概要: Let T_t denote the t-threshold function on the n-cube: $T_t(x) = 1$ if $|\{i : x_i = 1\}| \geq t$, and 0 otherwise. Define the distance between Boolean functions g and h, $d(g,h)$, to be the number of points on which g and h disagree. We consider the following extremal problem: Over a monotone Boolean function g on the n-cube with s zeros, what is the maximum of $d(g, T_t)$? We show that the following monotone function p_s maximizes the distance: For $x \in \{0,1\}^n$, $p_s(x) = 0$ if and only if $N(x) < s$, where

$N(x)$ is the integer whose n-bit binary representation is x. Our result generalizes the previous work for the case $t = \lceil n/2 \rceil$ and $s = 2^{n-1}$ by Blum, Burch, and Langford [BBL98-FOCS98], who considered the problem to analyze the behavior of a learning algorithm for monotone Boolean functions, and the previous work for the same t and s by Amano and Maruoka [AM02-ALT02].

11. N. Kanayama, M. Kida, N. Kunihiro, T. Nishino, K, Ohta and S. Okubo:
"Quantum Algorithms for Solving Exact Shortest Vector Problem", ERATO Workshop on Quantum Information Science 2005, pp. 179–180, 2005.
概要: In this paper, we propose a method for solving the shortest vector problem (SVP) by combing classical and quantum computations. Our method is composed of two steps. First, a searching space of the shortest vector is determined by classical computation. Next, the shortest vector in the fixed searching space is obtained by quantum computation. The complexity of quantum part depends on the size of searching space. Hence, as the searching space is smaller, we can find the shortest vector faster. We propose a method for choosing smaller searching space. First, we introduce a theorem characterizing a searching space of the shortest vector. By this theorem, we determine the appropriate searching space from the tentative shortest vector. Hence, we must obtain the relatively short vector before searching the true shortest vector. In this paper, we give a such vector by LLL-lattice basis reduction. Finally, we evaluate the efficiency of our LLL based Algorithm.

12. Y. Takahashi and N. Kunihiro:
"A Linear-size Quantum Circuit for Addition with no ancillary qubits", ERATO Workshop on Quantum Information Science 2005, pp. 113–114, 2005.
概要: We construct a quantum circuit for addition of two n-bit binary numbers that uses no ancillary qubits. The circuit is based on the ripple-carry approach. The depth and size of the circuit are $O(n)$. This is an affirmative answer to the question of Kutin as to whether a linear-depth quantum circuit for addition can be constructed without ancillary qubits using the ripple-carry approach. We also construct quantum circuits for addition modulo 2^n, subtraction, and comparison that use no ancillary qubits by modifying the circuit for addition.

文部科学省科学研究費補助金 特定領域研究 (課題番号 16092215)

B04: 回路計算量の下限の研究とその応用

築地は, 2 次数予想の証明, および格子暗号を解く量子アルゴリズムの開発を行った．陳は，築地と共同して相関データグラフから遺伝系統図を構築する問題の計算複雑さの研究，ならびに近似アルゴリズムの設計と解析を行った．松浦は k-CNF 式の非充足解の数え上げ, 組合わせゲームの解析, 有限オートマトンの状態数解析を行った.

研究組織

研究代表者： 築地 立家　東京電機大学 理工学部
研究分担者： 陳　致中　東京電機大学 理工学部
松浦 昭洋　東京電機大学 理工学部 (平成 17–19 年度)

交付決定額 (配分額)

平成 16 年度	3,500,000 円
平成 17 年度	3,500,000 円
平成 18 年度	3,900,000 円
平成 19 年度	1,800,000 円
合　計	12,700,000 円

研究成果の概要

- 学術誌
  雑誌名略称 (発表年), Journal of Combinatorial Optimization (2007 年), Theoretical Computer Science (2006 年), Journal of Algrithms (2006 年), IEICE Trans. on Information and Systems(2005 年) など
- 国際会議
  会議名略称 (開催地, 発表年), ALENEX/ANALCO08 (サンフランシスコ, 2008 年), MATH2007 (カイロ, 2007 年), ICOTA07 (神戸, 2007 年), COCOON04 (済州島, 2004 年), WG04 (ボン, 2004 年) など

1　はじめに

本研究の目的は,「回路計算量の下限研究における未解決問題の解決」と「下限研究の応用」にわけられる．前者は長期研究による革新的な結果が期待できる一方, 後者は比較的短期で着実な成果をあげることが期待される．以下に, 各々の要点を述べる．

「回路計算量の下限研究における未解決問題の解決」

回路計算量の下限研究はＮＰ完全性仮説に迫る伝統的な手法である．最近ラズボロフらは, 下限証明に関する既存の手法がＮＰ完全性仮説を証明「できない」ことを示した．新しい下限証明手法を開発することは理論計算機科学の最重要課題とみなされている（Workshop on Challenges for Theoretical Computer Science 2000）．そこで本研究は定数次数予想と呼ばれる次の数学予想の解決を目指す.「論理積関数は,『任意の定数 T および異なる素数 P, Q について, 上段は次数無制限の P 周期素子, 中段は次数無制限の Q 周期素子, 下段は次数 T の素子からなる 3 段回路』に関して指数下限をもつであろう.」この予想は 1990 年に Barrington により提起され, 下限証明技術の発達を促してきたが, T=1 の場合の 1 次数予想を除いて未解決である．本研究は 2 次数予想の解決を目指し, 定数次数予想の解決, そして ACC 回路の下限証明へと進む．これらはいずれもＮＰ完全性仮説にとり最重要の未解決問題であり, その解決により下限証明のための新しい代数的手法が創出されると考えられる．

「下限研究の応用」

- 築地は, 2 次数予想の証明, および格子暗号を解く量子アルゴリズムの設計と解析を行った.
- 陳は，築地と共同して相関データグラフから遺伝系統図を構築する問題の計算複雑さの研究，ならびに近似アルゴリズムの設計と解析を行った.
- 松浦は k-CNF 式の非充足解の数え上げ, 組合わせゲームの解析, 有限オートマトンの状態数解析を行った.

2　2 次数予想の解決

t 次数関数とは，t 次の $\mathbb{Z}_2$ 整数係数多項式 $P(x_1,\ldots,x_n)$ について $(-1)^{P(x_1,\ldots,x_n)}$ とかけるような関数のことである．ここでは, 論理関数を有限体上で計算する際の計算複雑さを考えたい．そこで，t 次数関数の定義域はブール球 $(x_1,\ldots,x_n)\in\{0,1\}^n$ とし，値域は任意に固定された，有限ガロア体 $\mathbb{F}\subseteq\{0,1\}$ とする．ただし，体 $\mathbb{F}$ の標数は奇数とする．このとき，t 次数予想とは，AND 関数を t 次数関数の $\mathbb{F}$ 上線形結合で書くときに, $2^{\Omega(n)}$ 個以上の非零成分を要するであろう，という予想である．この予想は，Barrington，Straubing，Thérien が 1990 年に書いた共著論文において提出された．彼らは，1 次数予想を解決している．本研究において，長年の未解決問題であった, 2 次数予想が解決された（投稿準備中）.

3　唯一最短格子ベクトル問題を解く量子アルゴリズムの設計と解析

唯一最短格子ベクトル問題を，各次元が多項式サイズの環で形成されるような多次元整数環上のサイモン問題に帰着させた．このように一般化されたサイモン問題を, さらに線型計画問題に帰着させて，多項式時間でとけることを確認した（投稿準備中）．以下において, この証明の概略を述べる.

3.1　はじめに

量子計算機とは, 量子力学の原理によって保障されている, 量子状態およびその量子力学的時間発展を模倣するような, 計算機構である．一般に, 量子状態はヒルベルト空間の要素として表現することができる．量子計算機の場合, ヒルベルト空間の基底は, エンタングルメント状態にあるようないくつかの量子ビットの量子状態によって, 形成されている．特に, n 個のエンタングルメント量子の量子状態は, 2^n 通りであるため, ヒルベルト空間の次元も 2^n となる．すなわち, 多項式個のエンタングルメント状態にあるような量子ビットを用意するだけで, 指数次元のヒルベルト空間における量子計算を模倣することが可能となる.

とくに, 模倣したい並列計算の計算分岐の全てを, この巨大な次元の中に完全に埋め込むことが可能となる．これにより, 量子並列計算が実現される．

実際, P. Shor (P. Shor, Algorithms for quantum computation: Discrete log and factoring, in Proc. 35th FOCS, pp 124-134, 1994) は, この量子並列計算のおかげで, 素因数分解や離散対数計算が, 量子多項式時間で実行可能であることを証明した．これらの問題は, 通常の古典計算機では, 経験上, 計算困難な問題として知られている．さらに, 現代暗号の安全性は, これらの問題の計算困難性に立脚して, 保障されている．しかしながら, 暗号理論の要請という観点からも, 古典計算機では計算困難と予想されている問題の中で, 量子コンピュータが解くことができることが証明されている問題は, 極めて限定されている．

そこで, この研究活動報告においては, この, 量子計算理論における根本的な未解決問題に答えるような, 新たな結果を報告する．すなわち, 唯一最短格子ベクトル探索が, 量子多項式時間で実行可能であることを証明する．さらに, より強い結果として, 一般の 2 面体群の隠れ部分群問題が, 量子多項式時間で実行可能であることを, 証明する．一般に, 群 G の隠れ部分群問題とは, 次の特徴を持つような, G 上の関数 f についてのブラックボックスを用いることにより, 群 G の任意の隠れ部分群 H を発見するような問題である．ここで, f の特徴とは,「$f(g) = f(g') \Leftrightarrow gH = g'H$」である．この隠れ部分群問題は, 効率的な量子アルゴリズムを研究する分野においては, 大変に一般的な問題として知られている．とくに, これまでに研究された, 効率的な量子アルゴリズムをもつことが証明されているような問題は, ほとんど全て, アーベル群上の隠れ部分群問題に帰着することが知られている．(M.A. Nielson and I.L. Chan, Quantum Computation and Quantum Information, pp 241 参照)

さらに, アーベル群上の隠れ部分群問題は, 次の特徴を持つような $\{0, 1, \ldots, N-1\}$ 上の関数 f に関するブラックボックスを用いることにより, 任意の周期 d を発見するような問題に帰着することが知られている．ここで, f の特徴とは,「$f(x) = f(x') \Leftrightarrow |x - x'| \in \{0, d\}$」である．さらに, この周期発見問題は, 標準的な量子サンプリングの手法によって, 次のようなブラックボックスを用いることにより, d を発見する問題に帰着される．

Definition 1 ℓ は 2 以上の整数であり, $0 \leq \delta \leq 1$ は実数であるとする．$\{0, 1, \ldots, N-1\}$ 上で定義されいる, δ ノイズつきの d 周期 ℓ 点状態生成機とは, 次のように定められる一定の混合状態 $(1-\delta)\rho_\ell + \delta\rho_{\ell-1}$ を出力するようなブラックボックスである．ただし, 正整数 ℓ について, $\rho_\ell = \sum_{i=0}^{N-d\ell+d-1} p_{a,x}|\psi_{\ell,x}\rangle\langle\psi_{\ell,x}|$, $p_\ell = \{p_{\ell,x}\}_x$ は任意の確率, $|\psi_{\ell,x}\rangle = \frac{1}{\sqrt{\ell}} \sum_{i=0}^{\ell-1} |x + di\rangle$ である．

Definition 2 δ ノイズつき ℓ 点状態生成機による周期発見問題とは, 任意に与えられた δ ノイズつきの d 周期 ℓ 点状態生成機にアクセスすることにより, 高確率で d を発見する問題である．

とくに, $\ell = \Omega(d)$ の場合, P.Shor のアルゴリズムは, 任意の $0 \leq \delta \leq 1$ について, δ ノイズつきの ℓ 点状態生成機による周期発見問題を多項式時間以内で解くことができる．さらに, アーベル群上の隠れ部分群問題は, この, $\ell = \Omega(d)$ の場合の δ ノイズつきの ℓ 点状態観測による周期発見問題に帰着することができる．

3.2 2 点状態生成機による周期発見問題

一方, 2 面体群上の隠れ部分群問題は, M.Ettinger と P.Høyer の共同研究 (On Quantum Algorithms for Noncommutative Hidden Subgroups, Appl. Math., 25:239-251, 2000) を応用することにより, 1/2 以下のノイズつきの 2 点状態生成機による周期発見問題に帰着することがわかる．さらには, 任意の定数 $\epsilon > 0$ について, $n^{1/2+\epsilon}$ 唯一最短ベクトル問題も, O. Regev の研究（Quantum Computation and Lattice Problems, in Proc. 43rd FOCS, pp 520-529, 2002）により, 同じ問題に帰着することがわかる．そこで, 本研究報告においては, 以降, ノイズつきの 2 点状態生成機による周期発見問題を扱う．

まず, 1 ノイズつきの 2 点状態生成機は, 常に基底状態を生成するために, d に関する情報が全く得られないことに注意されたい．この事実を拡張することにより, 以下の定理が得られる．

Theorem 1 $1-\delta$ が無視できる量（つまり, その逆数が超多項式的な量 $\mathrm{superpolylog}(N)$ であること）であるとき, δ ノイズつき 2 点状態生成機による周期発見問題を多項式時間以内で解くことはできない.

一方, 本研究報告においては, ノイズの量を限界値にいたる寸前まで最大に設定したとしても, ノイズつき 2 点状態生成機による周期発見問題を多項式時間以内で解くことができることを証明する.

Theorem 2 $1-\delta$ が無視できない量（つまり, その逆数が多項式的な量, つまり $\mathrm{polylog}(N)$, であること）であるとき, δ ノイズつき 2 点状態生成機による周期発見問題は多項式時間以内で解くことができる.

この定理の系として, 以下の定理が得られる.

Theorem 3 2 面体群上の隠れ部分群問題は, 量子多項式時間で解くことができる.

Theorem 4 $n^{1/2+\epsilon}$ 唯一最短ベクトル問題は, 量子多項式時間で解くことができる.

3.3 量子フーリエサンプリング

標準的な量子フーリエサンプリングは, $\{0,1,\ldots,N-1\}$ 上で定義されている d 周期 2 点状態（d 周期 2 点状態生成機で生成される量子混合状態）に, 量子フーリエ変換 $F_N = \frac{1}{N}\sum_{x,y=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} xy/N}|x\rangle\langle y|$ を施してから, 観測を行うことにより, サンプリングを行う. この結果得られたサンプルに対応する確率変数を $\mathbf{Z}$ とする. M.Ettinger と P.Høyer の共同研究によると, ノイズフリーで, $d \neq 0, N/2$ であるかぎり, $\mathbf{Z}$ の定める確率は, $\mathbf{P}[Z=a] = \frac{2}{N}\cos^2(\pi da/N)$ となる.

彼らの共同研究の主たる目的は, この確率変数 $\mathbf{Z}$ を解析することにより, d を発見する効率的な方法を確立することであった. 実際, $\cos(2\pi k\mathbf{Z}/N)$ の期待値を計算してみると, $k \in \{d, N-d\}$ の場合に $1/2$ となり, それ以外の場合は 0 となる. そこで, $O(N)$ 個のサンプルをとってからこの期待値を近似することにより, d を一意的に決定することができる. しかしながら, 最大化問題 $\max_k \cos(2\pi k\mathbf{Z}/N)$, $k \in \{0,1,\ldots,N-1\}$, を多項式時間以内にとくような手法は, 今のところ見つかっていない.

そこで, 本研究報告では, この標準的な量子フーリエサンプリングに改良を加えることにより, 最終的に, 2 点状態生成機による周期発見問題を線形計画問題に帰着させることを試みる. 以降, 本セクションにおいては, まず, 我々が採用する量子フーリエ変換についての定義を行い, 次に, その量子フーリエ変換を 2 点状態に施してサンプリングを行うときに得られるであろう確率変数の確率解析をおこなう.

$m = O(\log N)$ は十分大きな整数であるとする. 奇素数を 5 から初めて小さい順に m 個とり, $5 = p_1 < p_2 < \ldots < p_m$ とするとき, 次の事実が満たされる.

Fact 1 $\prod_{i=1}^m p_i \geq N$ である. また, $p_m = O(\log N \log\log N)$ である.

この事実により, 定義域の集合 $\{0,1,\ldots,N-1\}$ を剰余環 $\mathbb{Z}_{p_i}$ の積モジュール $\prod_{i=1}^m \mathbb{Z}_{p_i}$ に埋め込むことが可能となる. しかも, この埋め込み変換およびその逆変換は効率的な変換である. そこで, $[p_i] = \{j - \frac{p_i-1}{2} : 0 \leq j \leq p_i - 1\}$ において, その各要素 $j - \frac{p_i-1}{2}$ を $\mathbb{Z}_{p_i}$ の剰余とみなすことにより, $[p_i]$ と $\mathbb{Z}_{p_i}$ を同一視する. これにより, 定義域の集合 $\{0,1,\ldots,N-1\}$ は積モジュール $\prod_{i=1}^m [p_i]$ の中に, 効率的に埋め込まれたことになる. さらに, $\tilde{m} = O(\mathrm{polylog}(N))$ を十分大きくとって, この積モジュールに余分な次元である $[3]^{\tilde{m}-m}$ を付け足すことにする. この付け足しにおいて, $x \in \{0,1,\ldots,N-1\}$ を積モジュール $\prod_{i=1}^m [p_i] \times [3]^{\tilde{m}-m}$ に埋めむ際の $[3]^{\tilde{m}-m}$ 成分は, $(1,\ldots,1)$, というように 1 を $\tilde{m}-m$ 回だけ反復することとする. この次元付け足し埋め込みの理由は, 後々の量子フーリエサンプリングの出力に対する確率解析の際に, 出力結果の従う確率変数が安定的な正規分布となるようにするためである. （この方が数学的な解析が容易となるからであり, 次元の付け足しが量子計算の実際上必要であることを主張するものではない.）以上のことから, 本研究報告においては, 表記を簡易に記するために, $p_{m+1} = \cdots = p_{\tilde{m}} = 3$ と定める. そして, 積モジュール $\prod_{i=1}^{\tilde{m}} [p_i]$ を $D_{\tilde{m}}$ と表記して,「拡大され

た定義域」と呼ぶことにする．また, $\tilde{N} = \prod_{i=1}^{\tilde{m}} p_i$ をこの拡大された定義域のサイズとする．

また, $D_m = \prod_{i=1}^{m}[p_i]$ と記して, $d \in D_m$ と $d = (d_1, \ldots, d_m, 1, \ldots, 1) \in D_{\tilde{m}}$ を同一視することにより, D_m を $D_{\tilde{m}}$ に埋め込む．さらに, $R_m = \prod_{i=1}^{m}[-\frac{p_i-1}{2}, \frac{p_i-1}{2}]$ および $R_{\tilde{m}} = \prod_{i=1}^{\tilde{m}}[-\frac{p_i-1}{2}, \frac{p_i-1}{2}]$ を m 次元および $\tilde{m}$ 次元の実閉領域として, $x \in R_m$ を $x = (x_1, \ldots, x_m, 1, \ldots, 1)$ と同一視することにより, R_m を $R_{\tilde{m}}$ に埋め込む.

本研究報告においては, 拡大された定義域 $D_{\tilde{m}}$ 上で自然に定義される, 次の量子フーリエ変換を行う．

Definition 3

$$\bigotimes_{i=1}^{\tilde{m}} F_{p_i} = \frac{1}{\tilde{N}} \sum_{x,y \in D_{\tilde{m}}} \mathrm{e}^{2\pi \mathrm{i} \sum_{i=1}^{\tilde{m}} \frac{x_i y_i}{p_i}}$$

この量子フーリエ変換を $\{0, 1, \ldots, N-1\}$ で定義されている d 周期 δ ノイズつき 2 点状態 $\delta\rho_2 + (1-\delta)\rho_1$ に施して観測し, 確率分布を調べたい．そのために, まず, d 周期の純粋 2 点量子状態 $|\psi_{2,x}\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |x+d\rangle)$, および純粋 1 点状態（すなわち純粋基底状態） $|\psi_{1,x}\rangle = |x\rangle$ に施して, 測定してみると, 次の結果が得られる．

Lemma 1 $\bigotimes_{i=1}^{\tilde{m}} F_{p_i}|\psi_{2,x}\rangle$ を観測してえられる出力の従う確率変数を $X \in D_{\tilde{m}}$ とすると, 任意の $a \in D_{\tilde{m}}$ について,

$$\mathbf{P}[X = a] = \frac{2}{\tilde{N}} \cos^2(\pi(\sum_{i=1}^{m} \frac{a_i d_i}{p_i} + \sum_{i=m+1}^{\tilde{m}} \frac{a_i}{3}))$$

となる．とくに, 確率変数 X は, x に依存しない量となる．

Lemma 2 $\bigotimes_{i=1}^{\tilde{m}} F_{p_i}|\psi_{1,x}\rangle$ を観測してえられる出力の従う確率変数を $U \in D_{\tilde{m}}$ とすると, 任意の $a \in D_{\tilde{m}}$ について,

$$\mathbf{P}[U = a] = \frac{1}{\tilde{N}}$$

となる．とくに, 確率変数 U は, x に依存せず, $D_{\tilde{m}}$ 上の一様分布となる．

Corollary 1 $\bigotimes_{i=1}^{m} F_{p_i}((1-\delta)\rho_2 + \delta\rho_1)$ を観測して得られる出力が従う確率変数は, $\delta X + (1-\delta)U$ である．

この系により, 確率変数 $\delta X + (1-\delta)U$ から得られるサンプリングを解析することにより周期 d を見つける効率的な方法があれば, Theorem 2 を証明できたことになる．d を発見するもうひとつの手法として, 確率変数 $\delta X + (1-\delta)U$ と確率変数 U を効率的に識別する方法を確立することが挙げられる．この手法のアイデアについて, 以下に概略を述べる．

周期 $d = (d_1, \ldots, d_m) \in D_m$ を効率的に計算するためには, 任意に与えられた素数 p と 剰余 $m \in \{0, 1, \ldots, p-1\}$ と d の任意の成分 d_i について, $d_i \equiv m (\mathrm{mod} p)$ であるか否かを効率的に識別することができれば, 十分である．O. Regev の研究を拡張すれば, ある一定の δ ノイズつき d 周期 2 点状態を出力するようなブラックボックスが与えられたとき, 以下のようなブラックボックスを効率的に構成することができる．このブラックボックスは, $d_i \equiv m (\mathrm{mod} p)$ である場合には, ある一定の δ ノイズつき d' 周期 2 点状態を出力し, そうでない場合は, ある一定の 1 点状態（すなわち, 純粋基底状態のみを含むような量子混合状態）を出力する．ただし, d' は d の第 i 成分 d_i を $\frac{d_i - m}{p}$ で置き換えたものである．

このように, Corollary 1に O. Regev の研究を適用することにより, 次の系が得られる．

Corollary 2 確率変数 $\delta X + (1-\delta)U$ と U を（古典計算量の意味で）多項式時間以内で識別することができれば, *Theorem 2* が証明できたことになる．

3.4 確率変数の識別

本節ににおいては, 確率変数 X と U の古典計算機による効率的な識別を行う．前節の Corollary 2 では, $(1-\delta)X + \delta U$, ただし $1-\delta$ は無視できない量, と U を識別するはずであった．しかし, 証明は本質的に変わらないため, 以下においては, X と U の識別について議論する．

確率変数 U は $D_{\tilde{m}}$ 上の一様分布である．このことから, 任意に与えられた $x \in R_m$ について, 内積 $\frac{\ell(x,U)}{\sigma(x)}$ を正規確率分布 $\mathfrak{n}(u) = \mathrm{e}^{-\frac{u^2}{2}}$ で近似することができる．ただし,

Definition 4 任意の実ベクトル $x \in R_m$ にたいして,

$$\sigma(x) = \sum_{i=1}^{m} \frac{p_i^2 - 1}{12} x_i^2 + \frac{1}{3}(\tilde{m} - m)$$

と定義する.

さらには, $\frac{\ell(x,U)}{\sigma(x)}$ が奇関数であるため, Berry-Essen 定理 (W. Feller, An Introduction to Probability Theory and Its Applications, vol 2, chap XVI 参照) により, 次が成り立つ.

Lemma 3 与えられた $x \in R_{\tilde{m}}$, および任意に実数 t について, 以下の近似式が成立する.

$$|\mathbf{P}[\frac{\ell(x,U)}{\sigma(x)} < t] - \int_{u=-\infty}^{t} \mathfrak{n}(u)du| = O(\frac{1}{\tilde{m}})$$

Berry-Essen 定理の証明を修正することにより, 次の Lemma も証明できる.

Lemma 4 与えられた $x \in R_{\tilde{m}}$ について, 以下の近似式が成立する.

$$|\mathbf{E}[\frac{\ell^2(x,U)}{\sigma^3(x)}] - 2\int_{u=-\infty}^{0} u^2 \mathfrak{n}(u)du| = O(\frac{1}{\tilde{m}})$$

Lemma 5 以下の近似式が成立する.

$$|\mathbf{E}[\frac{\ell^2(d,X)}{\sigma^3(x)}] - 4\int_{u=-\infty}^{0} u^2 \cos^2(\pi u)\mathfrak{n}(u)du| = O(\frac{1}{\tilde{m}})$$

Lemma 6

$$2\int_{u=-\infty}^{0} u^2 \mathfrak{n}(u)du - 4\int_{u=-\infty}^{0} u^2 \cos^2(\pi u)\mathfrak{n}(u)du = -2.5...$$

以降においては, 与えられた確率変数 Y が X または U であるとき, $Y = U$ と仮定して, 期待値 $\mathbf{E}[\ell^2((\sqrt{d_1}, \ldots, \sqrt{d_m}), Y)]$ の計算を行う. もし, $Y = X$ ならば, それが計算の途中でばれることを証明する. 具体的には, 次の最小化問題をとく. ただし, C は $C - \frac{1}{\mathrm{polylog}(N)} \leq \sigma^2(d) \leq C$ を満たすように与えられる. ここで $\frac{1}{\mathrm{polylog}(N)}$ は十分小さい数, とする.

Problem 1

$$\max_{\substack{x \in \prod_{i=1}^{m} [-(\frac{p_i-1}{2})^2, (\frac{p_i-1}{2})^2] \\ : \sigma^2(\sqrt{x_1}, \ldots, \sqrt{x_m}) \leq C}} \mathbf{E}[\ell^2((\sqrt{x_1}, \ldots, \sqrt{x_m}), Y)]$$

この問題において, 制約条件 $\sigma^2(\sqrt{x_1}, \ldots, \sqrt{x_m}) \leq C$ は線形式であることに注意されたい. また, 本報告においては, この問題自体を解くのではなく, その近似版を解く. 具体的には, 十分大きな整数 $k = \mathrm{polylog}(N)$ について, Y から独立ランダムに k 回サンプリングを行い, 得られたデータを $a_1, \ldots, a_k$ とする. このデータを基にして平均値 $\frac{1}{k}\sum_{i=1}^{k} \ell^2((\sqrt{x_1}, \ldots, \sqrt{x_m}), a_i))$ を計算する. この平均値は, サンプル数 k を十分大きくとれば, 全ての $x \in \prod_{i=1}^{m} [-(\frac{p_i-1}{2})^2, (\frac{p_i-1}{2})^2]$ について, $\mathbf{E}[\ell^2((\sqrt{x_1}, \ldots, \sqrt{x_m}), Y)]$ に十分近いことがいえる. 実際, Hoeffding の不等式によれば, 両者の間の差の絶対値は, $O(\tilde{m}\sqrt{\frac{\log k}{k}})$ で抑えられる. しかも, $\ell((\sqrt{x_1}, \ldots, \sqrt{x_m}), a_i))$ の係数の絶対値の和は $O(\tilde{m})$ であることを考慮すれば, すべての実ベクトル $x \in \prod_{i=1}^{m} [-(\frac{p_i-1}{2})^2, (\frac{p_i-1}{2})^2]$ について, 両者の差の絶対値が上記のように小さいことが証明できる. そこで, Definition 1 の近似版として, 次の問題を定義する.

Problem 2

$$\max_{\substack{x \in \prod_{i=1}^{m} [-(\frac{p_i-1}{2})^2, (\frac{p_i-1}{2})^2] \\ : \sigma^2(\sqrt{x_1}, \ldots, \sqrt{x_m}) \leq C}} 1/k \sum_{i=1}^{k} \ell^2((\sqrt{x_1}, \ldots, \sqrt{x_m}), a_i))$$

先に述べたことから, この問題の解である最大値と, Problem 1の解である最大値との差の絶対値は, $O(\tilde{m}\sqrt{\frac{\log k}{k}})$ で抑えられる. この量は, サンプル数 k を十分おおきくとれば, 十分小さくできる. さて, $Y = U$ という仮定のもとでは, U の各成分はランダム独立であるために, 任意の $1 \leq i \neq j \leq \tilde{m}$ について, 期待値 $E[U_i U_j] = 0$ となる. よって, 平均値 $\frac{1}{k}\sum_{i=1}^{k} \ell^2((\sqrt{x_1}, \ldots, \sqrt{x_m}), a_i))$ を展開して $\sqrt{x_i x_j}$ の係数を計算すると, ほぼ 0 になるはずである. Hoeffding の不等式を適用すれば, サンプル数 $k = \mathrm{polylog}(N)$ を十分おおきくとることにより, $\sqrt{x_i x_j}$ の係数の絶対値は, $O(\sqrt{\frac{\log k}{k}})$ 以下であると仮定できる. もしも $\sqrt{x_i x_j}$ の係数がそれよりも大きければ, $Y = U$ という仮定が間違っていたことになり, $Y = X$ であると断定できる. 同様に, $\sqrt{x_i}$ の係数も, 期待値 $E[U_i U_j] = 0$, $j > m$, であるために, $O(\tilde{m}\sqrt{\frac{\log k}{k}})$ 以下であると仮定できる. そこで, Definition 2 の近似版として, 次の問題を定義する.

Problem 3

$$\max_{\substack{x\in\prod_{i=1}^{m}[-(\frac{p_i-1}{2})^2,(\frac{p_i-1}{2})^2] \\ :\ \sigma^2(\sqrt{x_1},\ldots,\sqrt{x_m})\le C}} \sum_{i=1}^{k} A_i x_i + C$$

ただし, A_i は $\frac{1}{k}\sum_{i=1}^{k}\ell^2((\sqrt{x_1},\ldots,\sqrt{x_m}),a_i))$ を展開したときの x_i の係数である．また, C はその展開式における定数項である．

この問題の解である最大値と, Problem 2の解である最大値との差の絶対値は, 高々 $O(\tilde{m}^2\sqrt{\frac{\log k}{k}})$ である．サンプル数 k を十分大きくとれば, この量は十分に小さくなる．また, この問題は, 目的関数も制約条件関数も線形式であるために, 多項式時間で解くことができる．このとき, 実際に $Y = U$ であれば, Lemma 4により, Problem 3をといた結果の最大値を $C^{3/2}$ で割った値は, $2\int_{u=-\infty}^{0} u^2\mathfrak{n}(u)du$ で近似されるはずである．一方, 実は $Y = X$ であったとすれば, Lemma 5により, その値は $4\int_{u=-\infty}^{0} u^2\cos^2(\pi u)\mathfrak{n}(u)du$ 以上の値で近似されるはずである．Lemma 6により, 後者の値は前者の値よりも 2.5 以上大きいため, この時点で, もしも $Y = X$ であったとすれば, そのことが明らかとなる．

以上により, U と X を多項式時間で識別できることが示された．Corollary 2も, 同様にして, 証明することができる．

4 相関グラフから遺伝系統図を構築する問題の計算複雑さ，ならびにその近似アルゴリズムの設計と解析について

与えられたグラフが非連結の場合でも，遺伝系統図の次数が有限であれば，ダイナミックプログラミングの手法が適用できて，線形時間アルゴリズムが適用されることを確認した．証明の詳細は, (Zhi-Zhong Chen and Tatsuie Tsukiji, Computing Bounded-Degree Phylogenetic Roots of Disconnected Graphs, Journal of Algrithms, 59(2), pp. 125-148, 2006) に譲る．また，遺伝系統図の次数が有限で，かつデータが誤差を含むとき，最適化問題の解法がＮＰ困難であることを証明した．証明の詳細は, (Tatsuie Tsukiji and Zhi-Zhong Chen, Computing Phylogenetic Roots with Bounded Degrees and Errors Is Hard, Theoretical Computer Science, 363(1)pp. 43-59, 2006) に譲る．

5 k-CNF 式の非充足解の数え上げ

5.1 k-CNF 式に対する整除原理

k-CNF 式の充足解の数え上げ問題（$\#k-$SAT）は, $k \geq 2$ のとき #P 完全であることが知られる．そのため, $\#k-$SAT を解く多項式時間アルゴリズムは存在しないと一般に考えられている．一方で, k-CNF 式の非充足解を数え上げるナイーブな方法として, 整除原理 (Inclusion-Exclusion Principle) を用いた方法が知られる．今 ϕ を n 変数, m 項を有する k-CNF 式とし, A_i を i 番目の項を 0(非充足) とする n 変数への変数割当の集合とする．このとき, ϕ の非充足解の総数は次の式より計算される:

$$\begin{aligned}|\bigcup_{i=1}^{m} A_i| &= \sum_{i+1}^{m}|A_i| - \sum_{i<j}|A_i\bigcap A_j| \\ &+ \sum_{i<j<k}|A_i\bigcap A_j\bigcap A_k| \\ &- \cdots \\ &+ (-1)^{m-1}|\bigcap_{i=1}^{m} A_i|.\end{aligned}$$

(但し, $|A_i|$ は A_i の要素数)　本式は $2^m - 1$ 項有するため, その直接的な計算は一般に m の指数時間を要する．Kahn らは, (Combinatorica, Vol. 16, pp. 465-477, 1996) において, n 変数 CNF 式の非充足解の総数は, $|S| \leq \log n + 1$ なる項集合 S の情報により一意に定まることを示した．その証明は “existential” なものであったが, その後, Melkman らにより, 上記整除原理の公式において, $|S| \leq \log n + 1$ なる S 全体に対する $|\bigcap_{i\in S} A_i|$ から非充足解の総数 $|\bigcup_{i=1}^{m} A_i|$ を陽に計算する手法が示された (Discr. Appl. Math., Vol. 73, pp. 23-26, 1997)．その後, Amano らにより, n 変数 k-CNF 式の非充足解の総数は, $|S| \leq \lfloor \log k \rfloor + 2$ なる項集合 S に対する $|\bigcap_{i\in S} A_i|$ の値により一意に定まることが示された (Inform. Process. Lett.,

Vol. 87, pp. 111-117, 2003). しかし, そこでも非充足解の総数を具体的に計算する方法は示されなかった. 今回, 我々はそのような手続きを示す.

5.2 主要結果

主要結果の説明のため, いくつか準備を行う. l ($\leq m$) を固定し, 二つの n 変数 k-CNF 式 $\phi = c_1c_2\cdots c_m$, $\psi = d_1d_2\cdots d_m$ が次の条件を満たすとする：$\forall S \subset \{1,2,\cdots,l\}$ s.t. $|S| \leq l-1$,

$$|\bigcap_{i\in S} c_i| = |\bigcap_{i\in S} d_i|.$$

ここで $\bigcap_{i\in S} c_i$ を $\{c_i\}_{i\in S}$ に共通の変数集合とし, $\bigcup_{i\in S} c_i$ を $\{c_i\}_{i\in S}$ の異なる変数の集合とする ($\{d_i\}$ についても同様). すると, 全ての項 c_i が正リテラルから成るとき, 次の式が成り立つ.

$$\forall S \subset \{1,2,\cdots,m\},\ |\bigcap_{i\in S} A_i| = 2^{n-|\bigcup_{i\in S} c_i|}.$$

本式により, 以下 $|\bigcap_{i\in S} A_i|$ の代わりに $|\bigcup_{i\in S} c_i|$ の値を評価する.

次が主要結果である.

Theorem 5 $l \geq 2$ とする. 上記の条件を満たす二つの n 変数 k-CNF 式 $\phi = c_1c_2\cdots c_m$, $\psi = d_1d_2\cdots d_m$ に対して,

$$\max\Big\{\Big||\bigcap_{i=1}^{l} c_i| - |\bigcap_{i=1}^{l} d_i|\Big|\Big\} = \Big\lfloor \frac{k}{2^{l-2}} \Big\rfloor$$

が成り立つ.

略証: 本定理の証明は大きく二つのパートに分けられる. 一つは, k-CNF 式に関して, $|\bigcap_{i=1}^{l} c_i|$ の取りうる値の上下限を計算する手続きの構築, (それら上下限の値の差により, 定理中の左辺の値の上限が得られる), もう一つは, その上下限の差を実現する二つの k-CNF 式の具体的構成である.

「$|\bigcap_{i=1}^{l} c_i|$ の上下限の差」の上限

$|\bigcap_{i=1}^{l} c_i|$ の上下限の差を評価するため, 以下の手続きを用いる. なお, 本手続きは Melkman らのものと類似のものを使うが, k-CNF 式という制約により, $|\bigcap_{i\in S} c_i|$, $|\bigcup_{i\in S} c_i|$ の値の手続き中の変化に違いがあることに注意を要する.

Procedure $bounds(\{c_i\}_{i=1}^{l}; N)$:
  if $l = 2$, then return
    low_bd $= \max\{|c_1| + |c_2| - N, 0\}$;
    upp_bd $= \min\{|c_1|, |c_2|\}$;
  else if $|c_l| \leq N/2$, for $i \in \{1,\cdots,l-1\}$,
    $c_i = c_i \cap c_l$;
    return $bounds(\{c_i\}_{i=1}^{l-1}; |c_l|)$;
  else $(N/2 < |c_l| \leq N)$ for $i \in \{1,\cdots,l-1\}$,
    $c_i = c_i - c_l$;
    (low_bd, upp_bd) := $bounds(\{c_i\}_{i=1}^{l-1}; N - |c_l|)$;
    return $(|\bigcup_{i=1}^{l-1} c_i| - \text{upp\_bd}, |\bigcup_{i=1}^{l-1} c_i| - \text{low\_bd})$;

最初 $N = \min\{kl, n\}$ とし, Procedure により $bounds$ を再帰的に計算する. すると, 最終的に更新された c_1, c_2 に関して, $|c_1 \cap c_2|$ の上下限の差と所望の $|\bigcap_{i=1}^{l} c_i|$ の上下限の差は一致することが分かり, さらに, $|c_{1,l-2} \cap c_{2,l-2}|$ の上下限は次のように評価される.

$$\max\{|c_{1,l-2}|+|c_{2,l-2}|-\Big\lfloor \frac{k}{2^{l-3}} \Big\rfloor, 0\} \leq |c_{1,l-2}\cap c_{2,l-2}|$$

$$|c_{1,l-2} \cap c_{2,l-2}| \leq \min\{|c_{1,l-2}|, |c_{2,l-2}|\}$$

したがって, $l \geq 2$ のとき, $|\bigcap_{i=1}^{l} c_i|$ の上下限の差が, もう一つの項集合 $\{d_i\}$ を用いて次のように上から評価される.

$$\max\Big\{\Big||\bigcap_{i=1}^{l} c_i| - |\bigcap_{i=1}^{l} d_i|\Big|\Big\} \leq \Big\lfloor \frac{k}{2^{l-2}} \Big\rfloor.$$

「$|\bigcap_{i=1}^{l} c_i|$ の上下限の差」の下限

このときは, 上記で求めた上限 $\lfloor k/2^{l-2} \rfloor$ を実現する二つの k-CNF 式の存在を示せばよい.

$l = 2$ のとき, 次の二つの k-CNF 式

$$\Phi = \Big(\sum_{i=1}^{k} x_i\Big)\Big(\sum_{i=1}^{k} \overline{x}_i\Big),\ \Psi = \Big(\sum_{i=1}^{k} x_i\Big)\Big(\sum_{i=1}^{k} y_i\Big)$$

が条件を満たす二式の例である.

$l \geq 3$ のときは, 前述の Amano らの論文で作られた, 次の条件を満たす k-CNF 式の組 $\phi = c_1c_2\cdots c_l$, $\psi = d_1d_2\cdots d_l$ を利用する：

$$k = 2^{l-2},\ |\bigcap_{i=1}^{l} c_i| = 0,\ |\bigcap_{i=1}^{l} d_i| = 1,$$

$$\forall S \subset \{1,\cdots,l\} \text{ s.t. } |S| \leq l-1, |\bigcap_{i\in S} c_i| = |\bigcap_{i\in S} d_i|.$$

l を $3 \le l \le \lfloor \log k \rfloor + 2$ を満たす整数とする．$k' = 2^{l-2}$ に対して，k'-CNF 式として上記に述べた二式 ϕ と ψ をとる．ϕ と ψ の各変数（例えば x）に対して，$\lfloor k/2^{l-2} \rfloor = \lfloor k/k' \rfloor$ 個の新しい変数 $x_1, x_2, \cdots, x_{\lfloor k/k' \rfloor}$ を作り，C_i, D_i を，それぞれ c_i, d_i の各変数（例えば x）を論理和 $x_1 + x_2 + \cdots + x_{\lfloor k/k' \rfloor}$ に変えた項とする．二つの k-CNF 式 Φ と Ψ を次のように定める：$\Phi = C_1 C_2 \cdots C_l$, $\Psi = D_1 D_2 \cdots D_l$．このとき，$|C_i| = |D_i| = k' \times \lfloor k/k' \rfloor \le k$ より，Φ と Ψ は k-CNF 式であり，さらに，$\forall S \subset \{1, \cdots, l\}$ s.t. $|S| \le l-1$, $|\bigcap_{i \in S} C_i| = |\bigcap_{i \in S} D_i|$ であり，

$$\Big|\bigcap_{i=1}^{l} C_i\Big| = 0, \ \Big|\bigcap_{i=1}^{l} D_i\Big| = \Big\lfloor \frac{k}{k'} \Big\rfloor = \Big\lfloor \frac{k}{2^{l-2}} \Big\rfloor$$

が成り立つ．よって，Φ, Ψ が所望の二式である．

□

本定理より，$l \ge \lfloor \log k \rfloor + 2$ とすれば，$|\bigcup_{i=1}^{m} A_i|$ の値が一意に定まる．

本章の詳細は，論文 (A. Matsuura, Trans. on Inform. and Sys., Vol. E88-D, pp. 100-102, 2005) に譲る．

6 ハノイの塔問題から一般化された再帰式の厳密解析

6.1 ハノイの塔問題

ハノイの塔は 1883 年に E. Lucas によって作られた組合わせゲームである．オリジナルのゲームは三本の柱を持ち，一本の柱に初期的に置かれた n 枚の円盤を他の一本の柱に全て移し替えるために必要な最小移動回数と手続きを問う．但し，円盤をその円盤により小さな円盤の上に置くことは禁じられている．この三本ハノイの塔問題に対しては，最小移動回数である $2^n - 1$ を取る再帰アルゴリズムがよく知られる．

本ハノイの塔問題は，柱の数を三本から k 本 ($k \ge 3$) とし，ある柱に置かれた n 枚の円盤を k 本の柱を用いて目的の柱に最小移動回数で移動させる問題（k 本ハノイの塔問題）として自然に一般化できる．k 本ハノイの塔問題に対しては，未だ最適解は分かっておらず，次のアルゴリズム（Frame-Stewart のアルゴリズム）が現在までに最良のアルゴリズムである．

Frame-Stewart のアルゴリズムでは，各 t ($1 \le t \le n$) に対して次の試行を行う．

1. n 枚の円盤のうち，上位の $n-t$ 枚を中間の一つの柱に再帰的に移す．
2. 下位の t 枚の円盤を目的の柱に再帰的に移す．
3. 残った $n-t$ 枚の円盤を目的の柱に再帰的に移す．

アルゴリズムは，全ての t における試行のうち，これら 1, 2, 3 ステップに要する移動回数の総和が最小となるものを選び，実際に移動を行う．$k = 4$ のとき，$S(n)$ を n 枚の円盤に対する移動回数とすると，アルゴリズムは次の再帰式に従う．

$$S(n) = \min_{1 \le t \le n} \big\{ 2\,S(n-t) + (2^t - 1) \big\}.$$

$S(n)$ の階差は次のようになる．

$$S(n) - S(n-1) = 2^{i-1}.$$

ここで，t_i を i 次三角数，すなわち $t_i = i(i+1)/2$ としたとき，$t_{i-1} < n \le t_i$ である．$S(n)$ の値を closed formula の形で与えることも可能である．

このように特筆すべき規則性を持つ本再帰式の組合わせ構造をより深く解明するため，次のような $\{T(n, \alpha, \beta)\}$（α と β は任意の自然数）に関する再帰式を考える．$T(0, \alpha, \beta) = 0$, $n \ge 1$ に対し，

$$T(n, \alpha, \beta) = \min_{1 \le t \le n} \big\{ \alpha T(n-t, \alpha, \beta) + \beta S(t, 3) \big\}.$$

特に $S(n) = T(n, 2, 1)$ である．$T(n, \alpha, \beta)$ に関して，まず分かることは，β に関する線形性である．つまり，任意の自然数 α, β に対して，

$$T(n, \alpha, \beta) = \beta\, T(n, \alpha, 1)$$

が成り立つ．したがって，$T(n, \alpha, \beta)$ を求めるには，$T(n, \alpha, 1)$ を考えれば十分である．

6.2 主要結果

次の定理が，$T(n, \alpha, 1)$ を特定する主要結果である．

Theorem 6 α を自然数とし，$\{a_n\}_{n\geq 1}$ を $2^i\alpha^j$ $(i,j\geq 0)$ なる自然数が昇順に並んだ数列とする．すると，任意の自然数 n に対して，次式が成り立つ．

$$T(n,\alpha,1)-T(n-1,\alpha,1)=\begin{cases}1 & (\alpha=1)\\ a_n & (\alpha\geq 2)\end{cases}$$

$T(n,\alpha,\beta)$ の β に関する線形性と定理6より，次の系が成り立つ．

Corollary 3 $T(n,\alpha,\beta)$ は次式より求められる．

$$T(n,\alpha,\beta)=\begin{cases}\beta n & (\alpha=1,\ n\geq 0)\\ \beta\sum_{i=1}^{n}a_i & (\alpha\geq 2,\ n\geq 1)\end{cases}$$

定理の略証: $\alpha=1$ のとき，任意の n に対して，$\min_{1\leq t\leq n}\{\alpha T(n-t,\alpha,1)+S(t,3)\}$ は $t=1$ で最小値 $T(n,1,1)=T(n-1,1,1)+S(1,3)=T(n-1,1,1)+1$ をとる．よって，$T(n,1,1)-T(n-1,1,1)=1$ が成り立つ．

$\alpha\geq 2$ のとき，証明は次の二つの場合に分けられる: (Case 1) α が任意の $l\geq 1$ に対して 2^l の形をしていないとき; (Case 2) それ以外．

Case 1. n に関する帰納法による．

$n=0$ のとき，$T(0,\alpha,1)=0$ であり，$T(1,\alpha,1)=\alpha T(0,\alpha,1)+S(1,3)=0+(2^1-1)=1$ であるので，$T(1,\alpha,1)-T(0,\alpha,1)=1$．一方で，$a_1=2^0\alpha^0=1$．したがって，$T(1,\alpha,1)-T(0,\alpha,1)=a_1$ が成り立つ．

$n\geq 1$ のとき，各 $i\,(\geq 0)$ に対して，k_i を $a_{k_i}=2^i$ を満たす自然数とする．今，次の式が $n\leq k_i$ において成り立つとする．

$$T(n,\alpha,1)-T(n-1,\alpha,1)=a_n.$$

この式が $k_i+1\leq n\leq k_{i+1}$ なる n でも成り立つことが示されればよい．

今，$T_{n,t}:=\alpha T(n-t,\alpha,1)+S(t,3)$ と略記すると，$T(n,\alpha,1)=\min_{1\leq t\leq n}\{T_{n,t}\}$ である．

$T_{n,t}$ がどのような t で最小となるかを示すのが，次の補題である．

Lemma 7 帰納法の仮定の下，$k_i\leq n\leq k_{i+1}-1$ のとき，$T(n,\alpha,1)=\min_{1\leq t\leq n}\{T_{n,t}\}$ は $t=i+1$ において最小となる．

次の補題は，補題7，および定理6を証明するために繰り返し利用される．

Lemma 8 p と q を $q\geq p\geq 2$ を満たす任意の自然数とし，$\{a_n\}_{n\geq 1}$ を p^iq^j $(i,j\geq 0)$ が昇順に並んだ数列とする．このとき，以下が成り立つ．

1. 任意の自然数 l に対して $q\neq p^l$ が成り立つとき，$p^i<a_n<p^{i+1}$ を満たす n に対して，$a_n=qa_{n-(i+1)}$ が成り立つ．
2. $q=p^l$ がある自然数 l について成り立つとき，$a_n=p^i$ を満たす自然数 i と n に対して，$a_{n+1}=qa_{n-i}$ が成り立つ．

本補題は $(p,\,q)=(2,\,\alpha)$ として利用される．

Case 1は，さらに次の二つに場合に場合分けされる．(Case 1-1) $k_i+1\leq n\leq k_{i+1}-1$ のとき; (Case 1-2) $n=k_{i+1}$ のとき．

Case 1-1. 上記の二つの補題より，$T(n,\alpha,1)-T(n-1,\alpha,1)$ は $k_i+1\leq n\leq k_{i+1}-1$ のとき，次のように計算される．

$$\begin{aligned}
& T(n,\alpha,1)-T(n-1,\alpha,1)\\
=\ & T_{n,i+1}-T_{n-1,i+1}\\
=\ & \alpha\{T(n-(i+1),\alpha,1)-T(n-1-(i+1),\\
& \alpha,1)\}+S(i+1,3)-S(i+1,3)\\
=\ & \alpha a_{n-(i+1)}\ \text{(帰納法の仮定より)}\\
=\ & a_n.
\end{aligned}$$

よって Case 1-1 が示された．

Case 1-2. $n=k_{i+1}$ のとき，示すべき式は，$T(k_{i+1},\alpha,1)-T(k_{i+1}-1,\alpha,1)=a_{k_{i+1}}\ (=2^{i+1})$ である．補題より，$T(k_{i+1},\alpha,1)$ と $T(k_{i+1}-1,\alpha,1)$ はそれぞれ $t=i+2$, $t=i+1$ で最小値をとる．したがって，

$$\begin{aligned}
& T(k_{i+1},\alpha,1)-T(k_{i+1}-1,\alpha,1)\\
=\ & T_{k_{i+1},i+2}-T_{k_{i+1}-1,i+1}\\
=\ & \alpha\{T(k_{i+1}-(i+2),\alpha,1)-T(k_{i+1}-1-\\
& (i+1),\alpha,1)\}+S(i+2,3)-S(i+1,3)\\
=\ & (2^{i+2}-1)-(2^{i+1}-1)=2^{i+1}.
\end{aligned}$$

よって，Case 1-2 が示された．

Case 2. このとき, ある $l\,(\geq 1)$ が存在して, $\alpha = 2^l$ である．Case 1 と同様, n に関する帰納法による．$i \geq 0$ のとき, k_i を $a_n = 2^i$ となる最大の n とする．

$n = 0$ のとき, 証明は Case 1 と同様である．

$n \geq 1$ のとき, 次の等式が $n \leq k_i$ で成り立つとする．

$$T(n, \alpha, 1) - T(n-1, \alpha, 1) = a_n.$$

本式が $k_i + 1 \leq n \leq k_{i+1}$ でも成り立つ, すなわち, $a_n = 2^{i+1}$ なる全ての n について成り立つことが示されればよい．Case 1 と同様, $T_{n,t}$ が最小化される t を特定するのが以下の補題である．

Lemma 9 帰納法の仮定の下, 以下が成り立つ．

1. $n = k_i$ のとき, $T(n, \alpha, 1) = \min_{1 \leq t \leq n}\{T_{n,t}\}$ は $t = i + 1$ で最小となる．
2. $k_i + 1 \leq n \leq k_{i+1} - 1$ のとき, $T(n, \alpha, 1) = \min_{1 \leq t \leq n}\{T_{n,t}\}$ は $t = i + 1, i + 2$ で最小となる．

本補題より, $T_{n,t}$ は n の値によらず, $t = i + 2$ で最小値を取り, $T_{n-1,t}$ は $t = i + 1$ で最小値を取ることが分かる．よって, $k_i + 1 \leq n \leq k_{i+1}$ のとき,

$$\begin{aligned} & T(n, \alpha, 1) - T(n-1, \alpha, 1) \\ = \; & T_{n,i+2} - T_{n-1,i+1} \\ = \; & \alpha\{T(n-(i+2), \alpha, 1) - T(n-1-(i+1), \\ & \alpha, 1)\} + (2^{i+2} - 1) - (2^{i+1} - 1) \\ = \; & 2^{i+1}. \end{aligned}$$

したがって, Case 2 が示された．

以上より, 定理 6 が証明された． □

本章の詳細は, 論文 (A. Matsuura, Proc. of ALENEX/ANALCO08, pp. 228-233, 2008) に譲る．

7 正六角盤面上の一般化三並べの先手必勝法

7.1 一般化三並べと従来結果

一般化三並べとは, 指定されたサイズの盤面上に 2 人で交互に石を置き, 指定された図形 (生物) の完成を競う二人完全情報ゲームである．本問題は, F. Harary によって提起された．その単純な問題設定にも関わらず, 現在までに一般的な多項式時間の探索法は知られておらず, ゲームの組合せ構造や必勝法に関する研究が行われている．本ゲームでは, 両者が最適な手を打つ限り, 先手が勝つか引き分けとなり, 先手が勝つ図形は**勝ち型**, 引き分けとなる図形は**負け型**と呼ばれる．

従来の結果として, 正方盤面に関して, Snaky と呼ばれるサイズ 6 の生物（6 細胞生物）が勝ち型か負け型か分かっていない他は, 全ての生物について勝ち型か負け型かが特定されている．正六角盤面に関して, Bode と Harborth により, 4 細胞生物までの勝ち型, 負け型が全て特定され, 22 種類ある 5 細胞生物のうち, 15 種類が勝ち型, 2 種類が負け型であることが明らかにされた (Discr. Math., Vol. 212, pp. 5-18, 2000)．しかし, 図 1 に示された 5 種類の 5 細胞生物が勝ち型か否かについては未解決であった．

本研究では, これら 5 種類の生物のうち, **Y, Z, C** と呼ぶ 3 種類の生物が勝ち型であることを示す．証明は, 各々に対して先手の必勝法を示すことにより行われる．

ここでは, **Y** について必勝法を具体的に示す．

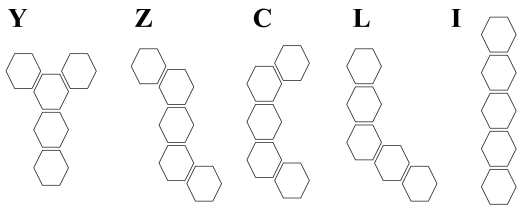

図 1: 未解決の 5 細胞生物 **Y, Z, C, L, I**

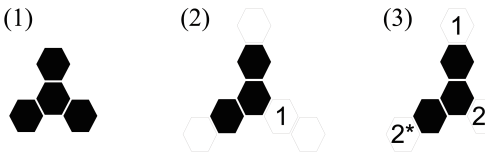

図 2: (1) propeller; (2)(3) **Y** に対する基本手順

7.2　Y に対する先手必勝法

基本手順

以下, 先手を A と記し, 後手を B と記す. 図 2(1) の 4 細胞生物を *propeller* と呼ぶ. もし propeller が A によって完成され, propeller の三つの末端のセルのうち二つが空いた状態で B に順番が来ると, A は **Y** を完成することができる. この観察に基づき, 次のような二つの基本手順を作成する.

まず, 図 2(2) において, 三つの黒いセルは A によってマークされ, その他のセルが空いており, B に順番が回ってきたとする. すると, B は 1 の書かれたセルにマークする他無い. 何故なら, そうしなければ, A がそのセルをマークし, 二つの末端のセルが空いた状態の propeller を作ることができるからである（その場合 A が勝利することは, 上に記述した）.

もう一つの基本手順が図 2(3) に示されている. 三つの黒いセルは A によってマークされ, 1 と書かれたセルは B によってマークされ, 今 B のマークする順番である. このとき, B は 2* の入っているセルのうちのいずれかに打たねばならない. 何故なら, A がこの場合も二つの末端のセルが空いた propeller を作るからである.

この二つの B の手を誘導する基本手順を用いて **Y** の先手必勝法を構築する.

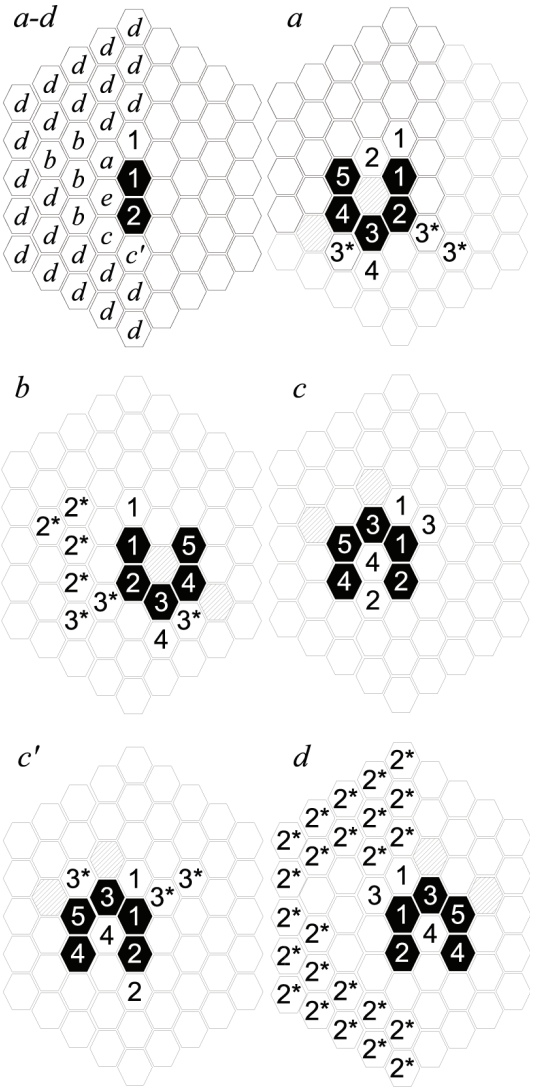

図 3: B の 2 手目の分類と a から d に対する先手必勝手順

必勝法の構築

我々は図 3 のように $5 \times 5 \times 5$ 正六角盤面を用いる. 先手 A は最初中央のセルをマークする. 以下, A のセルは常に黒くマークする. 以下, B の 1 手目が中央セルに隣接する場合 (Case 1) と隣接しない場合 (Case 2) に分けて考える.

Case 1. 盤面の対称性より, B の 1 手目は中央セルの上部のセルとしてよい. A の 2 手目は中央セルの下部のセルとする. B の 2 手目は図 3 の a から e の 5 通りに場合分けされる. 盤面の対称性より, B の 2 手目は晩面の左半面で考えてよい.

B が 2 手目で a をマークしたとき, A の 3 手目に対して B は, 図 2(3) の基本手順より, 3*の書かれてあるセルのいずれかをマークせねばならない. A の 4 手目に対して, B は図 2(2) の基本手順より, 4 とマークされたセルに打たねばならない. このとき A の 5 手目により, A は二つの網かけのセルのうちいずれかを打てば propeller を作ることができる. したがて, A は 7 手で勝利する.

B の 2 手目が b, c, c', d の各々であったときの必勝法は図 3 に個別に書かれている. いずれの場合も, A は 7 手で勝利する.

B が 2 手目で e にマークするとき, A の 3 手目に対して, B は図 4 の $3i$ か $3j$ の書かれているいずれかのセルに打たねばならない. もし B が $3i$ に打つとき, A は円環状に手を打ち, B の 4 手目, 5 手目を一意に定める. A の 6 手目により, さらに網かけセルのうち一つをマークすることにより, A は末端のセルが二つ空いた propeller を完成させることができる. よって, この場合 A は 8 手で

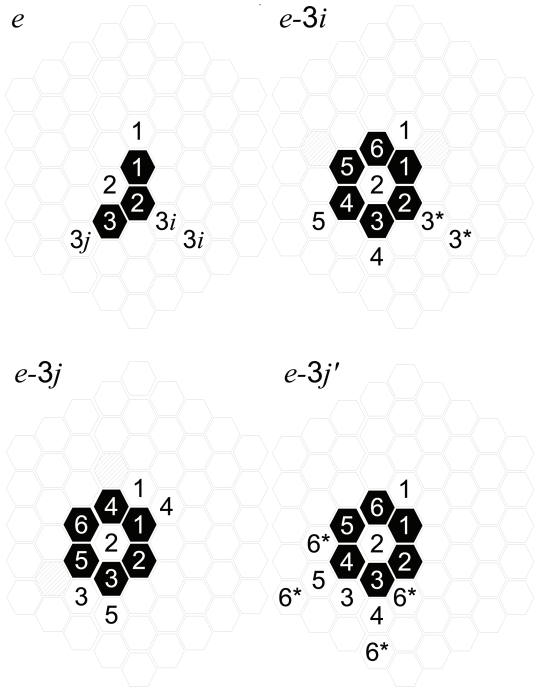

図 4: e に対する先手必勝手順

勝利する．B の 3 手目が $3j$ であった場合, B の 4 手目, 5 手目は A に誘導されて一意に定まり, この場合も A は 8 手で勝利する．なお, B が $3j$ を打つ場合, $3i$ と同じ手順は図 4 の e-$3j'$ に示された B の反撃があるため, 有効でない.

以上より, Case 1 は A が高々8 手で勝利することが示された.

Case 2. 盤面の対称性より, B の 2 手目は図 5 の $1*$ の書かれた 7 通りと考えてよい．A の 2 手目に対して, B の 2 手目は v から z の 5 通りに分類される．B が 2 手目も $1*$ のうちのいずれかに打った場合は, v の必勝法が用いられる.

B の 2 手目が v のとき, v か $1*$ を持つセルは, 先ほどの Case 1 の a の手と exclusive である．よって a の手順が適用でき, A は 7 手で勝利する．w に対しては, v と垂直軸に対する線対称な手順が用いられる．x, y, z のときの手順は図 5 に書かれた通りである．よって, Case 2 も A は高々8 手で勝利する.

以上より, **Y** に対して, 先手 A が高々8 手で勝利することが示された. □

生物 **Z**, **C** に対しても, 同様に先手必勝手順を構築することでき, **Z** は 7 手で先手必勝, **C** は 9 手で先手必勝であることが示される.

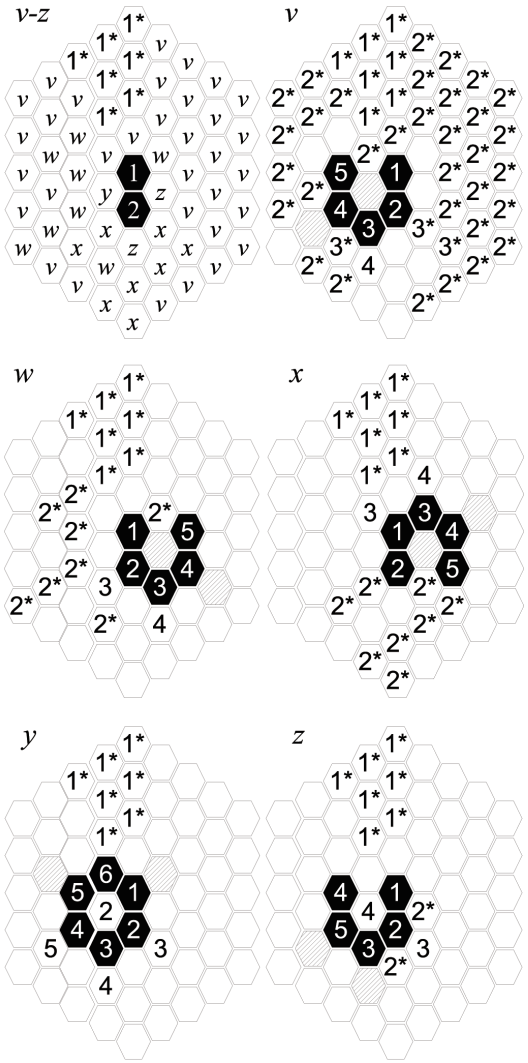

図 5: Case 2（v から z）に対する先手必勝手順

証明の詳細は, 論文 (K. Inagaki, A. Matsuura, Proc. of MATH2007, pp. 252-259, 2007) に譲る.

8 有限オートマトンの等価変換と状態数解析

有限オートマトンは, コンパイラにおける言語解析や正規表現, ソフトウェアの設計や検証といった応用において極めて重要な役割を果たし, 現在でも, 計算機モデルとしての研究が活発に行われている．代表的な有限オートマトンとしては, 入力記号に応じて遷移状態が一意に決定される決定性オートマトン (DFA) や複数の遷移状態を持つ非決定性オートマトン (NFA) が知られる．n 状態

の NFA を等価かつ極小な DFA に変換すると, 状態数は 2^n まで増大する．そのとき状態数は一種の計算能力の指標となるが, 任意の値 2^n に対し, その状態数を持つ決定性有限オートマトンと等価な n 状態非決定性有限オートマトンの組が存在するか否かは分かっていない.

これまでに, 入力記号が状態数に比例する程度である場合には, $0 \leq \alpha \leq 2^n - n$ を満たす任意の整数 α に対して, n 状態 NFA で, それと等価な DFA が $2^n - \alpha$ 状態有するものが存在することが示されている (G. Jirásková, Rairo Theoret. Inform. and Appl. Vol. 40, pp. 485-499, 2006). また最近, 入力アルファベットのサイズが 4 以上ならば, 任意の α に対して, そのような n 状態 NFA が構成できることが示された (J. Jirásek et al., Proc. of DLT, pp. 254-265, 2007). 入力記号が一種類, すなわち unary の場合は, 無数の α に対し, そのような NFA は存在しないことが示されている (V. Geffert, Proc. of MFCS, pp. 412-423, 2006). 未解決の場合は, 入力アルファベットのサイズが 2, 3 の場合であり, アルファベットが二値 $\{0,1\}$ を取る場合, $0 \leq \alpha \leq 2n-2$ の範囲にある α に対してそのような NFA の存在は知られている (Iwama et al., Theret. Comput. Sci. Vol. 301, pp. 451-462, 2003).

本研究においては, 入力アルファベットのサイズが 2 である場合に, これまでの結果を改良し, 以下の定理を示した.

Theorem 7 $\lfloor(\alpha-1)/3\rfloor$ が奇数で, かつ n と互いに素である, という条件を満たす $28 \leq \alpha \leq 3n-3$ の範囲の α に対して, 等価な最小 DFA の状態数が $2^n - \alpha$ であるような n 状態 NFA が存在する.

Theorem 8 $\lfloor(\alpha-1)/4\rfloor$ が n と互いに素で, α が 4 の倍数でない, という条件を満たすという条件を満たす $37 \leq \alpha \leq 4n-5$ の範囲の α について, 等価な最小 DFA の状態数が $2^n - \alpha$ であるような n 状態 NFA が存在する.

以下, 定理 7 について, 証明の概略を示す.

略証: 証明は NFA の具体的構成による．今, k と m を互いに素な自然数とし, $k \geq 9$, $m \geq 2$, かつ k は奇数であるとする．$\alpha = 3k+1$ を満たす NFAM_1 を以下の五つ組で定義する.

$$
\begin{aligned}
M_1 &= (Q, \Sigma, Q_0, \delta, F) \\
Q &= \{t_0, \cdots, t_{k-1}\} \cup \{s_0, \cdots, s_{m-1}\} \\
&= T \cup S \\
Q_0 &= F = \{t_0\}
\end{aligned}
$$

$$
\delta(t_i, \sigma) = \begin{cases} t_{i+1} & (\sigma = 0) \\ t_i & (i \neq 3,\ \sigma = 1) \\ s_0 & (i = 3,\ \sigma = 1) \\ t_0 & (4 \leq i \leq k-4,\ \sigma = 1) \\ t_2 & (i = 4,\ \sigma = 1) \end{cases}
$$

$$
\delta(s_j, \sigma) = \begin{cases} s_{j+1} & (\sigma = 0) \\ s_1 & (j = 0,\ \sigma = 1) \\ t_0, t_3 & (j = 1,\ \sigma = 1) \\ s_j & (2 \leq j \leq m-1,\ \sigma = 1) \end{cases}
$$

M_1 を有限オートマトンを等価変換するための手法 “subset construction” により変換して得られる DFA の各状態 P に対して, T の状態からなる部分を P_T, S の状態からなる部分を P_S と書くことにする．NFAM_1 と等価な最小 DFA が所望の状態数を持つことを示すために, 以下の補題群を利用する.

Lemma 10 $|P_S| = 0$, かつ $0 \leq |P_T| \leq 3$ を満たす状態 P について,

1. $|P_T| = 0$ のとき, すなわち空集合は到達不可能である.
2. $|P_T| = 1$ となる状態 P は全て到達可能である.
3. $|P_T| = 2$ となる状態 P は, $[t_i, t_{i+1}]$, $[t_i, t_{i+2}]$ と表せる $2k$ 個の状態のみ到達不可能で, 残りは全て到達可能である.
4. $|P_T| = 3$ となる状態 P は $[t_i, t_{i+1}, t_{i+2}]$ と表せる k 個の状態が到達不可能で, 残りは全て到達可能である.

Lemma 11 $|P_S| = 0$ かつ $|P_T| \geq 4$ のとき, 以下が成り立つ.

1. $\{t_i, t_{i+3}\} \subset P$ を満たす状態 P は, $|Q_S| = 1$, $|Q_T| = |P_T| - 2$ を満たす状態 Q から到達可能である.

2. $\{t_i, t_{i+3}\} \subset P$ を満たさない状態 P は, $|Q_S| = 0$, $|Q_T| = |P_T| - 1$ を満たす状態 Q から到達可能である.

Lemma 12 $|P_S| \geq 1$ のとき, 以下が成り立つ.

1. $\{t_i, t_{i+3}\} \subset P$ を満たす状態 P は, $|Q_S| = |P_S|$, $|Q_T| = |P_T| - 1$ を満たす状態 Q から到達可能である.

2. $\{t_i, t_{i+3}\} \subset P$ を満たさない状態 P は, $|Q_S| = |P_S| - 1$, $|Q_T| = |P_T| + 1$ を満たす状態 Q から到達可能である.

補題 10 により, $3k + 1$ 個到達不可能な状態が存在することが示され, 補題 11, 12 により, その他の状態が全て到達可能であることが帰納的に示される. また, 次の補題より, この DFA が最小であることが示される.

Lemma 13 到達可能な状態は全て互いに同値でない.

上記補題証明の詳細は, 2008 年 3 月発表予定の情報処理学会アルゴリズム研究会研究報告に譲る.

上記の NFAM_1 にさらに新たな遷移を付加することにより, 到達不可能な状態の数が $3k+2$, $3k+3$ である NFAM_2, M_3 も構築可能である. よって, $\alpha = 3k + 1, 3k + 2, 3k + 3$, $k \geq 9$ とすることで, $28 \leq \alpha \leq 3n - 3$ の範囲の任意の α に対して, 等価な最小 DFA が $2^n - \alpha$ 状態を持つ NFA が存在することが示された. □

定理 8 も, 条件を満たす NFA を具体的に構成し, 到達可能な状態数を数え上げることで証明される. 詳細は, 上記研究報告を参照されたい.

研究業績一覧

学術論文

1. Zhi-Zhong Chen, Tatsuie Tsukiji:
"Computing Bounded-Degree Phylogenetic Roots of Disconnected Graphs", Journal of Algrithms, 59(2), pp. 125-148, 2006.
概要: The Phylogenetic kth Root Problem (PR_k) is the problem of finding a (phylogenetic) tree T from a given graph $G = (V, E)$ such that (1) T has no degree-2 internal nodes, (2) the external nodes (i.e. leaves) of T are exactly the elements of V , and (3) $(u, v) \in E$ if and only if the distance between u and v in tree T is at most k, where k is some fixed threshold k. Such a tree T, if exists, is called a phylogenetic kth root of graph G. The computational complexity of PR_k is open, except for $k \leq 4$. Recently, Chen et al. investigated PR_k under a natural restriction that the maximum degree of the phylogenetic root is bounded from above by a constant. They presented a linear-time algorithm that determines if a given connected G has such a phylogenetic kth root, and if so, demonstrates one. In this paper, we supplement their work by presenting a linear-time algorithm for disconnected graphs.

2. Tatsuie Tsukiji, Zhi-Zhong Chen:
"Computing Phylogenetic Roots with Bounded Degrees and Errors Is Hard", Theoretical Computer Science, 363(1), pp. 43-59, 2006.
概要: The Degree-Δ Closest Phylogenetic kth Root Problem ($\Delta\mathrm{CPR}_k$) is the problem of finding a (phylogenetic) tree T from a given graph $G = (V, E)$ such that (1) the degree of each internal node of T is at least 3 and at most Δ, (2) the external nodes (*i.e.* leaves) of T are exactly the elements of V, and (3) the number of disagreements, $|E \oplus \{\{u, v\} : u, v$ are leaves of T and $d_T(u, v) \leq k\}|$ does not exceed a given number, where $d_T(u, v)$ denotes the distance between u and v in tree T. We show that this problem is NP-hard for all fixed constants $\Delta, k \geq 3$. Our major technical contribution is the determination of all phylogenetic roots that approximate the almost largest cliques. Specifically, let $s_\Delta(k)$ be the size of the largest clique having a kth phylogenetic root with maximum degree Δ. We determine all the phylogenic

kth roots with maximum degree Δ that approximate the $(s_\Delta(k)-1)$-clique within error 2, where we allow the internal nodes of phylogeny to have degree 2.

3. Zhi-Zhong Chen, Michelangelo Grigni, Christos H. Papadimitriou:
"Recognizing Hole-Free 4-Map Graphs in Cubic Time", Algorithmica, 45(2), pp. 227-262, 2006.
概要: We present a cubic-time algorithm for the following problem: Given a simple graph, decide whether it is realized by adjacencies of countries in a map without holes, in which at most four countries meet at any point. Key words. planar graphs, maps, map graphs, cliques, graph algorithms.

4. Zhi-Zhong Chen:
"New Bounds on the Number of Edges in a k-Map Graph", Journal of Graph Theory, (掲載予定).
概要: It is known that for every integer $k \geq 4$, each k-map graph with n vertices has at most $kn-2k$ edges. Previously, it was open whether this bound is tight or not. We show that this bound is tight for $k=4$. We also laboriously show that this bound is not tight for large enough k; more precisely, we show that for every $0<\epsilon<\frac{3}{328}$ and for every integer $k \geq \frac{140}{41\epsilon}$, each k-map graph with n vertices has at most $(\frac{325}{328}+\epsilon)kn-2k$ edges. This result implies the first polynomial (indeed linear) time algorithm for coloring a given k-map graph with less than $2k$ colors for large enough k. We further show that for every positive multiple k of 6, there are infinitely many integers n such that some k-map graph with n vertices has at least $(\frac{11}{12}k+\frac{1}{3})n$ edges.

5. Zhi-Zhong Chen:
"Approximation Algorithms for Bounded Degree Phylogenetic Roots", Algorithmica, (掲載予定).
概要: The Degree-Δ Closest Phylogenetic kth Root Problem (ΔCPR$_k$) is the problem of finding a (phylogenetic) tree T from a given graph $G=(V,E)$ such that (1) the degree of each internal node in T is at least 3 and at most Δ, (2) the external nodes (i.e. leaves) of T are exactly the elements of V , and (3) the number of disagreements, i.e., $|E \oplus \{\{u,v\} : u,v$ are leaves of T and $d_T(u,v) \leq k\}|$, is minimized, where $d_T(u,v)$ denotes the distance between u and v in tree T. This problem arises from theoretical studies in evolutionary biology and generalizes several important combinatorial optimization problems such as the maximum matching problem. Unfortunately, it is known to be NP-hard for all fixed constants Δ, k such that either both $\Delta \geq 3$ and $k \geq 3$, or $\Delta > 3$ and $k=2$. This paper presents a polynomial-time 8-approximation algorithm for ΔCPR$_2$ for any fixed $\Delta > 3$, a quadratic-time 12-approximation algorithm for 3CPR$_3$, and a polynomial-time approximation scheme for the maximization version of ΔCPR$_k$ for any fixed Δ and k.

6. Zhi-Zhong Chen, Takayuki Nagoya:
"Improved Approximation Algorithms for Metric Max TSP", Journal of Combinatorial Optimization, 13(4), pp. 321–336, (2007).
概要: We present two polynomial-time approximation algorithms for the metric case of the maximum traveling salesman problem. One of them is for directed graphs and its approximation ration is $\frac{27}{25}$. The other is for undirected graphs and its approximatin ratio is $\frac{7}{8}-o(1)$. Both algorithms improve on the previous bests.

7. Akihiro Matsuura:
"A Note on Approximating Inclusion-Exclusion for k-CNF Formulas", IEICE Trans. on Information and Systems, Vol. E88-D, pp. 100–102, Jan., 2005.

概要: The number of satisfying assignments of k-CNF formulas is computed using the inclusion-exclusion formula for sets of clauses. Recently, it was shown that the information on the sets of clauses of size $\leq \lfloor \log k \rfloor + 2$ already uniquely determines the number of satisfying assignments of k-CNF formulas (Amano et al., Information Processing Letters, Vol. 87, pp. 111-117, 2003). The proof was, however, only existential and no explicit procedure was presented. In this paper, we show that such a procedure exists.

8. Akihiro Matsuura:
"Analysis of the Recurrence Relation Generalized from the 4-Peg Tower of Hanoi", Proc. of the 7th International Conference on Optimization: Techniques and Applications (ICOTA7), pp. 155–156, Dec., 2007.
概要: This paper presents a brief note on the analysis of the recurrence relation generalized from the recursive algorithm for the 4-peg Tower of Hanoi problem. We obtain the solution for this recurrence relation.

9. Kazumine Inagaki, Akihiro Matsuura:
"Winning Strategies for Hexagonal Polyomino Achievement", Proc. of the 12th WSEAS International Conference on Applied Mathematics (MATH2007), pp. 252–259, Dec., 2007.
概要: In polyomino achievement games, two players alternately mark the cells of a tessellation and try to achieve a given polyomino. Bode and Harborth (Discr. Math. 212, 2000) investigated polyomino achievement games for the hexagonal tessellation and determined all but five polyominoes with at most five cells whether they are achieved by the first player. In this paper, we show winning strategies for the three hexagonal polyominoes with five cells called **Y**, **Z**, and **C**, which were left open in the article by Bode and Harborth.

10. Akihiro Matsuura:
"Exact Analysis of the Recurrence Relations Generalized from the Tower of Hanoi", Proc. of the 5th SIAM Workshop on Analytic Algorithmics and Combinatorics (ALENEX/ANALCO08), pp. 228–233, Jan., 2008.
概要: In this paper, we analyze the recurrence relations generalized from the Tower of Hanoi problem of the form $T(n, \alpha, \beta) = \min_{1 \leq t \leq n} \{\alpha T(n-t, \alpha, \beta) + \beta(2^t - 1)\}$. It is shown that when α and β are natural numbers and $\alpha \geq 2$, the sequence of differences of $T(n, \alpha, \beta)$'s, i.e., $T(n, \alpha, \beta) - T(n-1, \alpha, \beta)$, consists of numbers of the form $\beta 2^i \alpha^j$ $(i, j \geq 0)$ lined in the increasing order.

研究会等

1. 築地立家, 松浦昭洋:
"最大次数 Δ の C_4 フリーグラフの $(2\Delta - 4)$ 彩色数を数え上げるためのマルコフ連鎖モンテカルロ法", 情報処理学会研究報告, Vol. 2004, No. 76, 2004-AL-096, pp. 35–42, 2004.
概要: 本稿では, C_4 フリーグラフの k-彩色数を数え上げるための高速なマルコフ連鎖モンテカルロ法 (MCMC) を提案する. グラフの最大次数を Δ とすると, $\Delta \geq 6$ のときは $k \geq 2\Delta - 4$ に対して, また $\Delta = 3, 4, 5$ のときはそれぞれ $k \geq 5, 6, 7$ に対して, k-彩色数の数え上げが多項式時間で可能である. 実行時間は $o(\Delta^2 n \log n)$ である. 本結果は, 特に $\max(2\Delta - 4, \Delta + 2) \leq k < 11/6\Delta$, $3 \leq \Delta \leq 23$ のときに, C_4 フリーグラフに対する初めての多項式時間 k-彩色数数え上げアルゴリズムである.

2. 松浦昭洋:
"ハノイの塔問題に対する再帰方程式の一般化とその厳密解析", 情報処理学会研究報告, Vol. 2007, No. 119, pp. 49-56, 2007 年 11 月.
概要: 本稿では, ハノイの塔問題より

一般化された再帰方程式 $T(n,\alpha,\beta) = \min_{1\le t\le n}\{\alpha T(n-t,\alpha,\alpha) + \beta S(t,3)\}$ ($S(t,3) = 2^t - 1$ は 3 本の塔を持つハノイの塔問題に対する最小解）に対する厳密な解析を行い，その一般解を導出する．すなわち，α と β が $\alpha \ge 2$ なる任意の自然数であるとき，$\{T(n,\alpha,\beta)\}$ の階差数列が $\beta 2^i \alpha^j$ $(i,j>0)$ なる自然数が昇順に並んだものであることを示す．

3. Kazumine Inagaki, Akihiro Matsuura:
"Winning Strategies for Hexagonal Polyomino Achievement", 電子情報通信学会技術研究報告, Vol. 107, No. 390, COMP2007-49, pp. 9–15, 2007 年 12 月.
概要: ポリオミノアチーブメントゲームにおいては，二人のプレーヤーが盤面上で交互に手を打ち，先手は与えられたポリオミノを早く完成させれば，後手はそれを防げば勝者となる．Bode と Harborth は正六角盤面上のポリオミノアチーブメントゲームを考察し，セル数 5 以下のポリオミノについて，5 つを除き，先手必勝か否かを特定した (Discr. Math. 212, 2000)．本稿では，その中で未解決であった 3 つのポリオミノ **Y**，**Z**，**C** が先手必勝であることを示す．

4. 松浦昭洋, 齋藤祐輔:
"二値アルファベット上の有限オートマトンの等価変換と状態数解析", 情報処理学会研究報告, （2008 年 3 月発表予定）.
概要: 本稿では, 決定性有限オートマトンと非決定性有限オートマトンの等価変換に関して, 入力アルファベットが二値を取る場合, 自然数 n と α が, $n \ge 11$, $28 \le \alpha \le 3n-3$, $\lfloor(\alpha-1)/3\rfloor$ が奇数, かつある素条件 (coprimality condition) を満たすならば, n 状態最小非決定性有限オートマトンで，その等価な最小決定性有限オートマトンが $2^n - \alpha$ 状態を持つものが存在することを示す．さらに, α が 4 の倍数でなければ, $n \ge 11$, $37 \le \alpha \le 4n-5$ において, 同様の n 状態非決定性有限オートマトンが存在することを示す．

学会大会等

1. Akihiro Matsuura, Hiroaki Tohyama:
"Computing the Vertex-Cover Polynomial of a Graph with Some Limitation on Edges", SIAM Conference on Discrete Mathematics (DM'04), Jun. 2004.

2. Akihiro Matsuura:
"Analysis of Recurrence Relations Generalized from the Tower of Hanoi", 夏の LA シンポジウム, 2007 年 7 月.

3. 松浦昭洋:
"離散数学のすすめ／ハノイの塔", 理系への数学, 第 41 巻, 第 3 号, pp. 58–64, 2008 年 3 月.

文部科学省科学研究費補助金 特定領域研究 (課題番号 16092215)

B05: ブール理論に基づく離散システムの構造解析と計算限界の研究

本研究班では，ブール理論に基づく離散システムが有する構造的な性質を明らかにすることで，その離散システムを用いて記述される離散問題を効率的に解くアルゴリズムの開発，および，アルゴリズム設計するための統一的な指針を与えることを目指した．また，解析した離散構造を利用することで，離散問題のもつ計算量下界，近似比下界などの計算限界を明らかにすることを目指し，研究を遂行した．具体的には，動的フローに基づく施設配置問題，ソース配置問題，最小枝ランキング全域木問題などのネットワークデザイン問題，列挙問題として代表的な極大クリーク列挙，劣モジュラ性の一般化である複基多面体の構造解析，無向グラフの連結度の一般化である正モジュラシステムの最小横断問題，ロボットのスケジューリング問題などの研究を行い，アルゴリズム開発や計算限界の提示に成功した．本稿では，それらの成果の中で，動的フローに基づく施設配置問題，ソース配置問題，極大クリーク列挙，正モジュラシステムの最小横断問題に重点に置き，報告する．

研究組織

研究代表者： 牧野 和久　東京大学 大学院 情報理工学系研究科

交付決定額 (配分額)

平成 16 年度	2,600,000 円
平成 17 年度	4,200,000 円
平成 18 年度	3,800,000 円
平成 19 年度	3,200,000 円
合　計	13,800,000 円

研究成果の概要

- 学術誌
  Discrete Mathematics (2004 年), Journal of the Operations Research Society of Japan 48 (2005 年)，Discrete Applied Mathematics (2006 年) など.
- 国際会議
  SWAT (Humlebaek (Denmark), 2004)，ISAAC (Sanya (China) 2005)，LATIN (Valdivia (Chile)，2006)，ESA (Zurich (Switzerland)，2006)，FAW (Lanzhou (China)，2007)，SAT (Lisbon (Portugal)，2007) など.
- 受賞
  日本 IBM 科学賞 (2004)，Discrete Applied Mathematics 誌 Editors' Choice (2004)，情報処理学会 山下記念研究賞 (2005)，情報処理学会 研究開発奨励賞 (2006)，国立大学法人大阪大学 教育・研究功績賞 (2006).

1　はじめに

社会システムや産業活動などに関連して現れる生産計画，環境計画，スケジューリング，最適投資などを始めとする重要な問題の多くは，離散構造を有するシステムの問題として捉えることができる．この離散構造を有するシステムの問題が答易に解けるか否かは, その対象となるシステムの構造に強く依存する. 比較的容易に解ける最適化問題の組合せ的, 代数的, あるいは, ブール関数的構造については, 例えばマトロイド構造や劣モジュラ構造というような離散的な構造が深く関係することが知られているが, それだけでは説明のつかない問題も数多い. また，最適化問題以外の問題，例えば，列挙問題などが，効率的に解けるために離散構造を解析することは極めて重要である．本研究班では，比較的容易に解ける問題の構造的性質をさらに詳細に吟味し, その構造を明らかにし, 効率的なアルゴリズムを設計するための統一的な指針を与えること，および，計算量理論を用いて計算量下界の提示などの計算限界を明らかにすることを試みた.

本研究班では，以上のような目的意識を持って, 主に理論的な研究に重点をおいて活動を続けて来た．具体的な成果としては,

1. 無向グラフの極大クリーク列挙問題に対する結果 [22].
2. ソース配置問題に対する結果 [28, 29, 30].
3. 複基多面体に関する結果 [11].
4. 無向木の分割問題に対する結果 [25].
5. 動的な木構造ネットワークにおけるフロー問題に関する成果 [26].
6. 正モジュラシステムの最小横断に関する成果 [31].
7. 最小枝ランキング全域木に関する成果 [23].
8. 2 次元平面上を動くロボットのスケジューリング問題に関する成果 [4].
9. 単調論理関数の有理彩色に関する成果 [13].
10. ホーン論理関数の連結性に関する成果 [21].

などがある．本報告では，特に，1，2，5，6 について報告する．

2　無向グラフの極大クリーク列挙

無向グラフ $G = (V, E)$ に対して，$W \subseteq V$ 中の任意の 2 点 $v, w \in W$ が枝 $(v, w) \in E$ をもつとき，W はクリークと呼ばれる．さらに，任意の $W' \supsetneq W$ がクリークでないとき，極大クリークと呼ばれる．良く知られているように，最大クリーク（要素数が最大であるクリーク）を求める問題は，NP 困難であり [12]，極大クリークを 1 つ求めることは，多項式時間で可能である．極大クリークを全て求めるという，極大クリーク列挙問題は, 古くから盛んに行われている [7, 17, 19, 34]．また，この極大クリーク列挙問題は，データマイニング分野の閉集合列挙問題などと関連し，様々な応用をもっている (例えば，[18, 1, 2]).

1977 年に築山ら [34] は，最初の出力多項式（全多項式）時間である，$\mathrm{O}(nm)$ 時間遅延アルゴリズムを開発した．ただし，$n = |V|$，$m = |E|$ とする．また，アルゴリズムの計算時間が入出力長の多項式時間で押さえられるとき，そのアルゴリズムを出力多項式時間とよび，i 番目の出力してから $i + 1$ 番目を出力するまでに必要な時間が入力長の多項式で押さえられているものを多項式時間遅延とよぶ．Lawler ら [19] はこの結果を一般のハイパーグラフの問題に拡張した (Eiter ら [9] はさらに一般化した）．千葉と西関 [7] は，$\mathrm{O}(a(G)m)$ 時間遅延アルゴリズムを開発し，高速化に成功している．ただし，$a(G)$ は，グラフ G のアーボレシティ（arboricity）であり，一般に，$m/(n-1) \leq a(G) \leq m^{1/2}$ が成立する．Johnson ら [17] は，すべての極大クリークを辞書式順に $\mathrm{O}(nm)$ 時間遅延で列挙するアルゴリズムを開発している．ただし，彼らのアルゴリズムは $\mathrm{O}(nN)$ 領域必要とする．ここで N は，極大クリーク数である．

本研究では，高速な行列積計算を用いることにより，$\mathrm{O}(M(n))$ 時間遅延でかつ，$\mathrm{O}(n^2)$ 領域必要とする極大クリーク列挙アルゴリズムを開発した．ただし，$M(n)$ とは，2 つの $n \times n$ 行列の積を計算するために必要な時間であり，現在のところ $\mathrm{O}(n^{2.376})$ 時間で可能なことが知られている [8],

したがって，提案するアルゴリズムは密な，例えば，$m = \Omega(n^{1.689})$ であるグラフに対しては，最速である．

以下では，このアルゴリズムの概略を紹介する．

2.1 $O(M(n))$ 時間遅延アルゴリズム

提案するアルゴリズムは，築山ら [34] と Johnson ら [17] が用いた逆探索（reverse search）に基づくものである．ここで，逆探索は，列挙問題を高速に解くために，Avis と福田 [5] によって提案された手法である．

$G = (V, E)$ を点集合 $V = \{v_1, \ldots, v_n\}$，枝集合 $E = \{e_1, \ldots, e_m\}$ である無向グラフとする． 点 $v \in V$ と点集合 $S \subseteq V$ の近傍を以下に与える．

$$\Gamma(v) = \{u \in V \mid (u, v) \in E\}$$
$$\Gamma(S) = \{u \in V \setminus S \mid (u, v) \in E \text{ for some } v \in S\}.$$

点集合 S と $i \in \{1, 2, \ldots, n\}$ に対して，

$$S_{\leq i} = S \cap \{v_1, \ldots, v_i\}.$$

2 つの点集合 X と Y に対して，$(X \setminus Y) \cup (Y \setminus X)$ 中の最小添字をもつ点が X に含まれるとき， X は，Y よりも辞書式に大きいと呼ぶ．また，クリーク K に対して，$C(K)$ を K を含む辞書式に最大の極大クリークと定義する．

逆探索は，直感的には，列挙しようする対象に親子関係を定義し，その関係をなぞることにより，高速に列挙を可能としている．本研究で扱った極大クリークに関しては以下のように親子関係を定義する．

K_0 を辞書式に最大である極大クリークとする．K_0 でない極大クリーク K に対して，$C(K_{\leq i-1}) \neq K$ を満たす最大の i における $C(K_{\leq i-1})$ をその親 $P(K)$ と定義する．また，そのような i を親インデクスと呼び，$i(K)$ と記す．$K \neq C(K_{\leq 0})$ なので，上記の $P(K)$ は定義可能であることが分かる．さらに，定義から $P(K)$ が K より辞書式に大きくなることから以下の補題を得る．

補題 1 極大クリーク上の親子関係が非巡回であり，K_0 を根とする内向木になる．

補題 1中の内向木を列挙木と呼ぶ．[17, 34] のアルゴリズムは（見かけ上はかなり異なるが本質的に）この列挙木をなぞることにより，高速な極大クリーク列挙アルゴリズムを構成している．

定義からすぐに極大クリーク K からその親 $P(K)$ は線形時間で求められることが分かる．しかしながら，K からその子集合を求めることは，それほど簡単ではない．

極大クリーク K と $i \in \{1, 2, \ldots, n\}$ に対して，

$$K[i] \quad = \quad C\Big((K_{\leq i} \cap \Gamma(v_i)) \cup \{v_i\}\Big). \quad (2.1)$$

とする．

補題 2 K と K' をグラフ G の極大クリークとする．そのとき，K' が K の子であるために必要十分条件は，下記の 4 つの条件を満たす i に対して $K' = K[i]$ が成立することである．

(a) $v_i \notin K$.

(b) $i > i(K)$.

(c) $K[i]_{\leq i-1} = K_{\leq i} \cap \Gamma(v_i)$.

(d) $K_{\leq i} = C(K_{\leq i} \cap \Gamma(v_i))_{\leq i}$.

さらに，もし，i が (a) $\sim$ (d) を満たすならば，その i は，$K[i]$ の親インデクスとなる．

極大クリークの子集合を高速に求めるために，上記の補題 2の条件 (c) と (d) を以下のように言い換える．

補題 3 K を G の極大クリークとする．このとき，i が条件 (c) をみたす必要十分条件は，下記の 3 つの条件を満たす j が存在しないことである．

(c-1) $j < i$.

(c-2) $v_j \notin K_{\leq i} \cap \Gamma(v_i)$.

(c-3) v_j が $K_{\leq i} \cap \Gamma(v_i) \cup \{v_i\}$ に属するすべての点と隣接している．

補題 4 K を G の極大クリークとする．このとき，i が条件 (d) をみたす必要十分条件は，下記の 4 つの条件を満たす j が存在しないことである．

(d-1) $j < i$.

(d-2) $v_j \notin K$.

(d-3) v_j が $K_{\leq j}$ に属するすべての点と隣接している．

(d-4) v_j が $K_{\leq i} \cap \Gamma(v_i)$ に属するすべての点と隣接している．

詳細は省略するが，本研究ではこの特徴付けを用いることにより，極大クリークのすべての子集合を $O(M(n))$ 時間，$O(n^2)$ 領域で計算可能なことを示し，以下の定理を得る．

定理 1 与えられた無向グラフ $G = (V, E)$ のすべての極大クリークを $O(M(n))$ 時間遅延で，かつ，$O(n^2)$ 領域で列挙できる．

3 連結度要求に基づく施設配置問題

連結度要求に基づく施設配置問題とは，与えられたネットワークにおいて，フロー（連結度）に基づく制約条件の下で最小コストを与えるソース集合（配置）を求める問題である．この問題は，例えば，マルチメディアネットワーク中にサービス要求量を指定した複数のクライアントが与えられたとき，その要求を満足しながら最小コストで（ミラー）サーバを配置するという問題をモデル化したものであり，信頼度を考慮に入れた施設配置問題として，ソース配置問題とも呼ばれ，近年盛んに研究されている（例えば，[3, 6, 35, 15, 16, 27, 32, 33] など）．また，ネットワーク理論で有名な連結度増大問題とも深く関連している．

ソース配置問題における制約条件としては，枝連結度，および，点連結度に基づくものがある．枝連結度要求はリンク故障に対する信頼度，点連結度要求は点故障に対する信頼度に対応しており，点連結度要求に対しては，ソース故障の存否に関して 2 種類の要求が考察されている [16, 27]．

これまでの研究成果： ソース配置問題に対するアルゴリズム論的研究は，無向，あるいは，有向ネットワーク中で，コスト関数と要求関数がそれぞれ，一様，あるいは，一般の場合に分けて行われている．表 1, 2, 3 にこれまで得られている最良の結果を示す．ただし，n, m はそれぞれネットワーク中の点数，枝数を示す．表から分かるように，一ヶ所（太字）を除き，全て多項式時間で（効率的に）解けるか，あるいは，強 NP 困難であるかが知られている．

表 1: ソース配置問題に対する既存の結果（枝連結度）

		コスト：一様	コスト：一般
要求：一様	無向	$O(n(m + n\log n))$	$O(n(m + n\log n))$
	有向	$O(n^3 m \log(n^2/m))$	強 NP 困難
要求：一般	無向	$O(nM(n, m))$	**弱 NP 困難**
	有向	強 NP 困難	強 NP 困難

$M(n, m)$: ネットワーク (n 点, m 枝) 中の最大フローの計算時間

表 2: ソース配置問題に対する結果（点連結度・ソース故障なし）

	コスト：一様	コスト：一般
要求：一様	強 NP 困難	強 NP 困難
要求：一般	強 NP 困難	強 NP 困難

表 3: ソース配置問題に対する結果（点連結度・ソース故障あり）

		コスト：一様	コスト：一般
要求：一様	無向	$O(\min\{k, \sqrt{n}\}kn^2)$	$O(\min\{k, \sqrt{n}\}kn^2)$
(k:要求量)	有向	$O(\min\{k, \sqrt{n}\}mn)$	$O(\min\{k, \sqrt{n}\}mn)$
要求：一般		強 NP 困難	強 NP 困難

しかしながら，NP 困難な場合に対する近似精度保証付きの近似アルゴリズムは，未だ開発されておらず，ネットワークが特別な構造（例えば，木構造）をもつときに効率的に解けるかどうかも分かっていない．また，ソース配置問題では，コスト関数として建設費用のみを扱っているが，建設費用に加え，供給量にも依存するコスト関数の考察が求められていた．

本研究班の成果： 本研究では，以下の成果を得る．

1. まず，未解決問題として残されていた，無向ネットワーク中の枝連結度に基づくソース配置問題の強 NP 困難性を示す．さらに近似困難性も示す．

2. ソース配置問題を劣モジュラ被覆問題として定式化することにより，すべてのNP困難な場合に適用可能な精度保証付きの近似アルゴリズムを開発する．このアルゴリズムは，枝連結度要求に対して最適な近似精度を与える．

3. 木構造ネットワークにおけるソース配置問題は，枝連結度要求のときは擬多項式時間で解け，(２種類の)点連結度要求のときは多項式時間で解けることを示す．ここで，擬多項式時間の改善は，[1] の弱NP困難性より，不可能である．

4. 供給量に関して凹なコスト関数も扱えるようソース配置問題を拡張し，これに対して2. と同様の結果を得る．

5. 無向ネットワーク中の一様な枝連結度要求を持つ拡張されたソース配置問題を，ラミナー被覆問題として定式化することにより，$O(nm+n^2(q+\log n))$ 時間アルゴリズムを開発する．ただし，q は供給に対するコストを求めるために要する時間であり，コスト関数がオラクルで与えられるとき，上記のアルゴリズムは最適である．

また，コスト関数が建設費と線形な運営費の和として記述できる場合はさらに高速に $O(n(m+n\log n))$ 時間で解け，より一般的なコスト関数に対しては計算困難であることを示す．

また，本論文で開発した 2. , 4. の劣モジュラ被覆問題，5. のラミナー被覆問題に対するアルゴリズムはソース配置問題以外の多くの離散最適化問題へ適用可能である．

以下の節の構成： 第 2．1 節では，ソース配置問題とその拡張についての定義を与える．第 2．2，2．3 節ではそれぞれ，ソース配置問題とその拡張に関する結果を示す．頁数制限のため，定理の証明，アルゴリズムなど多くを省略する．

3.1 ソース配置問題とその拡張

点集合 V と枝集合 A をもつグラフ G に容量関数 $u : A \to \mathbb{R}_+$ を付与したネットワーク $\mathcal{N} = (G=(V,A),u)$ を考える．ただし，$\mathbb{R}_+$ は非負実数の集合である．このネットワーク $\mathcal{N}$，要求関数 $d^-, d^+ : V \to \mathbb{R}_+$，コスト関数 $c : V \to \mathbb{R}_+$ が与えられたとき，ソース配置問題は以下のように記述できる．

$$
\begin{aligned}
\text{(SLP)}\quad \text{Min.}\ & \textstyle\sum_{v\in S} c(v) \\
\text{s.t.}\ & \psi^-(S,v) \geq d^-(v), \\
& \psi^+(v,S) \geq d^+(v)\quad (v\in V), \\
& S \subseteq V.
\end{aligned}
$$

ただし，$\psi^-(X,Y)$，$\psi^+(X,Y)$ は点集合 X から Y への連結度を表す．また，$\psi^-(S,\{v\})$，$\psi^+(\{v\},S)$ をそれぞれ簡潔に $\psi^-(S,v)$，$\psi^+(v,S)$ と書く．本論文では，$\psi^\pm$ として，次の３種類の連結度を考察する．

(i) $\psi^-(S,v)=\lambda(S,v)$, $\psi^+(v,S)=\lambda(v,S)$,

(ii) $\psi^-(S,v)=\kappa(S,v)$, $\psi^+(v,S)=\kappa(v,S)$,

(iii) $\psi^-(S,v) = \hat{\kappa}^-(S,v)$, $\psi^+(v,S) = \hat{\kappa}^+(v,S)$,

ただし，$\lambda(X,Y)$ は点集合 X から Y への最大フロー値で，$X\cap Y\neq\emptyset$ のとき $\lambda(X,Y)=+\infty$ とする．また，$\kappa(X,Y)$ は X から Y への端点以外の点を共有しない最大パス数で，$X\cap Y\neq\emptyset$，または，$v\in X, w\in Y$ である枝 $(v,w)\in A$ が存在するとき，$\kappa(X,Y)=+\infty$ とする．$\hat{\kappa}^-(S,v)$，および，$\hat{\kappa}^+(v,S)$ は，それぞれ点集合 S から点 v，および，v から S への v 以外の点を共有しない最大パス数を表し，$X\cap Y\neq\emptyset$ のとき $\hat{\kappa}^-(S,v) = \hat{\kappa}^+(v,S) = +\infty$ とする．(i) は枝連結度，(ii) はソース故障を許さない点連結度，(iii) はソース故障を許す点連結度を表す．

問題の拡張： 上記のソース配置問題では，コスト関数として施設の建設費用 (v における建設費用 $c(v)$) のみを扱っている．しかしながら，現実的なコスト関数として，建設費用に加え，供給量にも依存するものを考察することが求められている．従って，本論文では以下のように供給量を考慮したソース配置問題を考察する．ここでは，頁数制限のため，枝連結度 λ に対する拡張についてのみ述べる．

ネットワーク $\mathcal{N}$ 中のフロー $\varphi : A \to \mathbb{R}_+$ が以下の条件を満たすとき，供給 $x : V \to \mathbb{R}_+$ に対して実行可能であると呼ぶ．

$$-x(v) \le \partial\varphi(v) \le x(v) \quad (v \in V) \tag{1}$$

$$0 \le \varphi(a) \le u(a) \quad (a \in A) \tag{2}$$

ただし，$\partial\varphi(v)$ はフロー φ の点 v における境界を示し，

$$\partial\varphi(v) = \sum_{(v,w)\in A} \varphi(v,w) - \sum_{(w,v)\in A} \varphi(w,v)$$

と定義される．$\lambda^-(x;v)$ と $\lambda^+(x;v)$ をそれぞれ供給 x における点 v への最大流入量 $(-\partial\varphi(v)+x(v))$ と v からの最大流出量 $(\partial\varphi(v)+x(v))$ とする．枝連結度要求を持つ拡張されたソース配置問題は，ネットワーク $\mathcal{N} = (G = (V,A), u)$，要求関数 $d^-, d^+ : V \to \mathbb{R}_+$，各点 $v \in V$ におけるコストを表す単調な凹関数 $c_v : \mathbb{R}_+ \to \mathbb{R}_+$ が与えられたとき，以下のように記述できる．

$$\begin{aligned} &\text{Min.} \ \textstyle\sum_{v\in V} c_v(x(v)) \\ &\text{s.t.} \quad \lambda^-(x;v) \ge d^-(v), \\ &\qquad \lambda^+(x;v) \ge d^+(v) \ \ (v \in V), \\ &\qquad x(v) \ge 0 \ \ (v \in V). \end{aligned}$$

ここで，c_v の単調凹性は，ネットワーク設計問題などでよく扱われる自然な仮定である．

3.2 ソース配置問題に対する成果

ソース配置問題に対して以下の結果を得る．

無向・枝連結度要求をもつ場合の計算困難性： 無向ネットワーク中の枝連結度要求（すなわち，$\psi (= \psi^- = \psi^+) = \lambda$, $d = d^+ (= d^-)$）を持つソース配置問題に対して，以下の定理が成立する．

定理 2 無向ネットワーク中の枝連結度要求を持つソース配置問題は強 *NP* 困難である．

これは，[1] で提示されていた未解決問題を解くものである．この定理は，NP 困難問題として有名な集合被覆問題 [12] をソース配置問題に帰着させることによって示される．

さらに，我々は，集合被覆問題の近似困難性，および，帰着のギャップ保存性より以下の定理を得る．

定理 3 *NP*$\not\subseteq$*DTIME*$(N^{\log\log N})$ ならば，ある定数 $c > 0$ が存在して，どんな連結度要求を持つソース配置問題に対しても多項式時間 $c \ln \sum_{v\in V} d(v)$-近似アルゴリズムは存在しない．

ここで，NP$\not\subseteq$DTIME$(N^{\log\log N})$ とは，N を入力長としたとき，任意の NP 完全問題が $\mathrm{O}(N^{\log\log N})$ 時間の決定性アルゴリズムを持たないことを意味し，多くの計算量理論の研究者によって信じられている．また，α-近似アルゴリズム A とは，近似比（すなわち，(A の出力する解のコスト値)/(最適値)）が必ず α 以内である解を出力するアルゴリズムのことをいう．

木構造ネットワーク中のソース配置問題： また，与えられたネットワーク $\mathcal{N}$ が木構造であるとき，以下の肯定的な定理が成立する．

定理 4 木構造ネットワーク $\mathcal{N}$ におけるソース配置問題は，容量関数と要求関数が整数のとき，擬多項式時間で解ける．

定理 5 木構造ネットワーク $\mathcal{N}$ 中の点連結度要求 $\kappa, \hat{\kappa}$ をもつソース配置問題はともに多項式時間で解ける．

[1] の弱 NP 困難性の結果から，定理 3 の擬多項式時間は計算限界である．また，定理 4 は，点連結度要求を持つソース配置問題に対する初めての効率的に計算可能な部分クラスを示している．

3.3 拡張されたソース配置問題に対する成果

拡張されたソース配置問題に対しては，以下の肯定的な結果を得る．

近似アルゴリズム： 拡張されたソース配置問題を劣モジュラ被覆問題として定式化する．

V を有限集合，単調な劣モジュラ関数 $f : \mathbb{R}_+^V \to \mathbb{R}_+$，実数 M，各 $v \in V$ におけるコストを表す単調な凹関数 $c_v : \mathbb{R}_+ \to \mathbb{R}_+$ が与えられたとき，劣モジュラ被覆問題は以下のように記述できる．

$$\begin{aligned} &\text{Min.} \ \textstyle\sum_{v\in V} c_v(x(v)) \\ &\text{s.t.} \quad f(x) \ge M, \ \ x(v) \ge 0 \ \ (v \in V). \end{aligned}$$

ただし，関数 $f : \mathbb{R}^V \to \mathbb{R}$ が劣モジュラであるとは，任意の $x, y \in \mathbb{R}^V$ に対して，$f(x) + f(y) \geq f(x \wedge y) + f(x \vee y)$ が成り立つことをいう．ここで，$(x \wedge y)(v) = \min\{x(v), y(v)\}$, $(x \vee y)(v) = \max\{x(v), y(v)\}$ である．この劣モジュラ被覆問題は，劣モジュラ集合被覆問題の拡張である．拡張されたソース配置問題は，例えば，枝連結度要求の場合，

$$\begin{aligned} f(x) &= \sum_{v \in V} (\min\{\lambda^-(x;v), d^-(v)\} \\ &\quad + \min\{\lambda^+(x;v), d^+(v)\}) \\ M &= \sum_{v \in V} (d^-(v) + d^+(v)) \end{aligned}$$

とすることで，劣モジュラ被覆問題として定式化できる．

本研究では，この劣モジュラ被覆問題に対して，貪欲アルゴリズムを開発する．詳細は省略するが，このアルゴリズムを拡張されたソース配置問題に適用すると，任意の $x \in \mathbb{R}_+^V$ と $v \in V$ に対して，$g(\alpha) = f(x + \alpha\chi_v) - f(x)$ (ただし，χ_v は v に対する特性ベクトル) が高々$2n + 1$ 区分からなる区分線形関数となり，また，その折れ点は最大フロー問題を高々$2n$ 回解くことにより計算可能であることなどを用いて，以下の結果を得る．

定理 6 （拡張された）ソース配置問題は，容量，および，要求関数が整数である場合，多項式時間で $(1 + \ln \sum_{v \in V}(d^-(v) + d^+(v)))$-近似可能である．

定理 2 より，この貪欲アルゴリズムは枝連結度要求に対して，（オーダーの意味で）最適である．

無向・一様な枝連結度要求をもつ拡張ソース配置問題： 無向ネットワークにおいて一様な枝連結度要求（すなわち，$d(v) = k$ $(v \in V)$ ）をもつ拡張されたソース配置問題をラミナー被覆問題として定式化する．

有限集合 V 上のラミナー族 $\mathcal{F} \subseteq 2^V$，コストを表す単調な凹関数 $F : \mathbb{R}_+^V \to \mathbb{R}_+$，要求関数 $d : \mathcal{F} \to \mathbb{R}_+$ が与えられたとき，ラミナー被覆問題は以下のように記述できる．

$$\begin{aligned} \text{Min.} \quad & F(x) \\ \text{s.t.} \quad & \textstyle\sum_{v \in X} x(v) \geq d(X) \ (X \in \mathcal{F}), \\ & x(v) \geq 0 \ (v \in V). \end{aligned}$$

ここで，ラミナー族 $\mathcal{F}$ とは，任意の $X, Y \in \mathcal{F}$ に対して，$X \cap Y$, $X - Y$, $Y - X$ のいずれか一つは空集合となる集合族である．

ラミナー族は様々な組織の階層構造を表現できるため，この問題は多くの応用をもつ．また，最大フロー・最小カットの定理などを用いることにより，無向ネットワーク中の枝連結度増大問題やこの拡張されたソース配置問題もラミナー被覆問題として定式化可能なことが分かる．

本論文では，この問題に対して以下の結果を得る．

定理 7 ラミナー被覆問題は，

1. F が分離可能な単調凹関数で記述できるならば，$O(n^2 q)$ 時間で解ける．さらに，F がオラクルで与えられるときは，$\Omega(n^2 q)$ 時間必要である．
2. F が固定費つき線形関数（すなわち，施設建設費と線形運営コストの和）の和で記述できるならば，$O(n \log^2 n)$ 時間で解ける．
3. F が一般の凹関数ならば，NP 困難であり，さらに F がオラクルで与えられるときは $\Omega(2^{\frac{n}{2}} q)$ 時間必要である．

ただし，q は各 $x \in \mathbb{R}_+$ に対して $F(x)$ を求めるために要する時間である．*1.* の結果は，F がオラクルで与えられるとき，最適なアルゴリズム開発に成功したことを意味する．

この系として，以下の結果を得る．

系 1 無向ネットワーク中の一様な枝連結度要求を持つ拡張されたソース配置問題は，

1. $O(nm + n^2(q + \log n))$ 時間で解ける．
2. 各コスト関数 c_v が固定費つき線形関数として記述できる場合は，$O(n(m + n \log n))$ 時間で解ける．
3. より一般的なコスト関数（すなわち，F が一般の凹関数）のとき，計算困難である．

4 動的ネットワーク中の避難施設配置問題

点集合がV, 枝集合がAである (有向) グラフを$G=(V,A)$と記す. ここで, $n=|V|$, $m=|A|$とする. $c:A\to\mathbb{R}_+$ $c:A\to\mathbb{R}_+$ は各枝に非負の実数を与える容量関数, $\tau:A\to\mathbb{Z}_+$ は各枝始点から終点への輸送時間を与える非負整数値関数である とする. このようにグラフGの枝に容量関数cと輸送時間τが付与されたものを動的ネットワーク (dynamic network) と呼び, $\mathcal{N}=(G=(V,A),c,\tau)$と表す.

いま, 動的ネットワークの各点に供給量$b:V\to\mathbf{R}_+$が与えられているとする. このとき全ての点vの供給量$b(v)$を最速で送り届けられるような出口$t\in V$を 求める問題を動的ネットワーク上における施設配置問題と呼ぶ. より正確には, $V\setminus\{t\}$からの供給量をtへ流す動的フローを考えたときに, その全てのフローがtに到着する時間を最小にする出口tを求める施設配置問題である. この問題は, 交通ネットワークにおいて, すべての人が 最速に避難できるような避難施設をネットワーク中に1ヵ所求めるという問題であり, 静的ネットワーク・フローに基づくソース/シンク配置問題 [3, 32, 33] の動的版, あるいは, 1-センター問題 [20] の動的フロー版としてとらえることができる.

以下では, 離散時間動的フローの定義を与える. 任意の枝$(u,v)\in A$, $\theta\in\{0,1,\cdots,\tau(u,v)\}$, $k\in\mathbf{Z}_+$ に対して, $f_k((u,v),\theta)$ を時刻 k に枝(u,v)の第θ部を流れるフロー量とする. ただし, $f_0((u,v),\theta)=0$ $(1\le\theta\le\tau(u,v))$ と定義する. これは, 時刻0において, 枝の始点以外の部分を流れるフローがないことを表す. この$f_k((u,v),\theta)$ $((u,v)\in A,\ \theta\in\{0,1,\cdots,\tau(u,v)\},\ k\in\mathbf{Z}_+)$が以下に示す (a), (b), (c) の条件を満足するとき, ネットワーク$\mathcal{N}$上の出口tに対する動的フローと呼ぶ.

(a) 容量条件 (Capacity constraints): 任意の$(u,v)\in A$, $\theta\in\{0,1,\cdots,\tau(u,v)\}$, $k\in\mathbf{Z}_+$ に 対して,

$$0\le f_k((u,v),\theta)\le c(u,v) \tag{4.1}$$

が成立する.

(b) フロー移動条件 (Flow transition): 任意の$(u,v)\in A$, $\theta\in\{0,1,\cdots,\tau(u,v)-1\}$, $k\in\mathbf{Z}_+$ に対して,

$$f_k((u,v),\theta)=f_{k+1}((u,v),\theta+1) \tag{4.2}$$

が成立する.

(c) 流量保存則 (Flow conservation): 任意の$v\in V\setminus\{t\}$, $k\in\mathbf{Z}_+$ に対して,

$$\sum_{u:(u,v)\in A} f_k((u,v),\tau(u,v))+h_{k-1}(v) = \sum_{w:(v,w)\in A} f_k((v,w),0)+h_k(v) \tag{4.3}$$

$$h_{-1}(v)=b(v),\quad h_k(v)\ge 0\quad (k=0,1,\cdots) \tag{4.4}$$

が成立する. ただし, $f_k((v,w),0)$ は, 時刻kにおいてwに向かいvを離れたフロー量, $h_k(v)$は, 時刻kにおいて点vに留まるフロー量を表す. すなわち, 各点でフローの滞留を許すモデルである.

この定式化において, 条件 (a) は, どの時刻どの地点においてもフロー量が容量条件をみたすことを意味している. 条件 (b) は, 枝(u,v)の第θ部を流れるフローは, 1単位時間で枝(u,v)の第$\theta+1$部に移動することを示している. また, 条件 (c) は, 出口t以外の点vでは, 各時刻kにvに到達するフロー量と時刻$k-1$にvで滞留したフロー量との総和が各時刻kにvを去るフロー量と時刻kにvで滞留したフロー量との総和と等しいことを示している.

我々が扱う施設配置問題においては, (c) に示すように各点でのフローの滞留を許すモデルを用いているが, 許さないモデルでも最適解等は不変である (この性質は, 例えば, [10, 14] で議論されている).

一般に動的フローに関する問題は, 与えられた動的ネットワークに対する時間展開ネットワーク上での静的フローを扱うことにより解かれる [10]. 動的ネットワーク$\mathcal{N}=(G=(V,A),c,\tau)$と時間区間$T$に対する時間展開ネッ トワーク (time-expanded network) $\mathcal{N}(T)$とは, 容量関数$c:A\to$

$\mathbb{R}_+$ 付き有向グラフ $G(T) = (V(T), A(T))$ のことである．ここで，$V(T)$ は，元の動的ネットワークの各点 $v \in V$ に対して，$(T+1)$ 個のコピー $v(0), \cdots, v(T)$ を作り，それらの全体としたもの，すなわち，

$$V(T) \quad = \quad \{v(0), \cdots, v(T) \mid v \in V\}$$

であり，$A(T)$ は，元の動的ネットワークの各枝 $(u,v) \in A$ に対して，$(u(\theta), v(\theta + \tau(u,v)))$ $(\theta = 0, 1, \cdots, T - \tau(u,v))$ というように，u と v を $\tau(u,v)$ 分ずらし結んだ $(T-\tau(u,v)+1)$ 個のコピーと，各点 $v \in V$ に対する T 本の残留枝 (holdover arc) $(v(\theta), v(\theta+1))$ $(\theta = 0, 1, \cdots, T-1)$ を要素とするものである．

$$\begin{aligned} A(T) \ = \ & \{(u(\theta), v(\theta + \tau(u,v))) \mid (u,v) \in A, \\ & \theta = 0, 1, \cdots, T - \tau(u,v)\} \ \cup \ \{(v(\theta), \\ & v(\theta+1)) \mid v \in V, \theta = 0, 1, \cdots, T-1\}. \end{aligned}$$

枝の容量は，コピー枝 $(u(\theta), v(\theta + \tau(u,v)))$ には元の枝の容量 $c(u,v)$，残留枝には無限大を与えるものとする．定義から明らかに，時刻 T までの動的フロー f は，$\mathcal{N}(T)$ 中の静的フローとして表現される。

本研究で扱う避難施設配置問題は，入口 $v \in V \setminus \{t\}$，出口 t とする多始点 1 終点の最速動的フロー問題を n 回（出口 t を取り替えることにより）解くことにより最適な出口 $t \in V$ を求めることができる．すなわち，時間展開ネットワークを用い，最速時間 T を求めること（例えば，2 分探索を行う）により解くことはできるが，一般に時間展開ネットワークのサイズは入力の多項式サイズではなく，多項式時間解法ではない．Hoppe–Tardos [14] は，多始点多終点の最速動的フロー問題をこのような時間展開ネットワークを用いない強多項式時間アルゴリズムを開発した．従って，動的ネットワーク上の施設配置問題も強多項式時間で解けることが分かる．しかしながら，Hoppe–Tardos のアルゴリズムは，高次多項式時間アルゴリズムであり，必ずしも，実用的であるとは言えない．次節では，ネットワークが木構造であるとき，施設配置問題が高速に解けることを示す．

木構造動的ネットワーク中の避難施設配置問題

$G = (V, A)$ の枝を無向化することによって得られるグラフが木（tree）になるとき，動的ネットワーク $\mathcal{N} = (G = (V, A), c, \tau)$ が木構造であると言う．本節では，木構造動的ネットワーク $\mathcal{N} = (G = (V, A), c, \tau)$ における施設配置問題のアルゴリズムを与える．

交通ネットワークにおいて，すべての人がある避難施設 t に退避する状況を考えよう．このとき，ある点 v にいる人 α さんと β さんが，異なった避難路で施設 t に避難誘導されたとすると，避難誘導が混乱し，また，α さんと β さんの間に不公平が生じる．1 つの解決策として，同じ点 v にいる人は，すべて同じ経路で避難するという方法が考えられる．したがって，本研究では，一般の動的ネットワーク中の施設配置問題を以下に示すように 2 つのステップに分けて解くことを提案する．

(i) ネットワーク中で全域木を作る．

(ii) (i) で求めた全域木の中で最適な施設配置問題を解く．

もちろん，(i)(ii) まとめて，最速に退避できるような全域木とそれに基づく避難施設配置点 t を同時に求めることが望ましい．しかしながら，このような問題は，計算量の観点から難しいので，本研究では，(i),(ii) を別にして，(i) では，供給量 b，移動時間 τ，容量 c，グラフの形状（例えば，次数 (degree) や直径 (diameter) など）を考慮して，退避時間が小さくなるように全域木を求め，(ii) で，それに基づく配置点 t を求めることとする．(i) の基準として，例えば，枝コスト τ/c を最小にする全域木などが考えられる．本節では，上記の (ii) を多項式時間で行うアルゴリズムを紹介する．

以下での説明を簡単にするため，$G = (V, A)$ は，(無向）木 $T = (V, E)$ の枝を有向化したグラフ，すなわち，$A = \vec{E}\,(= \{(u,v), (v,u) \mid \{u,v\} \in E\})$ であると仮定する．

提案するアルゴリズムは，各点 $v \in V$ が到着テーブル（Arriving Table）A_v と送出テーブル（Sending table）S_v という 2 つのテーブルを用い

る．到着，送出テーブルともに時刻 k の関数であり，到着テーブルは，時刻 k に点 v に到着するフロー量

$$\sum_{u:(u,v)\in\vec{E}} f_k((u,v),\tau(u,v)) + \eta_k(v) \qquad (4.5)$$

を表し（ただし，$\eta_0(v) = b(v)$ and $\eta_k(v) = 0$ $(k = 1, 2, \cdots)$），送出テーブルは，時刻 k に点 v からその親 v' に向う (与えられた出口 t を根としたとき) 送出されるフロー量

$$f_k((v,v'),0) \qquad (4.6)$$

を表す．図1では，到着，送出テーブルの例を示す．

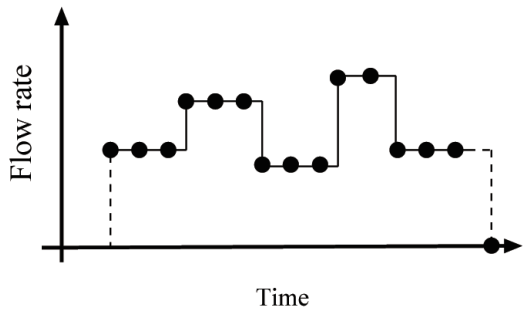

図 1: An example of table.

このようなテーブルを葉から順に構成する２つのフェイズから成る $O(n^2)$ 時間アルゴリズムが提案されていた [24]．本研究では，高速なアルゴリズムを開発するために，まず，１つのフェイズから成るアルゴリズムを構成し，次に，そのアルゴリズムにデータ構造として，動的に構造変更が可能な平衡２分木を用いる．このことにより，$O(n\log^2 n)$ 時間アルゴリズムを構成する．平衡２分木を用いたデータ構造の説明は，非常に技巧的，かつ，複雑であるので，本報告では，省略して，１つのフェイズから成るシンプルなアルゴリズムを紹介する．なお．このアルゴリズムは，素直なデータ構造を用いると $O(n^2)$ 時間必要となり，単にこのアルゴリズムを用いるだけでは，計算時間の改善はない．しかし，このアルゴリズムがシンプルであるため，上記の平衡２分木をうまく用いることがてきるため，結果として計算時間が改善される．

下記のシングルフェイズアルゴリズムは，直感的に，まず全ての葉のテーブルを作る．次に，作ったテーブルを利用することで，最適出口にはならない葉 v^*（より正確には，自分以外に最適出口が存在するような葉 v^*）を見つけ，その点を木 T から除く．v^* を除くことにより新たに葉となった点があれば，その点のテーブルを作る．ここで新たに葉となりうる点は高々一つであることに注意されたい．上記の作業を繰り返し行い，最終的に一点となったとき，その点を最適出口として出力するというものである．

アルゴリズム シングルフェイズ

入力: 木構造動的ネットワーク $\mathcal{N} = (T = (V,E), c, \tau, b)$.

出力: 最小輸送完了時間 $C(t)$ と，それを与える出口 t.

ステップ 0: $W := V$, T の葉の集合 を L とする．各 $v \in W$ に対して到着テーブル A_v をつくる．

ステップ 1: L に含まれる全ての点 v に対して，A_v に基づき v から $p(v)$ への送出テーブル S_v を作り，v から $p(v)$ へのフローの最終到着時刻 $Time(v)$ を求める．

ステップ 2: $\min_{v^*\in L} Time(v^*) = Time(v)$ である $v^* \in L$ に対して，$W := W \setminus \{v^*\}, L := L \setminus \{v^*\}$.
もし，$T[W]$ の葉でかつ，L に属さない点 v があれば，$L := L \cup \{v\}$ とする．さらに W に属さず v に隣接する点の送出テーブルに基づき v の到着テーブル A_v を作る．

ステップ 3: $|W| = 1$ であれば，そ の点を t として出力する．また，t の到着テーブルを作ることにより，最小輸送完了時間 $C(t)$ も出力する．そうでなければ，ステップ２へ．
□

このアルゴリズムの各反復において，ステップ２終了時には，L が絶えず $T[W]$ の葉 集合であることに注意されたい．

補題 5 シングルフェイズアルゴリズムは最適出口 t を出力する．

証明 点 t 以外の点 u が最適解であると仮定する．このとき，t と u を結ぶパス上で，t に隣接する頂点を w とする．いま，枝 (t,w) を除くことによりできる 2 つの連結成分で t 側のものを U_1 とする．また，$U_2 = U_1 \cup \{w\}$，$U_3 = (V - U_1) \cup \{t\}$ とする．木 $T[U_1]$ において出口を t としたときの最小輸送完了時間を k_1，木 $T[U_2]$ において出口を w としたときの最小輸送完了時間を k_2，木 $T[U_3]$ において出口を t としたときの最小輸送完了時間を k_3 とする．定義より明らかに

$$k_1 \leq k_2, \quad C(t) = max\{k_1, k_3\}, \quad C(u) \geq k_2 \tag{4.7}$$

また，k_3 はアルゴリズムのステップ 1 で計算され，ステップ 2 で，$Time(w) = min_{v \in L}\, Time(v)$ をみたすことにより，w が W, L から除かれているので，$k_3 \leq k_2$．さらに式 (4.7) より，$C(t) \leq C(u)$ が成立する．したがって，$C(t) = C(u)$ を得る．すなわち．アルゴリズムから出力された点 t も最適出口である． □

上記に説明したようにこのアルゴリズムにおいて，各テーブルを平衡 2 分木を用いて，間接的に表現することで高速化することができる．

定理 8 動的ネットワークが木構造であるとき，施設配置問題が $O(n \log^2 n)$ 時間で解くことができる．

5 正モジュラシステムの最小横断

最小横断問題とは，有限集合 V と $f(\emptyset) \geq d(\emptyset)$ を満たす 2 つの集合関数 $f : 2^V \to \mathbf{R}$，$d : 2^V \to \mathbb{R}$ から成るシステム (V, f, d) が与えられたとき，すべての $X \subseteq V - R$ に対して $f(X) \geq d(X)$ を満たす最小サイズの $R \subseteq V$ を求める問題である [31].

$$\begin{array}{ll} \text{Minimize} & |R| \\ \text{subject to} & f(X) \geq d(X) \text{ for all } X \subseteq V - R \\ & R \subseteq V. \end{array}$$

ここで，$f(\emptyset) \geq d(\emptyset)$ を仮定する．定義から明らかに，f，d が一般の集合関数のときは，効率に解くことができない．我々は，f が正モジュラ，劣モジュラ関数，d が模調関数であるときの最小横断問題を考察した．ここで，集合関数 $f : 2^V \to \mathbb{R}$ が劣モジュラであるとは，任意の V の部分集合 X, Y に対して，

$$f(X) + f(Y) \geq f(X \cup Y) + f(X \cap Y) \tag{5.1}$$

が成立することであり，正モジュラ関数であるとは，任意の V の部分集合 X, Y に対して，

$$f(X) + f(Y) \geq f(X - Y) + f(Y - X) \tag{5.2}$$

が成立することである．また，$d : 2^V \to \mathbb{R}$ が，すべての非空な $X \subseteq V$ が下記の条件を満たす $v \in X$ をもつとき， 模調であるといわれる．

$$d(Y) \geq d(X) \text{ for all } Y \subseteq X \text{ containing } v.$$

この問題は，ネットワーク設計問題として重要なソース配置問題や外部ネットワーク問題などの一般化とみなすことができる．ソース入り問題とは，与えられたネットワークにおいて，フロー (連結度)に基づく制約条件の下で最小コストを与えるソース集合(配置)を求める問題である．この問題は，例えば，マルチメディアネットワーク中にサービス要求量を指定した複数のクライアントが与えられたとき，その要求を満足しながら最小コストで (ミラー)サーバを配置するという問題をモデル化したものであり，信頼度を考慮に入れた施設配置問題として，近年盛んに研究されている．また，ネットワーク理論で有名な連結度増大問題とも深く関連している．より正確には，点集合 V と枝集合 A をもつグラフ G に容量関数 $u : A \to \mathbb{R}_+$ を付与したネットワーク $\mathcal{N} = (G = (V, A), u)$ を考える．ただし，$\mathbb{R}_+$ は非負実数の集合である．このネットワーク $\mathcal{N}$，要求関数 $p : V \to \mathbb{R}_+$ 与えられたとき，ソース配置問題は以下のように記述できる．

$$\begin{array}{ll} \text{Minimize} & |S| \\ \text{subject to} & \lambda_{\mathcal{N}}(S, v) \geq p(v) \text{ for all } v \in V \\ & S \subseteq V, \end{array}$$

ただし，$\lambda_{\mathcal{N}}(S, v)$ は，ネットワーク $\mathcal{N}$ 中の S-v 間の最大フロー量を示す．このソース配置問題は，最大フロー最小カット定理を用いることで，f が

正モジュラ，劣モジュラ関数，d が模調関数である最小横断問題であることが分かる．

我々は，正モジュラ f がであり，d が模調であるならば，極小な不足集合族が木ハイパーグラフとなることを示した．逆に，任意の木ハイパーグラフは，正モジュラ関数 f と 模調関数 d に対する最小横断問題の極小な不足集合族として表現可能であることも示した．

さらに，この構造的な特徴付けを用いることで，f が正，かつ劣モジュラ関数であり，d がある $p : V \to \mathbf{R}_+$ に対して，

$$d(X) = \max\{p(v) \mid v \in X\}$$

となるとき, あるいは, ある $r : V^2 \to \mathbf{R}_+$ に対して,

$$d(X) = \max\{r(v, w) \mid v \in X, w \in V - X\}$$

となるときに, 最小横断問題に対する多項式時間アルゴリズムを開発した．また，このアルゴリズムを用いることで無向ネットワークにおける外部ネットワーク問題も効率的に解けることを示した．

参考文献

[1] R. Agrawal and R. Srikant, Fast algorithms for mining association rules in large databases, *Proc. VLDB '94,* pp. 487–499, 1994.

[2] R. Agrawal, H. Mannila, R. Srikant, H. Toivonen and A. I. Verkamo, Fast discovery of association rules, *In Advances in Knowledge Discovery and Data Mining,* MIT Press, pp. 307–328, 1996.

[3] K. Arata, S. Iwata, K. Makino and S. Fujishige, Locating sources to meet flow demands in undirected networks, *Journal of Algorithms*, 42 (2002) 54-68.

[4] Y. Asahiro, T. Horiyama, K. Makino, H. Ono, T. Sakuma, and M. Yamashita, How to Collect Balls Moving in the Euclidean Plane, *Discrete Applied Mathematics*, 154 (2006) 2247-2262.

[5] D. Avis and K. Fukuda, Reverse search for enumeration, *Discrete App. Math.,* 65 (1996) 21–46.

[6] M. Bárász, J. Becker, and A. Frank: An algorithm for source location in directed graphs, *Operations Research Letters*, **33** (2005), 221–230.

[7] N. Chiba and T. Nishizeki, Arboricity and subgraph listing algorithms, *SIAM J. Comput.*, 14 (1985) 210-223.

[8] D. Coppersmith and S. Winograd, Matrix multiplication via arithmetic progression, *Journal of Symbolic Computation*, 9 (1990) 251–280.

[9] T. Eiter, G. Gottlob and K. Makino, New results on monotone dualization and generating hypergraph transversals, *SIAM J. Comput.*, 32 (2003) 514–537.

[10] L. R. Ford, Jr. and D. R. Fulkerson, *Flows in Networks*, Princeton University Press, Princeton, NJ, 1962.

[11] S. Fujishige, K. Makino, T. Takabatake, and K. Kashiwabara, Polybasic polyhedra: Structure of polyhedra with edge vectors of support size at most 2, *Discrete Mathematics*, 280 (2004) 13-27.

[12] M. R. Garey and D. S. Johnson, *Computers and Intractability*, Freeman, New York, 1979.

[13] D. Gaur and K. Makino, On the fractional chromatic number of monotone self-dual Boolean functions, *FAW 2007* LNCS **4613** (2007), 148-159.

[14] B. Hoppe and É. Tardos, The quickest transshipment problem, *Mathematics of Operations Research*, 25 (2000) 36–62.

[15] H. Ito and M. Yokoyama, Edge connectivity between nodes and node-subsets, *Networks*, 31 (1998) 157-164.

[16] H. Ito, M. Ito, Y. Itatsu, K. Nakai, H. Uehara, and M. Yokoyama: Source location problems cosidering vertex-connectivity and edge-connectivity simultaneously. *Networks*, 40 (2002) 63-70.

[17] D. S. Johnson, M. Yanakakis and C. H. Papadimitriou, On generating all maximal independent sets, *Info. Proc. Lett.*, 27 (1998) 119–123.

[18] S. R. Kumar, P. Raghavan, S. Rajagopalan, and A. Tomkins, Trawling the web for emerging cyber-communities, *Proc. the Eighth International World Wide Web Conference,* Toronto, Canada, 1999.

[19] E. L. Lawler, J. K. Lenstra and A. H. G. Rinnooy Kan, Generating all maximal independent sets, NP-hardness and polynomial-time algorithms, *SIAM J. Comput.*, 9 (1980) 558–565.

[20] P. B. Mirchandani and R. L. Francis: *Discrete Location Theory* (John Wile & Sons, Inc., 1989).

[21] K. Makino, S. Tamaki, and M. Yamamoto, On the Boolean connectivity problem for Horn relations, *SAT 2007*, LNCS 4501 (2007), 187-200.

[22] K. Makino, T. Uno, New algorithms for enumerating all maximal cliques, *Algorithm Theory – SWAT 2004*, edited by T. Hagerup and J. Katajainen, Humlebaek (Denmark), Lecture Notes in Computer Science 3111 (2004) 260-272.

[23] K. Makino, U. Uno, T. Ibaraki, Minimum Edge Ranking Spanning Trees of Split Graphs, *Discrete Applied Mathematics*, 154 (2006) 2373-2386.

[24] S. Mamada, K. Makino and S. Fujishige: Optimal sink location problem for dynamic flows in a tree network, *IEICE Trans. Fundamentals*, E85-A (2002) 1020–1025.

[25] S. Mamada, T. Uno, K. Makino, S. Fujishige, A tree partitioning problem arising from an evacuation problem in tree dynamic networks, *Journal of the Operations Research Society of Japan* 48 (2005) 196-206.

[26] S. Mamada, T. Uno, K. Makino, and S. Fujishige, An $O(n \log^2 n)$ algorithm for the optimal sink location problem in dynamic tree networks, *Discrete Applied Mathematics*, 154 (2006) 2387-2401.

[27] H. Nagamochi, T. Ishii and H. Ito, Minimum cost source location problem with vertex-connectivity requirements in digraphs, *Information Processing Letters*, 80 (2001) 287–294.

[28] 坂下麻里子，牧野和久，藤重悟, 無向ネットワーク中のソース配置問題に対する近似アルゴリズム, *FIT 2004*, 3 (2004) 5-6.

[29] M. Sakashita, K. Makino, and S. Fujishige: Minimizing a monotone concave function with laminar covering constraints, *ISAAC2005*, LNCS **3827** (2005), 71–81.

[30] M. Sakashita, K. Makino, and S. Fujishige: Minimum cost source location problems with flow requirements, *LATIN2006* LNCS **3887** (2006), 769–781.

[31] M. Sakashita, K. Makino, H. Nagamochi, and S. Fujishige, Minimum Transversals in Posi-modular Systems, *ESA 2006, Lecture Notes in Computer Science*, 4168 (2006) 576-587.

[32] H. Tamura, M. Sengoku, S. Shinoda and T. Abe, Some covering problems in location theory on flow networks, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E75-A (1992) 678-683.

[33] 田村, 菅原, 仙石, 篠田, 無向フローネットワークにおける総合被覆問題について, 電子情報通信学会論文誌, J81-A (1998) 863-869.

[34] S. Tsukiyama, M. Ide, H. Ariyoshi and I. Shirakawa, A new algorithm for generating all the maximal independent sets, *SIAM J. Comput.*, 6 (1977) 505–517.

[35] J. van den Heuvel and M. Johnson: Transversals of subtree hypergraphs and the source location problem in digraphs, *CDAM Research Report*, LSE-CDAM-2004-10, London School of Economics.

研究業績一覧

学術論文

1. S. Fujishige, K. Makino, T. Takabatake, and K. Kashiwabara:
"Polybasic polyhedra: Structure of polyhedra with edge vectors of support size at most 2", Discrete Mathematics, 280, 13-27, 2004.
概要: In the present paper we introduce a generalized concept of base polyhedron. We consider a class of pointed convex polyhedra in $\mathbf{R}^V$ whose edge vectors have supports of size at most 2. We call such a convex polyhedron a polybasic polyhedron. The class of polybasic polyhedra includes ordinary base polyhedra, submodular/supermodular polyhedra, generalized polymatroids, bisubmodular polyhedra, polybasic zonotopes, boundary polyhedra of flows in generalized networks etc. We show that for a pointed polyhedron $P \subseteq \mathbf{R}^V$ the following three statements are equivalent:

   (1) P is a polybasic polyhedron.
   (2) Each face of P with a normal vector of the full support V is obtained from a base polyhedron by a reflection and scalings along axes.
   (3) The support function of P is a submodular function on each orthant of $\mathbf{R}^V$.

   This reveals the geometric structure of polybasic polyhedra and its relation to submodularity.

2. K. Makino, T. Uno:
"New algorithms for enumerating all maximal cliques", SWAT 2004, Lecture Notes in Computer Science, 3111, 260-272, 2004.
概要: In this paper, we consider the problems of generating all maximal (bipartite) cliques in a given (bipartite) graph $G = (V, E)$ with n vertices and m edges. We propose two algorithms for enumerating all maximal cliques. One runs with $\mathrm{O}(M(n))$ time delay and in $\mathrm{O}(n^2)$ space and the other runs with $\mathrm{O}(\Delta^4)$ time delay and in $\mathrm{O}(n+m)$ space, where Δ denotes the maximum degree of G, $M(n)$ denotes the time needed to multiply two $n \times n$ matrices, and the latter one requires $\mathrm{O}(nm)$ time as a preprocessing.

   For a given bipartite graph G, we propose three algorithms for enumerating all maximal bipartite cliques. The first algorithm runs with $\mathrm{O}(M(n))$ time delay and in $\mathrm{O}(n^2)$ space, which immediately follows from the algorithm for the non-bipartite case. The second one runs with $\mathrm{O}(\Delta^3)$ time delay and in $\mathrm{O}(n + m)$ space, and the last one runs with $\mathrm{O}(\Delta^2)$ time delay and in $\mathrm{O}(n+m+N\Delta)$ space, where N denotes the number of all maximal bipartite cliques in G and both algorithms require $\mathrm{O}(nm)$ time as a preprocessing.

   Our algorithms improve upon all the existing algorithms, when G is either dense or sparse. Furthermore, computational experiments show that our algorithms for sparse graphs have significantly good performance for graphs which are generated randomly and appear in real-world problems.

3. 坂下麻里子，牧野和久，藤重悟:
"無向ネットワーク中のソース配置問題に対する近似アルゴリズム", FIT 2004, 3, 5-6, 2004.

概要: 本研究では，無向ネットワーク中のソース配置問題が強NP困難であり，かつ近似不可能であることを示す．さらに，欲張り法に基づく最適な近似アルゴリズムを構成する

4. M. Sakashita, K. Makino, S. Fujishige: "Minimizing a Monotone Concave Function with Laminar Covering Constraints", ISAAC 2005, Lecture Notes in Computer Science, 3827, 71-81, 2005.
概要: Let V be a finite set with $|V| = n$. A family $\mathcal{F} \subseteq 2^V$ is called *laminar* if for arbitrary two sets $X, Y \in \mathcal{F}$, $X \cap Y \neq \emptyset$ implies $X \subseteq Y$ or $X \supseteq Y$. Given a laminar family $\mathcal{F}$, a demand function $d : \mathcal{F} \to \mathbf{R}_+$, and a monotone concave cost function $F : \mathbf{R}_+^V \to \mathbf{R}_+$, we consider the problem of finding a minimum-cost $x \in \mathbf{R}_+^V$ such that $x(X) \geq d(X)$ for all $X \in \mathcal{F}$. Here we do not assume that the cost function F is differentiable or even continuous. We show that the problem can be solved in $\mathrm{O}(n^2 q)$ time if F can be decomposed into monotone concave functions by the partition of V that is induced by the laminar family $\mathcal{F}$, where q is the time required for the computation of $F(x)$ for any $x \in \mathbf{R}_+^V$. We also prove that if F is given by an oracle, then it takes $\Omega(n^2 q)$ time to solve the problem, which implies that our $\mathrm{O}(n^2 q)$ time algorithm is optimal in this case. Furthermore, we propose an $\mathrm{O}(n \log^2 n)$ algorithm if F is the sum of linear cost functions with fixed setup costs. These also make improvements in complexity results for source location and edge-connectivity augmentation problems in undirected networks. Finally, we show that in general our problem requires $\Omega(2^{\frac{n}{2}} q)$ time when F is given implicitly by an oracle, and that it is NP-hard if F is given explicitly.

5. S. Mamada, T. Uno, K. Makino, S. Fujishige: "A tree partitioning problem arising from an evacuation problem in tree dynamic networks", Journal of the Operations Research Society of Japan, 48, 196-206, 2005.
概要: In this paper, we present a first polynomial time algorithm for the monotone min-max tree partitioning problem and show that the min-max tree partitioning problem is NP-hard if the cost function is not monotone, and that the min-sum tree partitioning problem is NP-hard even if the cost function is monotone. We also consider an evacuation problem in dynamic networks as an application of the tree partitioning problem. The evacuation problem is one of the basic studies on crisis management systems for evacuation guidance of residents against large-scale disasters. We restrict our attention to tree networks and consider flows such that all the supplies going through a common vertex are sent out through a single arc incident to it, since one of the ideal evacuation plans makes everyone to be evacuated fairly and without confusion.

6. M. Sakashita, K. Makino, S. Fujishige: "Minimum Cost Source Location Problems with Flow Requirements", LATIN 2006, Lecture Notes in Computer Science, 3887, 769-780, 2006.
概要: In this paper, we consider source location problems and their generalizations with three connectivity requirements λ, κ and $\hat{\kappa}$. We show that the source location problem with edge-connectivity requirement λ in undirected networks is strongly NP-hard, and that no source location problems with three connectivity requirements in undirected/directed networks are approximable within a ratio of $\mathrm{O}(\ln D)$, unless NP has an $\mathrm{O}(N^{\log \log N})$-time deterministic algorithm. Here D denotes the sum of given demands. We also devise $(1 + \ln D)$-approximation algorithms for all the extended source location problems if we have the integral capac-

ity and demand functions. Furthermore, we study the extended source location problems when a given graph is a tree. Our algorithms for all the extended source location problems run in pseudo-polynomial time and the ones for the source location problem with vertex-connectivity requirements κ and $\hat{\kappa}$ run in polynomial time, where pseudo-polynomiality for the source location problem with the arc-connectivity requirement λ is best possible unless P=NP, since it is known to be weakly NP-hard, even if a given graph is a tree.

7. M. Sakashita, K. Makino, H. Nagamochi, S. Fujishige:
"Minimum Transversals in Posi-modular Systems", ESA 2006, Lecture Notes in Computer Science, 4168, 576-587, 2006.
概要: Given a system (V, f, d) on a finite set V consisting of two set functions $f : 2^V \to \mathbb{R}$ and $d : 2^V \to \mathbb{R}$, we consider the problem of finding a set $R \subseteq V$ of the minimum cardinality such that $f(X) \geq d(X)$ for all $X \subseteq V - R$, where the problem can be regarded as a natural generalization of the source location problems and the external network problems in (undirected) graphs and hypergraphs. We give a structural characterization of minimal deficient sets of (V, f, d) under certain conditions. We show that all such sets form a tree hypergraph if f is posi-modular and d is modulotone (i.e., each nonempty subset X of V has an element $v \in X$ such that $d(Y) \geq d(X)$ for all subsets Y of X that contain v), and that conversely any tree hypergraph can be represented by minimal deficient sets of (V, f, d) for a posi-modular function f and a modulotone function d. By using this characterization, we present a polynomial-time algorithm if, in addition, f is submodular and d is given by either $d(X) = \max\{p(v) \mid v \in X\}$ for a function $p : V \to \mathbb{R}_+$ or $d(X) = \max\{r(v, w) \mid v \in X, w \in V - X\}$ for a function $r : V^2 \to \mathbb{R}_+$. Our result provides first polynomial-time algorithms for the source location problem in hypergraphs and the external network problems in graphs and hypergraphs. We also show that the problem is intractable, even if f is submodular and $d \equiv \mathbf{0}$.

8. S. Mamada, T. Uno, K. Makino, S. Fujishige:
"An $O(n \log^2 n)$ algorithm for the optimal sink location problem in dynamic tree networks", Discrete Applied Mathematics, 154, 2387-2401, 2006.
概要: In this paper, we consider a sink location in a dynamic network which consists of a graph with capacities and transit times on its arcs. Given a dynamic network with initial supplies at vertices, the problem is to find a vertex v as a sink in the network such that we can send all the initial supplies to v as quickly as possible. We present an $\mathrm{O}(n \log^2 n)$ time algorithm for the sink location problem, in a dynamic network of tree structure where n is the number of vertices in the network. This improves upon the existing $\mathrm{O}(n^2)$-time bound [24]. As a corollary, we also show that the quickest transshipment problem can be solved in $\mathrm{O}(n \log^2 n)$ time if a given network is a tree and has a single sink. Our results are based on data structures for representing tables (i.e., sets of intervals with their height), which may be of independent interest.

9. K. Makino, U. Uno, T. Ibaraki:
"Minimum Edge Ranking Spanning Trees of Split Graphs", Discrete Applied Mathematics, 154, 2373-2386, 2006.
概要: Given a graph G, the minimum edge ranking spanning tree problem (MERST) is to find a spanning tree of G whose edge ranking is minimum. However, this problem is known to be NP-hard for general

graphs. In this paper, we show that the problem MERST has a polynomial time algorithm for split graphs, which have useful applications in practice. The result is also significant in the sense that this is a first non-trivial graph class for which the problem MERST is found to be polynomially solvable. We also show that the problem MERST for threshold graphs can be solved in linear time, where threshold graphs are known to be split.

10. Y. Asahiro, T. Horiyama, K. Makino, H. Ono, T. Sakuma, M. Yamashita:
"How to Collect Balls Moving in the Euclidean Plane", Discrete Applied Mathematics, 154, 2247-2262, 2006.
概要: In this paper, we study how to collect n balls moving with constant velocities in the Euclidean plane by k robots moving on straight track-lines through the origin. Since all the balls might not be caught by robots, differently from Moving-Target TSP, we consider the following 3 problems in various situations: (i) deciding if k robots can collect all n balls, (ii) maximizing the number of the balls collected by k robots, and (iii) minimizing the number of the robots to collect all n balls. The situations considered here contain the cases in which track-lines are given (or not), and track-lines are identical (or not). For all problems and situations, we provide polynomial time algorithms or proofs of intractability, which clarify the tractability-intractability frontier in the ball collecting problems in the Euclidean plane.

11. D. Gaur, K. Makino:
"On the Fractional Chromatic Number of Monotone Self-dual Boolean Functions", FAW 2007, Lecture Notes in Computer Science, 4613, 148-159, 2007.
概要: We compute the exact fractional chromatic number for several classes of monotone self-dual Boolean functions. We characterize monotone self-dual Boolean functions in terms of the optimal value of an LP relaxation of a suitable strengthening of the standard IP formulation for the chromatic number. We also show that determining the self-duality of a monotone Boolean function is equivalent to determining the feasibility of a certain point in a polytope defined implicitly.

12. K. Makino, S. Tamaki, M. Yamamoto:
"On the Boolean Connectivity Problem for Horn Relations", SAT 2007, Lecture Notes in Computer Science, 4501, 187-200, 2007.
概要: Gopalan et al. studied in ICALP06 connectivity properties of the solution-space of Boolean formulas, and investigated complexity issues on the connectivity problems in Schaefer's framework. A set S of logical relations is Schaefer if all relations in S are either bijunctive, Horn, dual Horn, or affine. They conjectured that the connectivity problem for Schaefer is in P. We disprove their conjecture by showing that there exists a set S of Horn relations such that the connectivity problem for S is coNP-complete. We also show that the connectivity problem for bijunctive relations can be solved in $O(\min n|\phi|, T(n))$ time, where n denotes the number of variables, ϕ denotes the corresponding 2-CNF formula, and $T(n)$ denotes the time needed to compute the transitive closure of a directed graph of n vertices. Furthermore, we investigate a tractable aspect of Horn and dual Horn relations with respect to characteristic sets.

研究会等

1. 間々田聡子, 宇野毅明, 牧野和久, 藤重悟:
"木構造動的ネットワークにおける複数個の施設配置問題", 日本応用数理学会研究部会連合発表会, 2005 年 3 月.

概要: 本研究では，各点に供給量 $b \in \mathbb{Z}_+^n$ をもつ木構造動的ネットワークと完了時間 θ が与えられたとき，θ 時間以内にすべての供給量を流し込むために必要な最小個数の点集合 W を求める問題を考察する．我々はこの施設配置問題に対する $O(n^2 \log^2 n)$ 時間アルゴリズムを開発する．

2. 坂下麻里子，牧野和久，藤重悟:
"フロー要求を持つ最小費用ソース配置問題",
日本応用数理学会研究部会連合発表会, 2005 年 3 月.
概要: ソース配置問題とは，与えられたネットワークにおいて，フロー（連結度）に基づく制約条件の下で最小コストを与えるソース集合（配置）を求める問題である．我々はこのソース配置問題に対して以下の結果を得る．
1. 無向ネットワーク中の枝連結度に基づくソース配置問題の強 NP 困難性を示す．さらに近似困難性も示す.
2.(拡張された) ソース配置問題に対する近似アルゴリズムを開発する．このアルゴリズムは，枝連結度要求に対して最適な近似精度を与える．
3. 木構造ネットワークにおけるソース配置問題は，枝連結度要求のときは擬多項式時間で解け,（２種類の）点連結度要求のときは多項式時間で解けることを示す.
4. 無向ネットワーク中の一様な枝連結度要求を持つ拡張されたソース配置問題に対する $O(nm + n^2(q + \log n))$ 時間アルゴリズムを開発する．ただし，q は供給に対するコストを求めるために要する時間であり，コスト関数がオラクルで与えられるとき，上記のアルゴリズムは最適である．また，コスト関数が建設費と線形な運営費の和として記述できる場合はさらに高速に $O(n(m + n \log n))$ 時間で解け，より一般的なコスト関数に対しては計算困難であることを示す.

3. 坂下 麻里子, 牧野 和久, 藤重 悟:
"Approximation Algorithms for Source Location Problems with Flow Requirements",
電子情報通信学会コンピュテーション研究会, COMP2005-25, 43-50, 2005 年 6 月.

概要: In this paper, we consider source location problems with three kinds of connectivity requirements, where the problem with arc-connectivity requirement λ is, for example, to find a minimum-cost set $S \subseteq V$ in a given graph $G = (V, A)$ with a capacity function $u : A \to \mathbb{R}_+$ such that for each vertex $v \in V$, the arc-connectivity $\lambda^-(S, v)$ from S to v (resp., $\lambda^+(S, v)$ from v to S) at least a given demand $d^-(v)$ (resp., $d^+(v)$). We show that the source location problem with edge-connectivity requirement in undirected networks is strongly NP-hard, which solves an open problem posed by Arata *et al.* [3], and that it is not approximable within a ratio of $O(\ln \sum_{v \in V} d(v))$, unless NP has an $O(N^{\log \log N})$-time deterministic algorithm. We also study the source location problems when a given graph is a tree. We devise a pseudo-polynomial time algorithm for the source location problem with arc-connectivity requirement, and a polynomial time algorithm for the source location problems with two kinds of vertex-connectivity requirements, where pseudo-polynomiality for the arc-connectivity requirement is best possible unless P=NP, since it is known to be weakly NP-hard, even if a given graph is a tree. We further study the extensions of the source location problems to take supply value of each source into account, where the extended problems has monotone concave cost functions c_v $(v \in V)$ which model the ones depending not only on the fixed setup cost, but also on the supply value. We devise $(1 + \ln \sum_{v \in V}(d^-(v) + d^+(v)))$-approximation algorithms for the extended source location problems if we have the integral capacity and demand functions. This shows that our approximation algorithm for the problem with arc-connectivity requirement is optimal.

4. 坂下 麻里子, 牧野 和久, 藤重 悟:

“ソース配置問題とその拡張”, 日本オペレーションズ・リサーチ学会アルゴリズム研究部会, 2005 年 5 月.
概要: フロー要求に基づく施設配置問題であるソース配置問題とその拡張にたいして主に計算量論的観点から考察する．解くに近似の可能性について議論する．

学会大会等

1. 牧野和久:
“単調ブール関数の双対化問題について”, 日本オペレーションズ・リサーチ学会秋季研究発表会, 182-183, 2004 年 11 月.

2. 間々田聡子, 宇野毅明，牧野和久, 藤重悟:
“木構造動的ネットワークにおける複数個の施設配置問題”, 日本オペレーションズリサーチ学会秋季研究発表会, 222-223, 2004 年 11 月.

3. 坂下麻里子，牧野和久，藤重悟:
“無向ネットワーク中のソース配置問題の強ＮＰ困難性とその近似アルゴリズム”, 日本オペレーションズ・リサーチ学会秋季研究発表会, 224-225, 2004 年 11 月.

文部科学省科学研究費補助金 特定領域研究 (課題番号 16092215)

B06: 暗号システムに対する実装攻撃の適用と限界に関する計算論的研究

現在活発ではあるが断片的に提案されている暗号アルゴリズムへの種々の実装攻撃に対して計算論的な立場からその限界を明らかし、現実性のある脅威かどうかの客観的評価指標を検討した。また、耐タンパ性を有するワードウエアを仮定し、公開鍵暗号を利用せず、非対称原理を実現する暗号システムの設計を行った。

研究組織

研究代表者： 櫻井 幸一　九州大学大学院 システム情報科学研究院
研究分担者： 酒井 康行　三菱電機株式会社 情報技術総合研究所
高木 剛　公立はこだて未来大学 システム情報科学部
(平成 17–19 年度)
田端 利宏　岡山大学大学院 自然科学研究科

交付決定額 (配分額)

平成 16 年度	360,000 円
平成 17 年度	360,000 円
平成 18 年度	360,000 円
平成 19 年度	360,000 円
合　計	1,440,000 円

研究成果の概要

- Yasuyuki SAKAI, Kouichi SAKURAI, *"On the Vulnerability of Exponent Recodings for the Exponentiation against Side Channel Attacks,"* IEICE Transactions, Vol.E88-A No.1, pp.154-160, Jan. 2005.
- Dong-Guk HAN , Tetsuya IZU, Jongin LIM, Kouichi SAKURAI, *"Side Channel Cryptanalysis on XTR Public Key Cryptosystem,"* IEICE Transactions, Vol.E88-A No.5, pp.1214-1223, May. 2005.
- 酒井　康行, 鈴木　大輔, 佐伯　稔, 佐藤　恒夫, "現実の脅威「サイドチャネル解析」" 日経エレクトロニクス 2005 年連載 (1)7 月 18 日号　(2) 8 月 1 日号　(3) 8 月 15 日号.
- Katsuyuki Okeya, Tsuyoshi Takagi, *"Security Analysis of CRT-Based Cryptosystems,"* International Journal of Information Security, Vol.5, No.3, pp.177-185, Springer-Verlag.
- Camille Vuillaume, Katsuyuki Okeya, Tsuyoshi Takagi, *"Defeating Simple Power Analysis on Koblitz Curves,"* IEICE Transactions, Vol.E89-A No.5 pp.1362-1369, IEICE, 2006.
- Kohei Tatara, Toshihiro Tabata, Kouichi Sakurai, *"Actively Modifying Control Flow of Program for Efficient Anormaly Detection,"* 10th International Conference on Knowledge-Based & Intelligent Information & Engineering Systems , Lecture Notes in Computer Science, Vol.4252, pp.737-744, (10, 2006).

1 一般化 Mersenne 素数など高速処理向けな定義体標数を用いた剰余算実装に対する SPA

1.1 はじめに

楕円曲線暗号実装に対するサイドチャネル解析法を考察する．楕円曲線ドメインパラメータは，数学的安全条件を満たすように選ぶことは必須要件である．しかし，実際の情報セキュリティシステムへ楕円曲線暗号を適用するためには，数学的に安全であるだけでなく高い速度性能が得られるようなドメインパラメータを選択することが重要な要件となる．素体 $\mathbb{F}_p$ 上楕円曲線においては，定義体標数 p として特別な型，例えば一般化 Mersenne 素数を選ぶと p による剰余算を高速に行える [13]．National Institute of Standards and Technology (NIST) が推奨する 5 つの素体上楕円曲線は，一般化 Mersenne 素数を定義体標数としている [6]．

一方，RSA 暗号実装では，法乗算に Montgomery 乗算法 [22] がよく用いられる．Montgomery 乗算は，法乗算への入力に依存した処理分岐が生じることから，タイミング攻撃が可能になることが知られている [19, 14, 23]．楕円曲線暗号においては，法 p を特殊な型にとって剰余算を高速化できることから，Montgomery 乗算ではなく，一般化 Mersenne 素数のような特殊な素数による専用剰余算アルゴリズムを用いることが多いと思われる．一般化 Mersenne 素数による剰余算の典型的な実装でも，後述するように Montgomery 乗算と同様に入力値に依存した処理分岐が生じる．

単純なバイナリ法のように，楕円点倍算において点加算と点 2 倍算とが秘密べき指数のビット値に依存して計算される時，単純電力解析 (Simple Power Analysis, SPA) によって秘密べき指数を導出することができる．SPA 対策の 1 つとして，異なる 2 点の加算と点 2 倍算とを同じ計算式で実行するというアプローチがある [15, 17, 18, 20]．これらの計算式は “unified code” と呼ばれる．Brier らは，Weierstrass 型楕円曲線 affine 座標系および射影座標系 $((x, y) = (X/Z, Y/Z))$ において，入力の 2 点が異なる場合でも同じ場合でも，同じ手順で動作する点加算アルゴリズムを示した [15]．

しかし Walter は，Montgomery 乗算を用いて Brier らの unified code を実装した場合，左バイナリ法による楕円点倍算は SPA に対して脆弱であることを示した [26]．この結果は Montgomery 乗算を用いた $\mathbb{F}_p$ 乗算であり，前述のように実際の情報セキュリティシステムで稼動している楕円曲線暗号は，p を一般化 Mersenne 素数など高速処理向きな楕円曲線ドメインパラメータによる専用の高速アルゴリズムが実装されていることが多いと思われる．

本稿では，より一般的な楕円曲線暗号実装である一般化 Mersenne 素数など高速処理向けな定義体標数を用いた剰余算実装に対する SPA を考察する．NIST 推奨曲線 [6] のような一般化 Mersenne 素数を用いた高速剰余算実装に対しても，unified code のように，楕円点加算と 2 倍算とを同じ処理手順で実装するだけでは SPA に対して安全ではないことを示す．特に NIST 推奨の素体上楕円曲線について，剰余算実装の SPA に対する脆弱性を考察する．5 つある推奨曲線のうち，192 ビットの曲線に用いられている素数 $p = 2^{192} - 2^{64} - 1$ による剰余算実装は，SPA に対してより脆弱になりやすいことを示す．

1.2 高速剰余算

RSA 暗号や (素体上) 楕円曲線暗号では，暗号や署名の演算は法演算の繰り返しである．除算命令は一般に演算時間がかかるため，除算命令無しで実装できる剰余算アルゴリズムを用いることが望ましい．Montgomery 乗算 [22] は，任意の法 n に対して除算命令を必要としないため，RSA 暗号ではよく用いられる．

一方，素体 $\mathbb{F}_p$ 上楕円曲線暗号では，p を法とする剰余算が行われる．p は公開パラメータであり，ランダムに選択する必要は無い．したがって，高速に演算可能な都合の良い p が選ばれる場合が多い[1]．

本章では，一般化 Mersenne 素数など，特別な型の素数を法とする高速剰余算アルゴリズムの概要を記述する．

[1] RSA 暗号では，法 n はプライベート鍵であるランダムに生成された 2 つの素数 p, q の積であるため，高速演算に都合の良い n を選ぶことはできない．

一般化 Mersenne 素数

NIST による素体上推奨曲線 [6] は，一般化 Mersenne 素数と呼ばれる次のような素数 p をドメインパラメータとしている．

P-192: $p_{192} = 2^{192} - 2^{64} - 1$
P-224: $p_{224} = 2^{224} - 2^{96} + 1$
P-256: $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
P-384: $p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$
P-521: $p_{521} = 2^{521} - 1$

p_{192}，p_{224}，p_{256}，p_{384}，p_{521} を法とする剰余算をそれぞれアルゴリズム 1.1，1.2，1.3，1.4，1.5 に示す [6, 16, 13].

Algorithm 1.1 Fast reduction modulo $p_{192} = 2^{192} - 2^{64} - 1$

Input integer $c = (c_5, c_4, c_3, c_2, c_1, c_0)$, where each c_i is a 64-bit word, and $0 \le c < p_{192}^2$.

Output $c \bmod p_{192}$.

1. Define 192-bit integers:
   $s_0 = (c_2, c_1, c_0)$
   $s_1 = (0, c_3, c_3)$
   $s_2 = (c_4, c_4, 0)$
   $s_3 = (c_5, c_5, c_5)$
2. Return $s_0 + s_1 + s_2 + s_3 \bmod p_{192}$

Algorithm 1.2 Fast reduction modulo $p_{224} = 2^{224} - 2^{96} + 1$

Input integer $c = (c_{13}, \ldots, c_1, c_0)$, where each c_i is a 32-bit word, and $0 \le c < p_{224}^2$.

Output $c \bmod p_{224}$.

1. Define 224-bit integers:
   $s_0 = (c_6, c_5, c_4, c_3, c_2, c_1, c_0)$
   $s_1 = (c_{10}, c_9, c_8, c_7, 0, 0, 0)$
   $s_2 = (0, c_{13}, c_{12}, c_{11}, 0, 0, 0)$
   $s_3 = (c_{13}, c_{12}, c_{11}, c_{10}, c_9, c_8, c_7)$
   $s_4 = (0, 0, 0, 0, c_{13}, c_{12}, c_{11})$
2. Return $s_0 + s_1 + s_2 - s_3 - s_4 \bmod p_{224}$

Algorithm 1.3 Fast reduction modulo $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$

Input integer $c = (c_{15}, \ldots, c_1, c_0)$, where each c_i is a 32-bit word, and $0 \le c < p_{256}^2$.

Output $c \bmod p_{256}$.

1. Define 256-bit integers:
   $s_0 = (c_7, c_6, c_5, c_4, c_3, c_2, c_1, c_0)$
   $s_1 = (c_{15}, c_{14}, c_{13}, c_{12}, c_{11}, 0, 0, 0)$
   $s_2 = (0, c_{15}, c_{14}, c_{13}, c_{12}, 0, 0, 0)$
   $s_3 = (c_{15}, c_{14}, 0, 0, 0, c_{10}, c_9, c_8)$
   $s_4 = (c_8, c_{13}, c_{15}, c_{14}, c_{13}, c_{11}, c_{10}, c_9)$
   $s_5 = (c_{10}, c_8, 0, 0, 0, c_{13}, c_{12}, c_{11})$
   $s_6 = (c_{11}, c_9, 0, 0, c_{15}, c_{14}, c_{13}, c_{12})$
   $s_7 = (c_{12}, 0, c_{10}, c_9, c_8, c_{15}, c_{14}, c_{13})$
   $s_8 = (c_{13}, 0, c_{11}, c_{10}, c_9, 0, c_{15}, c_{14})$
2. Return $s_0 + 2s_1 + 2s_2 + s_3 + s_4 - s_5 - s_6 - s_7 - s_8 \bmod p_{256}$

Algorithm 1.4 Fast reduction modulo $p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$

Input integer $c = (c_{23}, \ldots, c_1, c_0)$, where each c_i is a 32-bit word, and $0 \le c < p_{384}^2$.

Output $c \bmod p_{384}$.

1. Define 384-bit integers:
   $s_0 = (c_{11}, c_{10}, c_9, c_8, c_7, c_6, c_5, c_4, c_3, c_2, c_1, c_0)$
   $s_1 = (0, 0, 0, 0, 0, c_{23}, c_{22}, c_{21}, 0, 0, 0, 0)$
   $s_2 = (c_{23}, c_{22}, c_{21}, c_{20}, c_{19}, c_{18}, c_{17}, c_{16}, c_{15}, c_{14}, c_{13}, c_{12})$
   $s_3 = (c_{20}, c_{19}, c_{18}, c_{17}, c_{16}, c_{15}, c_{14}, c_{13}, c_{12}, c_{23}, c_{22}, c_{21})$
   $s_4 = (c_{19}, c_{18}, c_{17}, c_{16}, c_{15}, c_{14}, c_{13}, c_{12}, c_{20}, 0, c_{23}, 0)$
   $s_5 = (0, 0, 0, 0, c_{23}, c_{22}, c_{21}, c_{20}, 0, 0, 0, 0)$
   $s_6 = (0, 0, 0, 0, 0, 0, c_{23}, c_{22}, c_{21}, 0, 0, c_{20})$
   $s_7 = (c_{22}, c_{21}, c_{20}, c_{19}, c_{18}, c_{17}, c_{16}, c_{15}, c_{14}, c_{13}, c_{12}, c_{23})$
   $s_8 = (0, 0, 0, 0, 0, 0, 0, c_{23}, c_{22}, c_{21}, c_{20}, 0)$
   $s_9 = (0, 0, 0, 0, 0, 0, 0, c_{23}, c_{23}, 0, 0, 0)$
2. Return $s_0 + 2s_1 + s_2 + s_3 + s_4 + s_5 + s_6 - s_7 - s_8 - s_9 \bmod p_{384}$

Algorithm 1.5 Fast reduction modulo $p_{521} = 2^{521} - 1$

Input integer $c = (c_{1041}, \ldots, c_1, c_0)$, where $c_i \in \{0, 1\}$, and $0 \le c < p_{521}^2$.

Output $c \bmod p_{521}$.

1. Define 521-bit integers:
   $s_0 = (c_{1041}, \ldots, c_{522}, c_{521})$
   $s_1 = (c_{520}, \ldots, c_1, c_0)$
2. Return $s_0 + s_1 \bmod p_{521}$

Extra Reduction

アルゴリズム 1.1~1.5は，各アルゴリズムのステップ 2において入力に依存した条件付処理が生じる．例えば，p_{192} による剰余算アルゴリズム 1.1のステップ 2の典型的実装は次のようになる．

2.1. $t \leftarrow s_0 + s_1 + s_2 + s_3$

2.2. `While` $t \geq p_{192}$ `do:`

2.3. $t \leftarrow t - p_{192}$ (extra reduction)

2.4. `end of while`

2.5. `Return` t

アルゴリズム 1.1の出力が p_{192} 未満であることを保証するために，ステップ 2.1において s_0，s_1，s_2，s_3 を加算した結果 t が p_{192} 以上である場合，ステップ 2.3において必要な回数 t から p_{192} を引く．この条件付引き算を “extra reduction” と呼ぶこととする．extra reduction が生じるかどうかは，剰余算への入力，すなわち法乗算への入力に依存して決まる．

入力に依存して生じる extra reduction に起因するサイドチャネル情報を利用した暗号解析法を第 1.4章に示す．

その他の高速剰余算

Standards for Efficient Cryptography Group (SECG) が推奨している楕円曲線ドメインパラメータにも，素体 $\mathbb{F}_p$ 上楕円曲線の定義体標数 p として高速処理向けな型が選ばれている [24]．これらの素数には，NIST 推奨曲線のような一般化 Mersenne 素数や，$p = 2^t - c$ (c は小さい整数) という型の素数などが含まれている．

$p = 2^t - c$ 型素数に関しても，高速な剰余算アルゴリズムが知られている [21]．この剰余算アルゴリズムも，典型的な実装では，入力に依存した条件付処理，extra reduction，が生じる．したがって，第 1.4章に示すサイドチャネル解析法は，$p = 2^t - c$ 型素数のための剰余算実装に対しても適用可能となる．

1.3 Unified Code

Weierstrass 型楕円曲線上の異なる 2 点の加算および点 2 倍算を，同じ演算手順で行える方法 “unified code” を Brier と Joye が提案した [15]．素体 $\mathbb{F}_p$ 上射影座標系，$(x, y) = (X/Z, Y/Z)$，におけるアルゴリズムを次に示す．

Algorithm 1.6 Unified point addition/doubling formula

`Input` $P_0 = (X_0, Y_0, Z_0), P_1 = (X_1, Y_1, Z_1) \in E(\mathbb{F}_p)$
`Output` $P_2 = P_0 + P_1 = (X_2, Y_2, Z_2) \in E(\mathbb{F}_p)$

1. $u_1 \leftarrow X_0 Z_1$, $u_2 \leftarrow X_1 Z_0$, $t \leftarrow u_1 + u_2$
2. $s_1 \leftarrow Y_0 Z_1$, $s_2 \leftarrow Y_1 Z_0$, $m \leftarrow s_1 + s_2$
3. $z \leftarrow Z_0 Z_2$, $f \leftarrow zm$, $l \leftarrow mf$, $g \leftarrow tl$
4. $r \leftarrow t^2 - u_1 u_2 + az^2$, $w \leftarrow r^2 - g$
5. $X_2 \leftarrow 2fw$
6. $Y_2 \leftarrow r(g - 2w) - l^2$
7. $Z_2 \leftarrow 2f^3$
8. `Return` $P_2 = (X_2, Y_2, Z_2)$

Unified code は，異なる 2 点の加算と点 2 倍算とを同じ手順で行うことにより，SPA に対する防御をねらったものである．しかし，第 1.4章で述べるように，$\mathbb{F}_p$ 上乗算を Montgomery 乗算 [22] で実装した場合，SPA に対して脆弱になることを Walter が示した [26]．

1.4 サイドチャネル解析

本章では，前章までに述べた一般化 Mersenne 素数による剰余算 (アルゴリズム 1.1~1.5) および unified code (アルゴリズム 1.6) を用いた実装に対するサイドチャネル解析を行う．楕円点倍算としてアルゴリズム 1.7に示す左バイナリ法を用いる場合を考察する．

Algorithm 1.7 Left-to-right binary method of elliptic point multiplication

`Input` $G \in E(\mathbb{F}_p)$ and k, where $k = (k_{t-1} k_{t-2} \cdots k_0)$, $k_i \in \{0, 1\}$ for $0 \leq i \leq t-2$, and $k_{t-1} = 1$
`Output` $R = kG$

1. $R \leftarrow G$
2. `For` i `from` $t-2$ `down to` 0 `do:`
3. $\quad R \leftarrow 2R$
4. $\quad$ `If` $k_i = 1$ `then`
5. $\quad\quad R \leftarrow R + G$
6. $\quad$ `end if`
7. `end for`
8. `Return` R

Extra Reduction の確率

まず，Extra reduction が生じる確率を実験的に評価する．評価において次を仮定する．

- 法乗算 $c \leftarrow a \times b \bmod p$ への 2 つの入力 a, b は一様であると仮定する．
- まず $a \times b$ を計算し，次にアルゴリズム 1.1∼1.5 により剰余算を行う．
- アルゴリズム 1.1∼1.5 ステップ 2は，第 1.2 節に記述した手順で計算する．すなわち，まず全ての s_i について加減算を行い，その結果が p 以上の場合は，p 未満になるまで p を引く．

$c \leftarrow a \times b \bmod p$ の計算において，extra reduction が生じる確率は次の 3 つの場合で異なる．

- 法乗算への 2 つの入力 a，b が異なる場合
- $a = b$ の場合
- a と b の一方が定数の場合

一方が定数の場合，extra reduction の確率はその定数の値に依存する．

注意 1.1 楕円点倍算を左バイナリ法で行う場合は，点加算において常に決まった点 G を加算することになる *(アルゴリズム 1.7ステップ 5)*．したがって，*unified code* の最初の *2* つのステップは，異なる *2* 点の加算の場合，法乗算は定数 *(*ベースポイントの x，y または $z(=1)$ 座標*)* との乗算である．

ランダム入力の場合

表 1に法乗算への 2 つの入力整数が異なる場合，および 2 つの入力整数が同じ場合の extra reduction の確率を示す．ランダムに 100,000 個の整数ペア a, b $(0 \leq a, b < p)$ を生成し，extra reduction が生じるかどうかを実験的に調べた．擬似乱数生成関数には，FIPS 186-2[6] に記載されている SHA-1 ベースのアルゴリズムを用いた．

P-192 と P-384 は他の曲線と比較して extra reduction が生じる確率が大きい．アルゴリズム 1.1∼1.5 のステップ 2からわかるように，P-192 の s_i は全て加算されるの対し，P-224, P-256, P-521 は加算される s_i が少ないことが原因である．また，P-384 も相対的に加算される s_i が多い．P-256 は，減算される s_i が多いため，extra reduction の確率が特に小さい．

表 1: Probability of extra reduction with random inputs, where p is a recommended domain parameter.

Curve	$a \times b \bmod p$, $(a \neq b)$	$a \times a \bmod p$
P-192	0.69	0.73
P-224	0.30	0.27
P-256	0.11	0.20
P-384	0.65	0.69
P-521	0.25	0.33

ベースポイントの場合

表 2に法乗算への 2 つの入力整数のうち一方が NIST 推奨曲線のベースポイント x 座標または y 座標の場合の extra reduction の確率を示す．前節と同様，ランダムに生成した 100,000 個の整数 a $(0 \leq a < p)$ に対して平均をとった．

各曲線のベースポイントの x，y 座標値の上位桁のみを 16 進表記で次に示す．

P-192:

x_{192} =188da80eb03090f67cbf20eb43a18800f4f
...

y_{192} =07192b95ffc8da78631011ed6b24cdd573f
...

表 2: Probability of extra reduction with fixed base point $G = (x_G, y_G, 1)$, where p and G are recommended domain parameters.

Curve	$a \times x_G \bmod p$	$a \times y_G \bmod p$
P-192	0.54	0.51
P-224	0.22	0.22
P-256	0.04	0.02
P-384	0.70	0.57
P-521	0.19	0.28

P-224:

x_{224}: b70e0cbd6bb4bf7f321390b94a03c1d356c
...

y_{224}: bd376388b5f723fb4c22dfe6cd4375a05a0
...

P-256:

x_{256}: 6b17d1f2e12c4247f8bce6e563a440f2770
...

y_{256}: 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bc
...

P-384:

x_{384}: aa87ca22be8b05378eb1c71ef320ad746e1
...

y_{384}: 3617de4a96262c6f5d9e98bf9292dc29f8f
...

P-521:

x_{521}: 0c6858e06b70404e9cd9e3ecb662395b442
...

y_{521}: 11839296a789a3bc0045c8a5fb42c7d1bd9
...

表 2からわかるように，P-192 はランダムな入力の場合 (表 1) よりも extra reduction の確率が小さい．ベースポイントの x 座標値，y 座標値ともに，上位桁の値が小さい (それぞれ 1 と 0) ことに起因する．

一方，P-224 は，ベースポイントの x 座標値の最上位桁と y 座標値の最上位桁は共に b であるが，extra reduction の確率は小さい．アルゴリズム 1.2を見ると，剰余をとる整数 c の最上位ワード c_{13} は，和をとる s_0，s_1，s_2 の最上位ワードには含まれず，減じる s_3 の最上位ワードとなっている．したがって，c_{13} が大きいほど，すなわち法乗算への入力整数が大きいほど，extra reduction の確率は小さくなる．P-256，P-384，P-521 についても同様の現象を見ることができる．

なお，後述するように，ベースポイント座標値による法乗算において，extra reduction が生じる確率が大きいほど，SPA に対して脆弱となる．

攻撃法

Walter は条件付処理を持つ Montgomery 乗算実装に対する攻撃法を示した [26]．本節では，NIST 推奨素数による剰余算実装に対して同様の攻撃法を適用する．

楕円点倍算の実装に次の方法を用いる場合を考察する．

- **一般化 Mersenne 素数 p による剰余算:** 専用の高速アルゴリズム (アルゴリズム 1.1∼1.5 および第 1.2節に記載の手順)
- **楕円点加算および点 2 倍算:** unified code(アルゴリズム 1.6)
- **楕円点倍算:** 左バイナリ法 (アルゴリズム 1.7)

また，攻撃者は次の能力を持つと仮定する．

- 実装されているアルゴリズムが前述のものであると知っている．
- 剰余算において extra reduction の有無を検出できる．

Unified code の実装 (アルゴリズム 1.6) は，入力の 2 点 P_0 および P_1 が同じ点 ($X_0 = X_1$，$Y_0 = Y_1$，$Z_0 = Z_1$) である場合，ステップ 1における u_1 の計算と u_2 の計算は同じ計算となる．s_1，s_2 の計算 (ステップ 2) も同様である．したがって，u_1 と u_2 の計算のいずれか一方だけ，または s_1 と s_2 の計算のいずれか一方だけに extra reduction が生じた場合，点加算は同じ点に対するものとはなり得ず，必ず異なる 2 点に対するものだったことになる．このような場合，対応する秘密べき指数のビットは”1” と推定できる．

表 3: An Attack on P-192

k	1001 01 1 001 001 001 01 1 01 1 01 1 1 1 1 0001 01 1 01 001 01 01 001 0 ...
$\mathcal{AD}$	DDDADDADADDDADDDADDDADDADADDADADDADADADADADADDDDADDADADDADDDDADDADDADDDDAD ...
u_1	-*-----*-*-*-*-*-**--**-*-**---**-*-*-----****--*---**-***-*--**-***-* ...
u_2	-*----**-*-***-*-**--****-**--*****-*-----****--*--*********-********* ...
s_1	-**----*-**--***-**--*--*--*-*-**-*---*---***--*--*-**--*-----*--***-* ...
s_2	-**---*****-*******--*--*--********---*--****-**--*-**--*-*--**-****-* ...
Difference	------Y-Y---Y---Y------Y----Y-Y--Y-------Y----Y----Y--Y---Y--Y--Y---Y- ...
Recovered $\mathcal{AD}$	-----YYYYY-YYY-YYY----YYY--YYYYYYYY-----YYY--YYY--YYYYYY-YYYYYYYYY-YYY ...

攻撃例

楕円曲線 P-192 に対する攻撃例を表 3に示す. 表 3において，k は秘密べき指数の 2 進数表記である．ランダムに生成した 192 ビットの k のビットのうち，スペースの都合上，上位側のビットのみを示した．‘$\mathcal{AD}$’ は，左バイナリ法による楕円点倍算 (アルゴリズム 1.7) において，異なる 2 点の加算 $\mathcal{A}$ と同じ点の加算 (2 倍算)$\mathcal{D}$ のシーケンスを示す．シンボル ‘$*$’ は，u_1，u_2，s_1，s_2 の計算 (アルゴリズム 1.6) において，剰余算 (アルゴリズム 1.1) の際に extra reduction が生じたことを示す．シンボル ‘-’ は，extra reduction が生じなかったことを示す.

‘Difference’ の行には，u_1 と u_2 の一方だけに extra reduction が生じた場合，または s_1 と s_2 の一方だけに extra reduction が生じた場合にシンボル ‘Y’ を記述した．すなわち，‘Y’ の箇所では，unified code による点加算は，同じ点ではなく，異なる 2 点で行われたことになる．‘Recovered $\mathcal{AD}$’ は，サイドチャネル情報から推定できる $\mathcal{AD}$ のシーケンスを示している．推定可能な箇所にシンボル ‘Y’ を記述した．バイナリ法では，$\mathcal{A}$ の前後は必ず $\mathcal{D}$ であることに注意.

注意 1.2 この攻撃シミュレーションでは，*unified code* において，点 P_1 をアルゴリズム *1.7*における点 G とした．加算する固定点 G は署名生成などではベースポイントであり，通常は常に $Z_1 = 1$ である．したがって u_1 および s_1 の計算時に *extra reduction* は生じない.

防御法

Extra reduction の有無に起因する消費電力の違い，処理時間差などを観測できなくすることが本稿で述べた攻撃法に対する防御となる.

また，剰余算のアルゴリズムを考慮して，ベースポイントの座標値を適切に選択すれば，extra reduction の確率を減らすことができる.

1.5 まとめ

素体 $\mathbb{F}_p$ 上楕円曲線暗号実装において，剰余算に関するサイドチャネル情報漏洩を考察した．定義体標数 p には，通常，NIST 推奨曲線のように一般化 Mersenne 素数など高速に法乗算が行える素数が選ばれる．その素数専用の高速剰余算の典型的実装では，Montgomery 乗算の場合のように，入力に依存した extra reduction が生じる．Extra reduction の有無は，サイドチャネル攻撃の原因となり得る．Brier らの unified code は，異なる 2 点の加算と同じ点どうしの加算 (2 倍算) を，有限体演算レベルで同じ手順で行えるものであった．しかし，Montgomery 乗算における extra reduction の有無を攻撃者が検出できる場合，unified code のアプローチは SPA に対して脆弱となることが Walter によって指摘されていた [26]．本稿では，多くの楕円曲線暗号で用いられる一般化 Mersenne 素数による剰余算実装に対しても SPA が可能となることを示した．また，NIST による素体上推奨曲線のうち，192 ビットの曲線に用いられている素数による剰余算実装は，SPA に対して脆弱になりやすいことを示した.

2 中間変数を利用した電力解析法

2.1 はじめに

楕円曲線暗号は，IEEE，ANSI，ISO，CRYPTREC など様々な機関において推奨暗号アルゴ

リズムとして採用され，現在様々な情報セキュリティシステムで実用化が進んでいる．一方，暗号が実装されたデバイスから得ることができるサイドチャネル情報を利用して秘密情報得る解析法，すなわちサイドチャネル解析が，特にスマートカードなどの携帯機器で現実的脅威となっている．楕円曲線暗号は，RSA 暗号と比べて鍵長を小さくできることから，携帯機器上でより利点を発揮する．したがって，楕円曲線暗号をサイドチャネル解析に対して安全に実装することは重要な課題である．

楕円曲線暗号では楕円点倍算 $Q \leftarrow kP$ (k は整数，P と Q は楕円曲線上の点) と呼ばれる計算を行う．楕円点倍算は，楕円曲線暗号において計算時間が支配的な演算であり，様々な計算法が研究されている．また，署名生成や復号においては，整数 k は秘密情報であるため，サイドチャネル情報から k を導き出すことが楕円曲線暗号に対するサイドチャネル解析の目的となる．

楕円点倍算に対するサイドチャネル解析の方法および対策法はすでに数多く提案されている．単純電力解析 (SPA) に対しては，Double-and-Add always 法など，暗号処理手順を秘密鍵に依存させずに一定にする対策法があり [3, 12]，差分電力解析 (DPA) に対しては，べき指数のランダム化や入力点のランダム化 (ランダム化射影座標)[3] などの対策法がある．

DPA 対策として何らかの方法でランダム化を取り入れることは一般的である．しかし，ランダム化にも関わらず，暗号演算中の中間変数が乱数の影響を受けないある不変な性質を持つことがあり，この不変な性質を利用してサイドチャネル解析が可能となることが Goubin により指摘された [7]．例えば，点の座標値が 0 ならば，ランダム化しても 0 であり続ける．このような特殊な性質を持つ点を利用して行う電力解析を改良電力解析 (Refined Power Analysis, RPA) と呼ぶ [7]．また，RPA の拡張であるゼロ値解析 (Zero-Value Register Attack, ZRA) と呼ばれる手法も開発された [1]．

さらに，値が 0 ということの他，点の座標値のハミング重みに関する相関を不変な性質として扱う解析法も提案されている [4]．National Institute of Standards and Technology (NIST)，ANSI, Standards for Efficient Cryptography Group (SECG)，などが推奨する楕円曲線では，素体 $\mathbb{F}_p$ 上楕円曲線の定義体標数 p として一般化メルセンヌ素数を用いるなど，高速演算可能なドメインパラメータが選ばれている．[4] では，このような定義体標数を持つ楕円曲線において射影座標系 $(x, y) \leftarrow (X/Z, Y/Z)$ 表現を用いた場合，アファイン座標に変換した時に点 $(2^\lambda, y)$，λ は小さい非負整数，という形になる点 (X, Y, Z) は，X 座標値と Z 座標値とのハミング距離が近くなることが示された．

本稿では，このような，楕円点倍算中に現れる不変な性質を持つ中間変数の存在についてさらに考察する．素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線を，Jacobian 座標系 $(x, y) \leftarrow (X/Z^2, Y/Z^3)$，Double-and-Add always 法，ランダム化射影座標法，を用いて実装する場合を検討する．この場合，楕円点倍算の途中で $(2^\lambda, y)$，$(2^\lambda + 1, y)$，$(x, 2^\lambda)$ という形の点になるような点を楕円点倍算への入力として与えると，点 2 倍算においてハミング重みに強い相関を持つ中間変数の組が出現することを示す．

2.2 推奨楕円曲線

楕円曲線ドメインパラメータは，楕円離散対数問題が困難になるように選ばなければならない．しかし，実際の情報セキュリティシステムへ楕円曲線暗号を適用する際は，安全であるだけでなく，高い速度性能が得られるようなドメインパラメータを選択することも重要な要件となる．素体 $\mathbb{F}_p$ 上楕円曲線においては，定義体標数 p として特別な型，例えば一般化 Mersenne 素数を選ぶと p による剰余算を高速に行うことができる [13]．NIST が推奨する 5 つの素体 $\mathbb{F}_p$ 上楕円曲線は，一般化 Mersenne 素数と呼ばれる次の 5 つの素数を定義体標数としている [6]．

曲線 P-192: $p_{192} = 2^{192} - 2^{64} - 1$

曲線 P-224: $p_{224} = 2^{224} - 2^{96} + 1$

曲線 P-256: $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$

曲線 P-384: $p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$

曲線 P-521: $p_{521} = 2^{521} - 1$

例えば p_{192} による剰余算は，$2^{192} \equiv 2^{64} + 1 \bmod p_{192}$ であることを利用すると，Algorithm 2.1 のように除算無しで高速に行える．

さらに，例えば $2 \times a \bmod p_{192}$ を計算する場合は，Algorithm 2.1において $c_3 = 1$ (シフトによるキャリーがあった場合)，$c_4 = 0$，$c_5 = 0$ となるので，a の最下位ビット (0 番目のビット) と 64 番目のビットにそれぞれ 1 を加算するだけの簡単な処理となる．

Algorithm 2.1 Fast reduction modulo $p_{192} = 2^{192} - 2^{64} - 1$

Input an integer $c = (c_5, c_4, c_3, c_2, c_1, c_0)$, where each c_i is a 64-bit word, and $0 \leq c < p_{192}^2$.

Output $c \bmod p_{192}$.

1. Define 192-bit integers:
   $s_0 = (c_2,\ c_1,\ c_0)$
   $s_1 = (\ 0,\ c_3,\ c_3)$
   $s_2 = (c_4,\ c_4,\ 0\ )$
   $s_3 = (c_5,\ c_5,\ c_5)$
2. return $s_0 + s_1 + s_2 + s_3 \bmod p_{192}$

2.3 楕円点倍算に対する電力解析

ディジタル署名生成や，復号，鍵共有などで実行される楕円点倍算は，ユーザプライベート鍵などの秘密情報を用いる．したがって，楕円点倍算はサイドチャネル解析の対象となり，電力解析に関しても様々な解析法や対策法が提案されている．

単純電力解析 (SPA): SPA は，演算手順が秘密べき指数の値に依存している時可能となる．例えば，Algorithm 2.2に示す左バイナリ法は，秘密べき指数 k のビットが 1 の時のみ点加算を実行する．したがって，点加算と点 2 倍算のシーケンスが電力解析により識別できれば，k を導出可能となる．

SPA 対策には，Algorithm 2.3に示した Double-and-Add always 法や Montgomery ladder など，加算鎖を秘密べき指数に依存させずに一定にする方法がある [3, 11, 12],

差分電力解析 (DPA): DPA では，解析者は複数の入力に対して消費電力を測定し，秘密情報の推測を行う．秘密情報の推測値が正しいかどうかを，測定した消費電力を用いて判定する [9]．DPA が可能となるためには，暗号演算中のある中間値が，暗号演算への既知の入力と，秘密情報 (の一部) に依存して決まる必要がある．したがって，DPA 対策としては，乱数を用いて何らかのランダム化を行い，暗号演算中の中間値が，既知の入力と秘密情報 (の一部) とから一意に決まらないようにすることが一般的である．楕円点倍算の DPA 対策には，入力点のランダム化 (ランダム化射影座標) やべき指数のランダム化などがある [3].

ランダム化射影座標法は，射影座標系 $(x, y) \leftarrow (X/Z, Y/Z)$ において，$\theta \in \mathbb{F}_p^\times$ に対して点 $(X : Y : Z)$ と点 $(\theta X : \theta Y : \theta Z)$ が等価であることを利用する．まずランダムに $\theta \in \mathbb{F}_p^\times$ を生成し，入力点 (x, y) を射影座標表現 $(\theta x, \theta y, \theta)$ に変換してから楕円点倍算を実行する．楕円点倍算処理中の中間値は，入力点と秘密情報とだけからでは決まらない乱数の影響を受けているため，DPA 対策となる．

改良電力解析 (RPA)，ゼロ値解析 (ZRA): DPA 対策としてランダム化射影座標を用いた場合でも，使用された乱数に影響されない不変な性質を持つ中間変数が存在し得ることが指摘された [7]．例えば，ある座標値が 0 であった場合，ランダム化しても 0 であり続ける．RPA[7] とその拡張である ZRA[1] は，不変な中間変数の性質として，点の座標値が 0 であることや，点 2 倍算や点加算中の中間値が 0 であることを利用する．これら不変な性質を持つ中間変数が存在し，電力解析などにより解析者がその中間変数の出現を認識できると，秘密べき指数の導出が可能となる．解析法の詳細は次章で述べる．

RPA や ZRA に対する対策には，ランダム化初期点を用いる方法がある [27, 10].

Algorithm 2.2 Left-to-right binary method

Input a point P, an integer k, where $k = (k_{t-1}k_{t-2}\cdots k_0)_2$

Output kP

1. $R \leftarrow \mathcal{O}$

2. for i from $t-1$ down to 0
3. $R \leftarrow 2R$
4. If $k_i = 1$ then
5. $R \leftarrow R + P$
6. end if
7. end for
8. return R

Algorithm 2.3 Double-and-Add always method

Input a point P, an integer k, where $k = (k_{t-1}k_{t-2}\cdots k_0)_2$
Output kP

1. $R[0] = \mathcal{O}$
2. for i from $t-1$ down to 0
3. $R[0] \leftarrow 2R[0]$
4. $R[1] \leftarrow R[0] + P$
5. $R[0] \leftarrow R[k_i]$
6. end for
7. return $R[0]$

2.4 特殊な性質を持つ中間変数を利用した電力解析法

本章では，楕円点倍算において，入力点のランダム化に対して不変な性質を持つ中間変数を利用した電力解析法を述べる．$p > 3$ を素数とし，$a, b \in \mathbb{F}_p$，$4a^3 + 27b^2 \neq 0$ とする．次に示す素体 $\mathbb{F}_p$ 上楕円曲線 E を対象とする．

$$E : y^2 = x^3 + ax + b \tag{2.1}$$

素体 $\mathbb{F}_p$ 上楕円曲線として NIST が推奨する曲線，Jacobian 座標，を用いた場合において，ランダム化に依存しない特殊な性質を持つ中間が存在することを示す．

解析法の一般的枠組み

楕円点倍算中に現れるある特殊な性質を持つ点 P_0 の出現を認識できると仮定する．この認識は，例えば電力解析などによってランダムな点と識別することにより行う．特殊な性質を持つ点を認識することを利用した解析法が Goubin によって提案され [7]，その後いくつかの拡張が行われている [1, 4]．これら，特殊な性質を持つ点を利用した解析法の一般的枠組みを以下に記述する．

楕円点倍算 Algorithm 2.3 への入力を P，$k = (k_{t-1}k_{t-2}\ldots k_0)_2$ とする．$K_j = \sum_{i=t-1-j}^{t-1} k_i 2^{i-(t-1-j)}$ とすると，j 番目のループ終了時には，次の点 K_jP が計算されているはずである．

$$K_jP = \sum_{i=t-1-j}^{t-1} k_i 2^{i-(t-1-j)} P$$

したがって，n をベースポイントの位数とすると，点 $(K_j^{-1} \bmod n)P_0$ を入力点とすれば，j 番目のループ終了時に点 P_0 が現れる．

よって，k の上位ビット $K_{j-1} = (k_{t-1}\ldots k_{t-j})$ が既知であると仮定すると，次のビット k_{t-1-j} は次のようにして推測することができる．

- $k_{t-1-j} = 0$ つまり $K_j = 2K_{j-1}$ と仮定する．点 $(K_j^{-1} \bmod n)P_0$ を入力点として与えた時，もし点 P_0 が認識できれば，$k_{t-1-j} = 0$ という仮定は正しいと判断する．
- もし認識できなければ，$k_{t-1-j} = 1$ つまり $K_j = 2K_{j-1} + 1$ と判断する．

以上の操作を k の上位ビットから繰り返せば，秘密べき指数 k の全ビットを推測することができる．

ハミング重みに関する相関

素体 $\mathbb{F}_p$ 上の NIST 推奨楕円曲線において，Dupuy らはアファイン座標系で表現した場合に，

$$P_0 = (2^\lambda, y),\ \lambda \text{は小さい非負整数}$$

となる点を，特殊な点 P_0 として考察した [4] [2]．

[2] 文献 [4] では，標数 2 拡大体 $\mathbb{F}_{2^m}$ 上楕円曲線についても議論されている．$\mathbb{F}_{2^m}$ 上の場合は，特殊な点として，点 $P_0 = (x^\lambda, y)$ が考察されている．

射影座標系 $(x, y) \leftarrow (X/Z, Y/Z)$ を用いると，ランダムな $\theta \in \mathbb{F}_p^\times$ に対して，λ が小さな非負整数の場合，$X = 2^\lambda\theta$ と $Z = \theta$ とのハミング距離は小さくなる可能性が高い．ハミング距離が小さくなるのは，NIST 推奨の素体 $\mathbb{F}_p$ 上楕円曲線が (SECG など他の機関の推奨楕円曲線も)，定義体標数 p として *sparse* な素数を用いていることが大きく影響している．

例えば $\lambda = 1$ の場合，第 2.2章で述べたように，$2\theta \bmod p_{192}$ の計算は，θ を 1 ビット左シフトした時にキャリーが生じた場合に限り，θ の 0 番目のビットと 64 番目のビットに 1 を加算することにより行われる．よって，$X = 2\theta$ と $Z = \theta$ のハミング距離は小さいと期待できる．ハミング距離の詳細な評価は文献 [4] を参照のこと．

本稿における以下の議論では，上記 P_0 は認識可能な特殊な性質を持つと仮定する．楕円点倍算の途中で P_0 が現れるような入力点を与えると，2.4 節で述べた手法により秘密べき指数を導出することができる．

解析対象の実装

本稿で解析対象とするデバイスの実装は，次の特徴を持つと仮定する．

- 素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線を用いる．すなわち，定義体標数 p は sparse な素数である．
- 楕円点倍算中，点は Jacobian 座標 $(x, y) \leftarrow (X/Z^2, Y/Z^3)$ で表現する．
- 入力点はランダム化する．すなわち入力点 (x, y) は，ランダムに生成された $\theta \in \mathbb{F}_p^\times$ を用いて，$(\theta^2 x, \theta^3 y, \theta)$ と変換する．
- 加算鎖のランダム化等，計算手順のランダム化は行わない．
- 楕円点倍算には Double-and-Add always 法 (Algorithm 2.3) を用いる．
- 楕円点 2 倍算は，Algorithm 2.4に示す計算手順で実行する．

IEEE 1363-2000 に記述されている素体 $\mathbb{F}_p$ 上楕円曲線 Jacobian 座標系における点 2 倍算アルゴリズムを Algorithm 2.4に示す [8]．ただし，入力点が無限遠点 $\mathcal{O}$ だった場合などに必要な例外処理は記述を省略した．また，一般の a に対するアルゴリズムを記述したが，NIST 推奨楕円曲線は全て $a = -3$ である．

Algorithm 2.4 Point doubling in terms of Jacobian coordinates

Input $P_1(X_1, Y_1, Z_1) \in E(\mathbb{F}_p)$
Output $P_2(X_2, Y_2, Z_2) = 2P_1$

1. $T_1 \leftarrow X_1$
2. $T_2 \leftarrow Y_1$
3. $T_3 \leftarrow Z_1$
4. `if` $a = -3$ `then`
5. $\quad T_4 \leftarrow T_3^2$
6. $\quad T_5 \leftarrow T_1 - T_4$
7. $\quad T_4 \leftarrow T_1 + T_4$
8. $\quad T_5 \leftarrow T_4 \times T_5$
9. $\quad T_4 \leftarrow 3 \times T_5$
10. `else`
11. $\quad T_4 \leftarrow a$
12. $\quad T_5 \leftarrow T_3^2$
13. $\quad T_5 \leftarrow T_5^2$
14. $\quad T_5 \leftarrow T_4 \times T_5$
15. $\quad T_4 \leftarrow T_1^2$
16. $\quad T_4 \leftarrow 3 \times T_4$
17. $\quad T_4 \leftarrow T_4 + T_5$
18. `end if`
19. $T_3 \leftarrow T_2 \times T_3$
20. $T_3 \leftarrow 2 \times T_3$
21. $T_2 \leftarrow T_2^2$
22. $T_5 \leftarrow T_1 \times T_2$
23. $T_5 \leftarrow 4 \times T_5$
24. $T_1 \leftarrow T_4^2$
25. $T_1 \leftarrow T_1 - 2 \times T_5$
26. $T_2 \leftarrow T_2^2$
27. $T_2 \leftarrow 8 \times T_2$

28. $T_5 \leftarrow T_5 - T_1$
29. $T_5 \leftarrow T_4 \times T_5$
30. $T_2 \leftarrow T_5 - T_2$
31. $X_2 \leftarrow T_1$
32. $Y_2 \leftarrow T_2$
33. $Z_2 \leftarrow T_3$
34. `return` (X_2, Y_2, Z_2)

Jacobian 座標系点 2 倍算における特殊な中間変数

本節では，前節で述べた実装に対し，点のランダム化にも関わらず点 2 倍算中に現れる特殊な性質を持つ中間変数について考察する．前述のように，このような中間変数が存在すれば，電力解析が可能となる．

特殊な性質を持つ点として次がすでに考察されている [1, 7] [3].

> **特殊点 1**: 点の座標値が 0 の点，および点 2 倍算中の中間変数が 0 となる点.

点 P_0 が上記特殊点 1 である必要十分条件は，次の条件 C1∼C5 のいずれか 1 つを満たすことである [1].

C1. $x = 0$ または $2P_0$ の x 座標が 0
C2. $y = 0$ または $2P_0$ の y 座標が 0
C3. P_0 の位数が 3
C4. $3x^2 + a = 0$
C5. $5x^4 + 2ax^2 - 4bx + a^2 = 0$

また，[4] においては，NIST 推奨曲線の定義体標数 p が sparse であることに着目し，特殊な性質を持つ点として次が考察された.

> **特殊点 2**: 射影座標表現において X 座標と Z 座標とのハミング距離が小さくなるような点 $P_0 = (x, y)$.

我々は，点 2 倍算 (Algorithm 2.4) 中の中間変数に着目し，上記概念を次のように拡張する.

[3] [1] では，点 2 倍算だけでなく，点加算中の中間変数についても検討されている.

> **特殊点 3**: 点 2 倍算 (Algorithm 2.4) の演算中，中間変数 T_i のうち，ハミング距離が小さい T_i の組が存在するような点 $P_0 = (x, y)$.

定義より，特殊点 2 は特殊点 3 に含まれる．特殊点 3 が電力解析などによりランダムな点と識別できると仮定すれば，電力解析が可能となる．次に，Algorithm 2.4中に上記特殊点 3 が存在することを示す.

特殊点 $P_0 = (x, y)$ は，楕円点倍算中，ランダムな $Z \in \mathbb{F}_p^\times$ に対して $P_0 = (Z^2x, Z^3y, Z)$ と表現されているものとする．Algorithm 2.4では，x 座標に関して次の計算を行っている.

X1. $T_1 = Z^2x$ (`step 1`)
X2. $T_4 = Z^2$ (`step 5`)
X3. $T_5 = Z^2(x - 1)$ (`step 6`)
X4. $T_4 = Z^2(x + 1)$ (`step 7`)

$x = 2^\lambda$，λ は小さい非負整数，とすれば標数 p が sparse なため，式 X1 と X2 における T_1 と T_4 のハミング距離は小さくなる確率が高い．また，$x = 2^\lambda + 1$，λ は小さい非負整数，とすれば $x - 1 = 2^\lambda$，$x + 1 = 2^{\lambda+1}$ であるから，式 X3 と X4 における T_5 と T_4 のハミング距離は小さくなる確率が高い．(詳細な確率評価は今後の課題である．)

次に，y 座標に関しては次の計算を行っている.

Y1. $T_3 = Z^4y$ (`step 19`)
Y2. $T_3 = Z^42y$ (`step 20`)

よって，$y = 2^\lambda$，λ は小さい非負整数，とすれば式 Y1 と Y2 における T_3 と T_3 のハミング距離は小さくなる確率が高い.

以上より，特殊点 3 として次の 3 種類が存在することがわかる.

1. $P_0 = (2^\lambda, y)$
2. $P_0 = (2^\lambda + 1, y)$
3. $P_0 = (x, 2^\lambda)$

Algorithm 2.4の `step 21` 以降は，全ての中間値 T_i は，X 座標値と Y 座標値との積に依存する値，または，X 座標値または Y 座標値の奇数倍

となるため，ハミング距離が小さい T_i の組は現れない．

なお，$a \neq -3$ の場合は次の計算が行われる．

X′1. $T_5 = Z^4$ (step 13)

X′2. $T_4 = Z^4 x^2$ (step 15)

よって，$x = 2^\lambda$，λ は小さい非負整数，とすれば式 X′1 と X′2 における T_5 と T_4 のハミング距離は小さくなる確率が高い．

素体 $\mathbb{F}_p$ 上楕円曲線 (式 (2.1)) においては，点 $(2^\lambda, y)$ は $2^3\lambda + a2^\lambda + b$ が平方剰余の時，点 $(2^\lambda + 1, y)$ は $(2^\lambda + 1)^3 + a(2^\lambda + 1) + b$ が平方剰余の時に存在する．5 つの素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線においては，いずれの曲線も小さい非負整数 λ に対して解を持つ．λ が最小な $(2^\lambda, y)$ と $(2^\lambda + 1, y)$ を付録 3.5に示す．

2.5 まとめ

本稿では，楕円点倍算の DPA 対策であるランダム化射影座標を用いた実装に対する電力解析を考察した．素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線による楕円点倍算を，Jacobian 座標系による点の表現とランダム化射影座標とを用いて実装した場合，点 $(2^\lambda, y)$，点 $(2^\lambda + 1, y)$，点 $(x, 2^\lambda + 1)$ λ は小さい非負整数，はランダム化の影響を受けない特殊な性質を持つこと，すなわち，ハミング距離が小さくなる中間変数が現れることを示した．この中間変数を利用して，選択入力解析によって秘密べき指数を導出可能となる．

ハミング距離に関する詳細な評価，および標数 2 拡大体 $\mathbb{F}_{2^m}$ 上楕円曲線に対する中間変数の評価は今後の課題である．

本稿で述べた解析法の対策としては，べき指数のランダム化などの暗号処理手順のランダム化や，ランダム化初期点法 [27, 10] などが考えられる．

3 耐タンパ性を備えたユニークデバイスに基づく暗号認証基盤の検討

3.1 はじめに

情報通信技術や情報セキュリティ技術の普及・発展，法制度の整備に伴い，電子マネーや電子選挙，電子商取引など，情報技術に基づいて実現された様々なアプリケーションが急速に利用され始めている．このようなサービスの電子化により，遠隔地の利用者に対し，インターネットなどの通信を利用したサービス提供が可能となった．しかし，利便性が増すと同時に，様々な安全性の問題も発生する．特に，これらの中には，利用者のプライバシ保護，通信相手の認証が必須となるアプリケーションが多い．

このような問題を解決するためには，正しい通信相手のみが通信内容を理解できるような通信方式、もしくは、送信者が誰であるか受信者が確認できるような通信方式が必要となる．これを実現する手法として、証明書を用いた公開鍵基盤（PKI）が提案されている。ユーザは、証明書発行機関（CA：Certificate Authority）に依頼し、公開鍵の値と、自分がその公開鍵ペアの保持者であることを証明する証明書（公開鍵証明書）を発行してもらう。この証明書に記載されてる公開鍵を用いて通信を暗号化することにより、通信内容はその保持者のみが復号化できる事が保障される。

上記のアプローチによる PKI に対しては多くの研究がされており、商用サービスも多く行われているが、通信相手ごとに対応する証明書を入手する手続きが必要となるため、公開鍵を入手する手間が大きい。これを解決するため、ID 情報（名前、メールアドレスなど）を公開鍵として利用する ID ベース暗号／署名方式が Shamir により初めて提案された [32]。本システムでは、マスタ鍵と各パーティの ID 情報から秘密鍵が生成され、各パーティへ配布される。よって、ユーザは通信相手の ID 情報を知っていればそれを公開鍵として利用できるため、公開鍵を入手する手間が省け、ユーザにとって利便性の高いシステムとなる。

その後、これと同様の機能を実現するため、様々なセッティングに基づいた手法が提案されている [2]〜[28], [30]。本論文では、これらの方式について検討を行った上で、それぞれの類似点・相違点を挙げる。

3.2 既存技術

通信相手の ID 情報を用いて通信情報の暗号化や送信者認証を行うことが可能なシステムを、ID

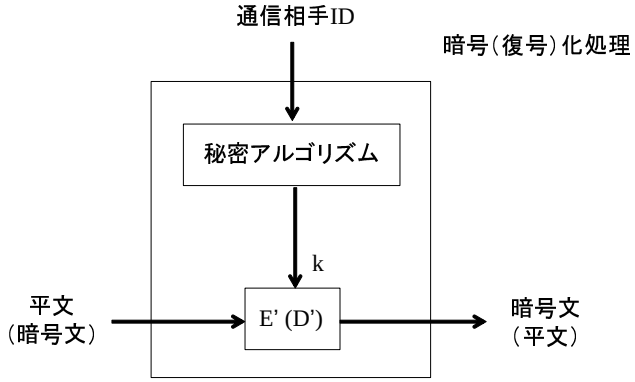

図 1: 鍵事前配布方式（KPS)

ベース暗号認証基盤と呼ぶ。本章では、既存方式である松本ら [30]、Desmedt ら [5]、Boneh ら [2] の提案手法をそれぞれ説明する。各方式を説明する図で用いられている E'、E''、D'、D''は、それぞれ共通鍵暗号・復号化関数を意味する。また、k は暗号化／復号化鍵を意味し、s はマスタ鍵（秘密鍵生成センタ（PKG）と呼ばれる第三者機関が選択する、システム全体で用いられる秘密鍵）を意味する。各方式では、全てのパーティに対してユニークな ID 情報が割り当てられていると仮定される。

鍵事前配布方式（KPS)

松本らにより提案された鍵事前配布方式（KPS: Key Predistributionb System）[30] とは、任意のパーティを含んだグループ内で鍵を共有するための方式である。本方式では、Shamir らの方式と同様、最初に PKG により各パーティの秘密鍵を生成するためのアルゴリズム（センタアルゴリズム）を決定する。センタアルゴリズムへ ID 情報を適用することによって、各パーティの秘密アルゴリズムが決定され、各パーティへ安全に配布される。パーティは、自身が保持する秘密アルゴリズムへグループに属する全パーティの ID 情報（自身の ID 情報は除く）を入力することにより、そのグループのパーティのみが計算可能な鍵を得ることが出来る（図 1)。KPS を用いることにより、誰とでも簡単に秘密鍵を当事者間の予備的な通信なしに共有し暗号通信を行うことができる。上記の機能を実現するためには、下記の性質を満たす関数 f()、g() が必要となる。

$$S_i = f(s; ID_i) \tag{3.1}$$

$$K_{ij} = g(S_i; ID_j) = g(S_j; ID_i) \tag{3.2}$$

$$= f(s; ID_j; ID_i) = f(s; ID_i; ID_j) \tag{3.3}$$

ここで、s はマスタ鍵を表し、PKG が選択する。S_i はパーティ i に配布される秘密鍵を表し、K_{ij} はパーティi および j の間の共通鍵を表す。関数 g() を公知のアルゴリズムとすることで、各パーティは任意の通信相手の ID 情報と自身の秘密鍵 Si を用いて共通鍵が計算できる。具体的な実現法として、[30] では線形スキームと呼ばれる方式が提案されている。本方式では、PKG は最初に $(\omega+1)\times(\omega+1)$ 対称行列 A を作成し、パーティi に対し秘密アルゴリズム $S_i = v_i A$ を配布する。ここで、ω は想定される最大結託者数とし、v_i は ID_i より一意に定まる $\omega+1$ 次の横ベクトルとする。また、v_i より ID_i が一意に求まるものとする。パーティi はパーティ j との共有鍵 Kij を以下の式により導出する。$Kij = S_i \cdot^t v_j$ 上記は 2 者間の鍵共有方式であるが、3 者間以上の鍵共有も構成可能となっている。現在まで、計算の効率性と安全性のトレードオフを考慮した様々な KPS が提案されている [31]。

Desmedt らによる PKI システム

Desmedt らは、耐タンパ性デバイスを利用した ID ベース暗号／署名方式を設計している [5]。具体的な構成法として 2 通りの方式を提案しており、耐タンパデバイスのほか、選択平文攻撃に対して安全な共通鍵暗号・復号化関数（E '、E "、D '、D "）を使用する。また、KPS 同様、第三者期間である PKG が秘密鍵生成を行う。ここで使用される耐タンパ性デバイスとは、外部からデバイス内部の情報を読み取られることを防ぐため、半導体チップなどの内部解析や改ざんを物理的及び論理的に防衛する性能を備えたデバイスを指す。図 2、3 中に灰色で描かれている領域は、耐タンパ性を備えたデバイスにおける処理を表す。デバイスへの入力値（平文・ID 情報など）はデバイス保持者が任意に設定できるが、内部で入力／生

成される値は保持者でも解析／変更できないと仮定する。

最初の方式（図 2：以降、DQ1 と呼ぶ）では、PKG により各パーティの ID 情報をマスタ鍵を用いて復号化する事により、各パーティの秘密鍵（k）が生成され、それぞれ安全に配布される。暗号化を行う際、送信者は自身が保持する耐タンパデバイスへ平文、および受信者の ID 情報を入力する。デバイス内部にはマスタ鍵を用いた復号化関数が内蔵されており、受信者の ID 情報はこれに入力され、秘密鍵が生成される。入力した平文は、この秘密鍵を用いて暗号化され、デバイスから出力される。復号化の際、受信者は TTP から受け取った秘密鍵を用いて暗号文を復号化することにより、平文が出力される。

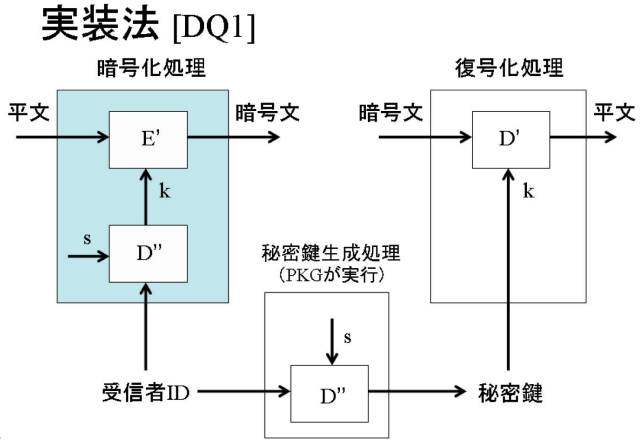

図 2: Desmedt-Quisquater 方式（1）

2 番目の方式（図 3：以降、DQ2 と呼ぶ）では、暗号／復号化の際に送信者の情報を入力することが可能になっている。すなわち、暗号化の際、送信者は平文、受信者の ID 情報に加え、送信者自身の秘密鍵を耐タンパデバイスへ入力する。上記の方式と同様、デバイス内部にはマスタ鍵を用いた復号化関数が内蔵されており、受信者の ID 情報はこれに入力され、その出力と送信者の秘密鍵を排他的論理和した値が暗号化鍵として生成される。入力した平文は、この鍵を用いて暗号化され、デバイスから出力される。復号化の際においては、暗号文、受信者の秘密鍵に加え、送信者の ID 情報をデバイスへ入力する。送信者の ID 情報はマスタ鍵で復号化され、受信者の秘密鍵と排他的論理和した値が復号化鍵として用いられる。

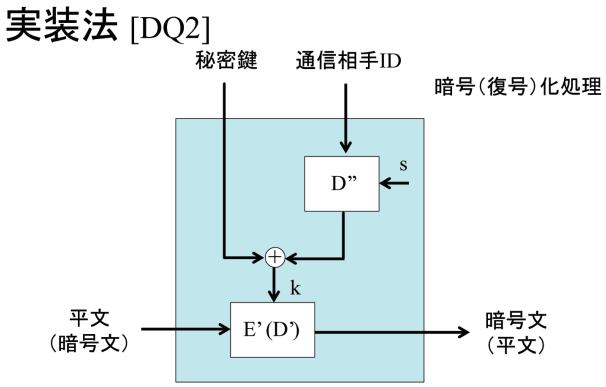

図 3: Desmedt-Quisquater 方式（2）

DQ1 では、暗号化の際にデバイス内部でマスタ鍵が使用されるが、送信者固有の情報を入力することはなく、復号化の際にも送信者に関する情報を入力することはない。暗号化の場合、ID 情報を入力された受信者のみが復号化可能な暗号文（送信者でさえ、復号化するための鍵の値は分からない）が出力される。この性質から、本方式は ID ベース暗号と考えられ、電子署名も実現できる。一方、DQ2 では送信者、および受信者それぞれに固有の情報（ID 情報や秘密鍵）を入力し、入力されたパーティ間で利用される共通鍵を用いて暗号／復号化を行うため、本方式は KPS を実現する一手法と考えられる。ただし、送信者情報を入力しない場合は DQ1 と同じ構成となるため、この場合は ID ベース暗号と考えられる。

ID ベース暗号システム

ID ベース暗号システムでは、最初に PKG によりマスタ鍵と各パーティの ID 情報から秘密鍵が生成され、各パーティへ安全に配布される。Boneh、Franklin らによる ID ベース暗号システムを説明 2001 年、Boneh-Franklin らによりペアリングを用いた初めての実用的な ID ベース暗号 [2] が提案されて以降、多くの ID ベース暗号／署名方式が提案されている．ID ベース署名では，秘密鍵生成センタ（PKG）と呼ばれる TTP を考える．システムセットアップにより，PKG は秘密鍵である master secret と，公開鍵に対応するシステムパラメーターのペアを生成する．master secret

はユーザーの秘密鍵生成に使用し，システムパラメーターは検証時に必要に応じて検証者が使用する．PKG が複数のユーザーの秘密鍵を生成する場合は，同じ master secret を利用して秘密鍵生成を行う．本方式の安全性は、Bilinear Diffie-Hellman (BDH) 問題に基づいている。（図 4 参照）

図 4: ID ベース暗号

デバイス固有値を用いた対称鍵暗号技術による ID ベース暗号化方式（IST)

3.3 デバイス固有値を用いた対称鍵暗号技術による ID ベース暗号化方式（IST)

本章では、深谷らにより提案された方式である、デバイス固有値を用いた対称鍵暗号技術による ID ベース暗号化方式（IST：An ID-based encryption scheme based on symmetrickey technique with a trusted device）[28] を紹介する。本方式では、各耐タンパデバイスごとにユニークな秘密アルゴリズムを持たせることにより機器認証を行う。機器認証とは、利用機器固有の値を用いて、その機器がなりすましなどのない正しい機器であるかどうかが確認するための手続きを意味する。本方式は、Desmedt らが提案した方式と同様、耐タンパ性デバイスを仮定している。ただし、Desmedt らが提案した方式では、デバイス内部は全て解析不能性・改ざん不能性を満たした耐タンパデバイスが使用されるが、IST では各デバイスに割り当てられたユニーク値（ユニーク ID）は公開されている。すなわち、ユニーク ID は、改ざん不能性を満たすデバイス領域内に格納されるが、解析不能性については必要としない。以下では、改ざん不可能なユニーク ID を格納した耐タンパデバイスをユニークデバイスと呼ぶ。

通信手順

IST 方式の手順は以下の通り（図 5)。送信者は自身が保持するユニークデバイスへ平文、受信者の ID 情報を入力すると、デバイス内の秘密アルゴリズムにおいて受信者の ID と送信者の ID の組み合わせが行われ、送信者・受信者のみが計算可能な共通鍵が生成される。さらに、平文の共通鍵による暗号化、認証子の付加が実行され、デバイスより出力される。また、暗号文を受信した場合、受信者は暗号文、および送信者 ID を自身のデバイスへ入力する。暗号化時と同様に、デバイス内部では受信者の ID と送信者の ID の組み合わせが行われ、共通鍵が生成される。これを用い、暗号文の復号化、および認証子の検証が行われ、送信者認証が行われた場合は平文を出力し、認証が不受理の場合は通信を拒否する。

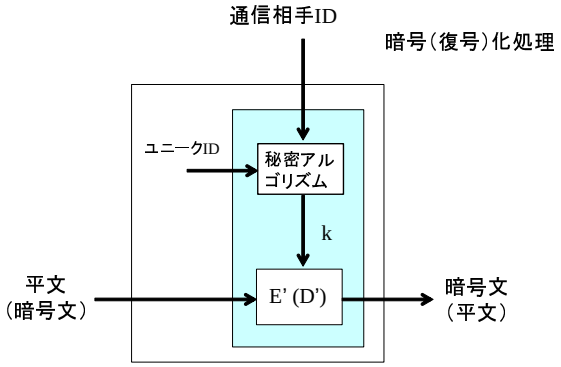

表 1 各方式における入力情報

方式	暗号化			復号化		
	秘密鍵	ID	平文	秘密鍵	ID	暗号文
証明書ベース PKI	–	○*	○	○	–	○
KPS	内部	○	○	内部	○	○
DQ1	–	○	○	○	–	○
DQ2	○	○	○	○	○	○
ID ベース暗号	–	○	○	○	–	○
IST	内部	○	○	内部	○	○

図 5: デバイス固有値を用いた対称鍵暗号技術による ID ベース暗号化方式（IST）

各手法の相関関係（入力情報の観点から）

性質

IST を用いることにより、KPS と同様、当事者間の予備的な通信なしに秘密鍵（対称鍵）を用いた認証付きの暗号通信を行うことができる。上記の機能を実現するためには、下記の性質を満たす関数 f() が必要となる。

$$K_{ij} = f(s; ID_j; ID_i) = f(s; ID_i; ID_j) \quad (3.4)$$

各記号の意味は 2. 1 章を参照。関数 $f()$ を秘密アルゴリズムとして各デバイス内に格納することで、各パーティは任意の通信相手の ID 情報と自身のユニーク ID を用いて共通鍵が計算できる。f() に入力されるユニーク ID の値はデバイス保持者自身にも変更不可であるため、あるデバイスを利用した場合、そのデバイスに格納されているユニーク ID を含んだグループの鍵のみ生成できる。IST における共通鍵生成のメカニズムは KPS の定義に含まれるため、鍵生成手順は KPS の一方式であると考えられる。Desmedt らの方式と同様、IST では耐タンパデバイスを用いて実装されるが、IST の特徴は各デバイス内部に固有の ID 情報を持たせる点である。また、ユーザ自身も秘密情報を知らない。2. 章で紹介した各方式やパスワード認証などでは、どの端末からでも認証処理を行うことが出来る。一方、IST の通信処理を正しく行うためには、ユーザは正しい機器を使用する必要がある。これにより、企業などの組織において、本来は使用が禁止されている私物端末を使って組織内の情報にアクセスし、機密情報を漏洩してしまう、という問題を解決できる。次章では、より具体的に各方式の相違点を検討する。

実装法

ユニークデバイスの製造方法は [28] に記述されている。ユニーク値を持つデバイスを製造するには、ハードウェアに変更できない固有値（ユニーク値）を持たせるよう製造する必要がある。例えば、ユニーク回路となる電気的ステートメント（通路）を各デバイスごとに異なるよう製造する、または回路そのものをレーザーで物理的に切断するなどの方法が考えられている。

3.4 比較検討

2. 章において、既存の ID ベース暗号認証基盤を説明した。本章では、各手法の特徴を挙げた上で、それぞれの相関関係を明らかにする。特に、各方式での暗号化・復号化における入出力情報、およびシステムを構成する際に必要となる条件や仮定などの観点からそれぞれの特徴を検討する。

入出力情報

まず、各手法におけるアルゴリズムの違いを明確にするため、入出力情報の違いを検討する。どの方式においても出力情報は暗号文であるが、入力情報については違いがある。それぞれの入力情報は表 1 の通り。

上記の表で挙げたどの方式においても、暗号化の際は受信者の ID 情報、および平文を入力する（証明書を用いた PKI の場合、ID 情報の代わりに受信者の公開鍵証明書を入力）。送信者の秘密鍵については、KPS・IST 方式では耐タンパデバイス内部や秘密アルゴリズムにおいて入力され、DQ2 ではユーザがデバイス外部から入力する。アルゴリズムや耐タンパデバイス内部で入力される値であるため、ユーザは入力値を変更できない。一方、DQ2 の構成では、ユーザは秘密鍵を入力しない、という選択も可能となっている。また、証明書ベース PKI・DQ1・ID ベース暗号では秘密鍵の入力がない。

復号化の際は、どの方式においても暗号文が入力される。受信者の秘密鍵はどの方式においても入力されるが、KPS・IST 方式では暗号化の際と同様、内部で入力される。送信者の ID 情報については、証明書ベース PKI・DQ1・ID ベース暗号では入力しないが、それ以外の方式では入力される。DQ2 においては、暗号化の際に送信者の秘密鍵を入力しなかった場合、復号化における送信者 ID 情報の入力は必要ない。

上記より、入出力情報の観点から、各手法は図 6 のような包含関係にあると考えられる。すなわち、証明書ベース PKI・DQ1・ID ベース暗号、および KPS・IST はそれぞれ異なるタイプの ID ベース暗号認証基盤であるとみなされ、DQ2 は入力値によってどちらの方式も実現できる。各方式においてパーティが知りうる情報の観点から考え

ると、KPS・IST ではグループ内の全パーティが同一の鍵を生成・共有するが、証明書ベース PKI・DQ1・ID ベース暗号では復号鍵の値を送信者は知ることが出来ないため、これらの方式では電子署名システムが容易に構成できる。このことからも、上記と同様の分類がされる。

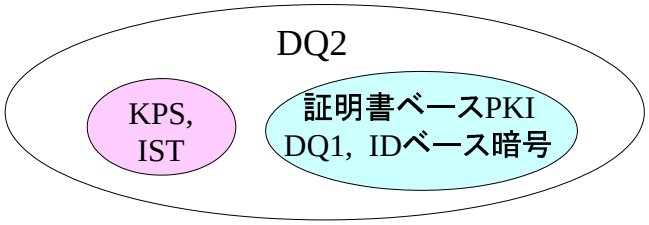

表 2 各方式における仮定・条件

	秘密鍵生成者	安全性の根拠
証明書ベース	ユーザ／ CA	公開鍵証明書の信頼性
KPS (松本先生)	PKG	システム次第
Desmedt-Quisquater	PKG	耐タンパ性
ID ベース暗号 (Boneh-Franklin)	PKG	システム次第 (ペアリングの計算困難性)
IST	PKG	耐タンパ性 (ユニークデバイスの利用)

図 6: 各手法の相関関係（入力情報の観点から）

仮定・条件

各方式の具体的な実装法を考えた場合、システムのセッティングや安全性を満たすために必要な仮定・条件がそれぞれ異なる。表 2 では、各方式において秘密鍵を生成するパーティ、安全性の根拠についてまとめた。PKG を用いた方式では、上記の条件に加え、マスタ鍵の秘匿性も必要となる。

証明書ベース PKI では、秘密鍵は通常ユーザ自身が生成し、その公開鍵に対する証明書を CA に作成してもらう。このとき、CA に対して秘密鍵を隠しておくことが可能である。よって、CA が悪意を持っていたとしても、正しい公開鍵で暗号化された通信は、それに対応する秘密鍵を持った受信者以外は復号化できない。ただし、正しくない公開鍵を正しいものであるかのように見せかけた証明書の偽造が可能であるため、これを利用した盗聴・フィッシングなどの攻撃が存在する。一方、その他の方式では秘密鍵は PKG が生成するため、PKG が悪意を持っている場合、全ての暗号化された通信を復号化できる。これは証明書偽造よりも容易であり、かつユーザに気付かれにくい攻撃であるため、PKG に対する信頼性は CA より高い必要がある。

証明書を用いた場合、システムの安全性は証明書に記載された公開鍵の正当性に拠る。すなわち、CA が悪意を持っている可能性がある場合、もしくは CA の（証明書生成に用いる）署名鍵が漏洩した場合、システムの安全性は破綻する。DQ1・DQ2・KPS では耐タンパ性デバイスの安全性に拠る。特に DQ1 の場合、デバイス内部で使用される暗号化鍵が漏洩すると、それの保持者宛の暗号通信が全て解読され、署名偽造も可能となる。

ユニークデバイスの利用

IST や Desmedt らの方式では耐タンパ性デバイスを用いているが、デバイス内に格納される情報はそれぞれ異なる。Desmedt らの方式ではユーザが耐タンパデバイス外部から秘密鍵の入力を行うが、IST ではデバイス内部に秘密鍵が保持されている。よって、Desmedt らの方式を使用する場合、各ユーザが保持するデバイスは全て同一のものであり、ユーザが入力する秘密情報によって認証が行われる。よって、本方式はユーザ認証（通信相手が目的の相手であることを確認）に用いられる。それに対し、IST で配布されるデバイスはユーザごとに異なり、ユーザ自身も内部の秘密鍵を知ることが出来ないようになっている。これにより、IST は機器認証（通信に特定の機器が使用されていることを確認）を実現する方式として利用され、コンテンツ保護などへの利用が考えられている [29]。

IST で用いられているユニークデバイスを利用することにより、ID ベース暗号や DQ1 のような PKI システムが構成できる。構成の一例を図 7 に示す。本構成は DQ1 の構成をベースとし、暗号化の際は DQ1 と同様の処理が行われる。暗号化の際に入力される受信者 ID（＝受信者が保持しているデバイスに格納されているユニーク ID）は、送信者が任意に選択する。復号化処理の際は IST と同様の処理が行われ、ユニーク ID を備えた耐タンパデバイスを利用している。このとき、

ユニーク ID は各デバイスごとに固定された値であるため、そのデバイス宛てに送られてきた暗号文のみが復号化できる。また DQ1 と同様、平文を復号化処理の入力とすることで、その出力文を電子署名として利用できる。

図 7: ユニークデバイスを利用した PKI

3.5 まとめ

本論文では，既存の ID ベース暗号認証基盤である KPS、Desmedt らの方式、ID ベース暗号、IST について調査を行い、それぞれの特徴や相違点について検討した。

付録：素体 $\mathbb{F}_p$ 上の NIST 推奨楕円曲線上の点 $(2^\lambda, y)$ および $(2^\lambda + 1, y)$

素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線上に存在する点 $(2^\lambda, y)$ および $(2^\lambda + 1, y)$ のうち，非負整数 λ が最小である点を以下に示す.

P-192:

$x = 2$

y = 2df5fa08 ab474e8f 8f2ad5ca ca826434 7d1fb300 43214687

$x = 3$

y = 64fc66b7 c0f932d5 564fa514 b3ba7858 c8ee083f 8c728022

P-224:

$x = 8$

y = 2f2754f8 eca72d77 84910c31 1e78caf3 88d07390 3d01dba6 956fb093

$x = 3$

y = 8353d963 9842aa15 eb1000b1 52101a17 b687aeb5 0eb37705 4b913fbb

P-256:

$x = 8$

y = b706288a ca290db0 d624d1d2 3f37f6a6 27249b16 d631ff69 2242d085 636041b3

$x = 5$

y = 459243b9 aa581806 fe913bce 99817ade 11ca503c 64d9a3c5 33415c08 3248fbcc

P-384:

$x = 2$

y = 8cdeadbb d04911a3 c1931e26 df3fa643 9dca9c7e b286fbd4 6fc319f0 e2bb7802 32baf578 25fc0c19 12ada2fe fe84024c

$x = 3$

y = 6660041b 1c798462 0e8d7fd7 ccdb50cc 3ba816da 14d41a4d 8affaba8 488867f0 ca5a24f8 d42dd7e4 4b530a27 dc5b58da

P-521:

$x = 2$

y = d9 254fdf80 0496acb3 3790b103 c5ee9fac 12832fe5 46c63222 5b0f7fce 3da4574b 1a879b62 3d722fa8 fc34d5fc 2a8731aa d691a9a8 bb8b554c 95a051d6 aa505acf

x = 1

y = 10 e59be93c 4f269c02 69c79e2a
fd65d6ae aa9b701e acc194fb 3ee03df4
7849bf55 0ec636eb ee0ddd4a 16f1cd94
06605af3 8f584567 770e3f27 2d688c83
2e843564

参考文献

[1] T. Akishita and T. Takagi, "Zero-value resister attack on elliptic curve cryptosystems," IEICE, Trans. Fundamentals, vol. E88-A, No.1, pp.132–139, 2005.

[2] D. Boneh, M. Franklin, "Identity Based Encryption from the Weil Pairing," Crypto 2001.

[3] J.-S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," Cryptographic Hardware and Embedded Systems – CHES '99, LNCS 1717, pp.292–302, Springer-Verlag, 1999.

[4] W. Dupuy and S.K. Jacques, "Resistance of randomized projective coordinates against power analysis," Cryptographic Hardware and Embedded Systems – CHES 2005, LNCS 3659, pp.1–14 Springer-Verlag, 2005.

[5] Y. Desmedt, J. Quisquater, "Public-Key Systems Based on the Difficulty of Tampering (Is There a Difference Between DES and RSA?)," Crypto 1986.

[6] "Digital signature standard (DSS)," FIPS PUB 186-2, U.S. National Institute of Standards and Technology, 2000.

[7] L. Goubin, "A refined power-analysis attack on elliptic curve cryptosystems," Public Key Cryptography – PKC 2003, LNCS 2567, pp.199–211, Springer-Verlag, 2003.

[8] IEEE 1363-2000, "Standard Specifications for Public Key Cryptography," 2000.

[9] P.C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Advances in Cryptology – CRYPTO'99, LNCS 1666, pp.388–397, Springer-Verlag, 1999.

[10] M. Mamiya, A. Miyaji, and H. Morimoto, "Efficient countermeasure against RPA, DPA, and SPA," Cryptographic Hardware and Embedded Systems – CHES 2004, LNCS 3156, pp.343–356, Springer-Verlag, 2005.

[11] P. Montgomery, "Speeding the Pollard and elliptic curves methods of factorization," Math. Comp, vol. 44, 1985.

[12] K. Okeya and T. Takagi, "SCA-resistant and fast elliptic scalar multiplication based on wNAF," IEICE, Trans. Fundamentals, vol. E87-A, No.1, pp.75–84, 2004.

[13] J.A. Solinas, "Generalized Mersenne numbers," Technical Report CORR 99-39, University of Waterloo, 1999.

[14] J.F. Dhem, F. Koeune, P.A. Leroux, P. Mestré and J.-J. Quisquater, "A practical implementation of the timing attack," CARDIS 1998, LNCS 1820, pp.175–190, Springer-Verlag, 1998.

[15] E. Brier and M. Joye, "Weierstrass elliptic curves and side-channel attacks," Public Key Cryptography – PKC 2002, LNCS 2274, pp.335–345, Springer-Verlag, 2002.

[16] M. Brown, D. Hankerson, J. Lopez and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields," Technical Report CORR 2000-56, University of Waterloo, 2000.

[17] C. Gebotys and R. Gebotys, "Secure elliptic curve implementations: an analysis of resistance to power-attacks in a DSP processor," Cryptographic Hardware and Embedded Systems – CHES 2002, LNCS 2523, pp.114–128, Springer-Verlag, 2002.

[18] M. Joye and J.-J. Quisquater, "Hessian elliptic curves and side channel attacks,"

Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS 2162, pp.402–410, Springer-Verlag, 2001.

[19] P.C. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” Advances in Cryptology – CRYPTO ’96, LNCS 1109, pp.104–113, Springer-Verlag, 1996.

[20] P.-Y. Liardet and N.P. Smart, “Preventing SPA/DPA in ECC systems using the Jacobi form,” Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS 2162, pp.391–401, Springer-Verlag, 2001.

[21] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, “Handbook of Applied Cryptography,” CRC Press, 1966.

[22] P.L. Montgomery, “Modular multiplication without trial division,” Mathematics of Computation, vol. 44, no. 170, pp.519–521, 1885.

[23] W. Schindler, “A timing attack against RSA with the Chinese Remainder Theorem,” Cryptographic Hardware and Embedded Systems – CHES 2000, LNCS 1965, pp.109–124, Springer-Verlag, 2000.

[24] Certicom, “Standard for efficient cryptography, SEC2: Recommended elliptic domain parameters,” 2000.

[25] C.D. Walter, “Sliding windows succumbs to Big Mac Attack,” Cryptographic Hardware and Embedded System – CHES 2001, LNCS 2162, pp.286–299, Springer-Verlag, 2001.

[26] C.D. Walter, “Simple power analysis of unified code for ECC double and add,” Cryptographic Hardware and Embedded System – CHES 2004, LNCS 3156, pp.191–204, Springer-Verlag, 2004.

[27] 伊藤, 伊豆, 武仲, “ランダム化初期点を用いた電力解析対策法について (その 3),” SCIS 2005.

[28] 深谷博美, 櫻井幸一, “デバイス固有値を用いた対称暗号技術による ID ベース暗号化方式の実現,” ISEC, 2006 年 3 月.

[29] 深谷博美, 櫻井幸一, “機器認証 DRM システムの設計,” ISEC, 2006 年 7 月.

[30] T. Matsumoto, H. Imai, “On the key predistribution systems: A practical solution to the key distribution problem,” in Advances in Cryptology - Crypto 1987.

[31] M. Ramkumar, “I-HARPS: An Efficient Key Predistribution Scheme,” Cryptology ePrint Archive 2005/138.

[32] A. Shamir, “Identity-based cryptosystems and signature schemes,” Advances in cryptology, Crypto 1984.

研究業績一覧

著書

1. Chunhua Su, Jianying Zhou, Feng Bao, Guiling Wang, Kouichi Sakurai:
“Chapter10 Privacy-Preserving Techniques in Data Mining, Digital Privacy: Theory, Technologies, and Practices”, Auerbach Publications, 2007 年 12 月.
概要: In today ’s information age, data collection is ubiquitous, and every transaction is recorded somewhere. Data mining is becoming increasingly common in both the private and public sectors. Industries, such as banking, insurance, medicine, and retailing, commonly use data mining to reduce costs, enhance research, and increase sales. However, their real concern is that their information should not be misused. The fear is that once information is released, it will be impossible to prevent misuse. To do this, we need technical solutions that ensure data will not be released. This chapter presents some suggestions for defining and measuring privacy preservation. We have shown how these relate to both privacy policy and

practice in the wider community, and to techniques in privacy-preserving data mining. We apply the privacy-preserving statistical databases techniques and cryptographic protocols to a scheme to preserve the privacy of a dataset when executing distributed data mining.

学術論文

1. Yasuyuki Sakai and Kouichi Sakurai:
"On the Vulnerability of Exponent Recodings for the Exponentiation against Side Channel Attacks", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E88A, No.1, 154-160, 2005年1月.
概要: In this paper we propose a new side channel attack, where exponent recodings for public key cryptosystems such as RSA and ECDSA are considered. The known side channel attacks and countermeasures for public key cryptosystems were against the main stage (square and multiply stage) of the modular exponentiation (or the point multiplication on an elliptic curve). We have many algorithms which achieve fast computation of exponentiations. When we compute an exponentiation, the exponent recoding has to be carried out before the main stage. There are some exponent recoding algorithms including conditional branches, in which instructions depend on the given exponent value. Consequently exponent recoding can constitute an information channel, providing the attacker with valuable information on the secret exponent. In this paper we show new algorithms of attack on exponent recoding. The proposed algorithms can recover the secret exponent, when the width-w NAF and the unsigned/signed fractional window representation are used.

2. Yasuyuki Sakai and Kouichi Sakurai:
"Timing Attacks against a Parallelized RSA Implementation", IPSJ, Vol. 45, No.8, 1813-1822, 2004年8月.
概要: We discuss timing attacks against RSA using the parallel modular exponentiation. We describe a parallel algorithm for the modular exponentiation $y \equiv x^d \bmod n$. Then timing attacks against the parallel implementation are demonstrated. When we have two processors, which perform the modular exponentiation, an exponent d is scattered into two partial exponents $d^{(0)}$ and $d^{(1)}$, where $d^{(0)}$ and $d^{(1)}$ are derived by bitwise AND operation from d such that $d^{(0)} = d \wedge (0101\cdots01)_2$ and $d^{(1)} = d \wedge (1010\cdots10)_2$. Two partial modular exponentiations $y_0 \equiv x^{d^{(0)}} \bmod n$ and $y_1 \equiv x^{d^{(1)}} \bmod n$ are performed in parallel using two processors. Then we can obtain y by computing $y \equiv y_0 y_1 \bmod n$. In general, the hamming weights of $d^{(0)}$ and $d^{(1)}$ are smaller than that of d. Thus a fast computation of the modular exponentiation $y \equiv x^d \bmod n$ can be achieved. We describe a timing attack against RSA with and without the Chinese Remainder Theorem (CRT) using the parallel modular exponentiation. Both the secret exponents $d_p = d \bmod p-1$ and $d_q = d \bmod q-1$, where $n = pq$, are scattered into two partial exponents, respectively. We show that timing attacks are still applicable to that case.

3. Yasuyuki Sakai and Kouichi Sakurai:
"A New Attack with Side Channel Leakage during Exponent Recoding Computations", Cryptographic Hardware and Embedded Systems – CHES 2004, Springer LNCS No. 3156, 298-311, 2004年8月.
概要: In this paper we propose a new side channel attack, where exponent recodings for public key cryptosystems such as RSA and ECDSA are considered. The known side channel attacks and countermeasures

for public key cryptosystems were against the main stage (square and multiply stage) of the modular exponentiation (or the point multiplication on an elliptic curve). We have many algorithms which achieve fast computation of exponentiations. When we compute an exponentiation, the exponent recoding has to be carried out before the main stage. There are some exponent recoding algorithms including conditional branches, in which instructions depend on the given exponent value. Consequently exponent recoding can constitute an information channel, providing the attacker with valuable information on the secret exponent. In this paper we show new algorithms of attack on exponent recoding. The proposed algorithms can recover the secret exponent, when the width-w NAF and the unsigned/signed fractional window representation are used.

4. Dong-Guk Han, Tetsuya Izu, Jongin Lim, and Kouichi Sakurai:
"Side Channel Cryptanalysis on XTR Public Key Cryptosystem", IEICE Trans. Fundamentals, Special Section on Discrete Mathematics and Its Applications 2005, 1214-1223, .
概要: The XTR public key cryptosystem was introduced in 2000. XTR is suitable for a variety of environments including low-end smart cards, and is regarded as an excellent alternative to RSA and ECC. Moreover, it is remarked that XTR single exponentiation (XTR-SE) is less susceptible than usual exponentiation routines to environmental attacks such as the timing attack and the differential power analysis (DPA). This paper investigates the security of side channel attack (SCA) on XTR. In this paper, we show the immunity of XTR-SE against the simple power analysis if the order of the computation of XTR-SE is carefully considered. In addition, we show that XTR-SE is vulnerable to the data-bit DPA, the address-bit DPA, the doubling attack, the modified refined power analysis, and the modified zero-value attack. Moreover, we propose some countermeasures against these attacks. We also show experimental results of the efficiency of the countermeasures. From our implementation results, if we compare XTR with ECC with countermeasures against "SCAs", we think XTR is as suitable to smart cards as ECC.

5. Dong-Guk Han, Jongin Lim, and Kouichi Sakurai:
"On security of XTR public key cryptosystems against Side Channel Attacks", Proceedings of Information Security and Privacy (ACISP 2004), LNCS 3108, 454-465, 2004年7月.
概要: The XTR public key system was introduced at Crypto 2000. It is regarded that XTR is suitable for a variety of environments, including low-end smart cards, and XTR is the excellent alternative to either RSA or ECC. Previous works remarked that XTR single exponentiation (XTR-SE) is less susceptible than usual exponentiation routines to environmental attacks such as timing attacks and Differential Power Analysis (DPA). In this paper, however, we investigate the security of side channel attack (SCA) on XTR. This paper shows that XTR-SE is immune against simple power analysis under assumption that the order of the computation of XTR-SE is carefully considered. However, we show that XTR-SE is vulnerable to Data-bit DPA, Address-bit DPA, and doubling attack. Moreover, we propose countermeasures that prevent the proposed attacks. As the proposed countermeasure against doubling attack is very inefficient, a good countermeasure against doubling attack is actually necessary to maintain the advantage of efficiency of XTR.

6. Dong-Guk Han, Tetsuya Izu, Jongin Lim and Kouichi Sakurai:
"Modified Power-Analysis Attacks on XTR and An Efficient Countermeasure", Information and Communications Security (ICICS 2004), LNCS 3269, 305-317, 2004年11月.
概要: Han et al. presented a nice overview of some side channel attacks (SCA), and some classical countermeasures. However, their proposed countermeasures against SCA are so inefficient that the efficiency of XTR with SCA countermeasures is at least 129 times slower than that of XTR without them. Thus they remained the construction of the efficient countermeasures against SCA as an open question. In this paper, we show that XTR can be also attacked by the modified refined power analysis (MRPA) and the modified zero-value attack (MZVA). To show validity of MRPA and MZVA on XTR, we give some numerical data of them. We propose a novel efficient countermeasure (XTR-RSE) against "SCAs": SPA, Data-bit DPA, Address-bit DPA, Doubling attack, MRPA, and MZVA. We show that XTR-RSE itself without other countermeasures is secure against all "SCAs". From our implementation results, if we compare XTR with ECC with countermeasures against "SCAs", we think XTR is as suitable to smart-cards as ECC due to the efficiency of the proposed XTR-RSE.

7. Yasuyuki Sakai and Kouichi Sakurai:
"Simple Power Analysis on Fast Modular Reduction with Generalized Mersenne Prime for Elliptic Curve Cryptosystems", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,, E89A, No. 1, pp.231–237, Jan.2006.
概要: We discuss side channel leakage from modular reduction for NIST recommended domain parameters. FIPS 186-2 has 5 recommended prime fields. These primes have a special form which is refered to as generalized Mersenne prime. These special form primes facilitate especially efficient implementation. A typical implementation of efficient modular reduction with such primes includes conditional reduction. A conditional reduction in modular reduction can constitute an information channel on the secret exponent. Several researchers have produced unified code for elliptic point addition and doubling in order to avoid a simple power analysis (SPA). However, Walter showed that SPA still be possible if Montgomery multiplication with conditional reduction is implemented within the unified code. In this paper we show SPA on the modular reduction with NIST recommended primes, combining with the unified code for elliptic point operations. As Walter stated, our results also indicate that even if the unified codes are implemented for elliptic point operations, underlying field operations should be implemented in constant time. The unified approach in itself can not be a countermeasure for side channel attacks.

8. Katja Schmidt-Samoa, Olivier Semay and Tsuyoshi Takagi:
"Analysis of Fractional Window Recoding Methods and Their Application to Elliptic Curve Cryptosystems", IEEE TRANSACTIONS ON COMPUTERS,, VOL. 55, NO. 1,, JANUARY 2006.
概要: Elliptic curve cryptosystems (ECC) are suitable for memory-constraint devices like smart cards due to their small key-size. A standard way of computing elliptic curve scalar multiplication, the most frequent operation in ECC, is window methods, which enhance the efficiency of the binary method at the expense of some precomputation. The most established win-

dow methods are sliding window on NAF (NAF+SW), wNAF, and wMOF, where NAF and MOF are acronyms for nonadjacent form and mutually opposite form, respectively. A common drawback of these schemes is that only a small portion of the numbers are possible sizes for precomputation tables. Therefore, in practice, it is often necessary to waste memory because there is no table fitting exactly the available storage. In the case of wNAF, there exists a variant that allows arbitrary table sizes, the so-called fractional wNAF (Frac-wNAF). In this paper, we give a comprehensive proof using Markov theory for the estimation of the average nonzero density of the Frac-wNAF representation. Then, we propose the fractional wMOF (Frac-wMOF), which is a left-to-right analogue of Frac-wNAF. We prove that Frac-wMOF inherits the outstanding properties of Frac-wNAF. However, because of its left-to-right nature, Frac-wMOF is preferable as it reduces the memory consumption of the scalar multiplication. Finally, we show that the properties of all discussed previous schemes can be achieved as special instances of the Frac-wMOF method. To demonstrate the practicability of Frac-wMOF, we develop an on-the-fly algorithm for computing elliptic curve scalar multiplication with a flexibly chosen amount of memory.

9. Tatsuya Toyofuku and Toshihiro Tabata and Kouichi Sakurai:
   " Program Obfuscation Scheme Using Random Numbers to Complicate Control Flow", The First International Workshop on Security in Ubiquitous Computing Systems (SECUBIQ 2005) in EUC Workshops 2005, Springer LNCS, pp.916-925, 2005 Dec..
   概要: For the security technology that has been achieved with software in the computer system and the protection of the intellectual property right of software, software protection technology is necessary. One of those techniques is called obfuscation, which converts program to make analysis difficult while preserving its function. In this paper, we examine the applicability of our program obfuscation scheme to complicate control flow and study the tolerance against program analysis.

10. Yasuyuki Sakai and Kouichi Sakurai:
    "Simple Power Analysis on Fast Modular Reduction with NIST Recommended Elliptic Curves,", ICICS 2005, Springer LNCS, pp.169-180, 2005.
    概要: We discuss side channel leakage from modular reduction for NIST recommended domain parameters. FIPS 186-2 has 5 recommended prime fields. These primes have a special form which is referred to as generalized Mersenne prime. These special form primes facilitate especially efficient implementation. A typical implementation of efficient modular reduction with such primes includes extra reduction. The extra reduction in modular reduction can constitute an information channel on the secret exponent. Several researchers have produced unified code for elliptic point addition and doubling in order to avoid a simple power analysis (SPA). However,Walter showed that SPA still be possible if Montgomery multiplication with extra reduction is implemented within the unified code. In this paper we show SPA on the modular reduction with NIST recommended primes, combining with the unified code for elliptic point operations. As Walter stated, our results also indicate that even if the unified codes are implemented for elliptic point operations, underlying field operations should be implemented in constant time. The unified approach in itself cannot be a countermeasure for side channel attacks.

11. Chunhua Su, Feng Bao, Jianying Zhou, Tsuyoshi Takagiand Kouichi Sakurai:
"Privacy-Preserving Two-Party K-Means Clustering via Secure Approximation", AINA Workshops, IEEE CS, 385-391, May, 2007.
概要: K-means clustering is a powerful and frequently used technique in data mining. However, privacy breaching is a serious problem if the k-means clustering is used without any security treatment, while privacy is a real concern in many practical applications. Recently, four privacy-preserving solutions based on cryptography have been proposed by different researchers. Unfortunately none of these four schemes can achieve both security and completeness with good efficiency. In this paper, we present a new scheme to overcome the problems occurred previously. Our scheme deals with data standardization in order to make the result more reasonable. We show that our scheme is secure and complete with good efficiency.

12. Chunhua Su, Jianying Zhou, Feng Bao, Tsuyoshi Takagi and Kouichi Sakurai:
"Two-Party Privacy-Preserving Agglomerative Document Clustering", ISPEC 2007, Springer LNCS, 193-208, May, 2007.
概要: Document clustering is a powerful data mining technique to analyze the large amount of documents and structure large sets of text or hypertext documents. Many organizations or companies want to share their documents in a similar theme to get the joint benefits. However, it also brings the problem of sensitive information leakage without consideration of privacy. In this paper, we propose a cryptography-based framework to do the privacy-preserving document clustering among the users under the distributed environment: two parties, each having his private documents, want to collaboratively execute agglomerative document clustering without disclosing their private contents.

13. Masaaki Shirase, Dong-Guk Han, Yasushi Hibino, Ho Won Kim, Tsuyoshi Takagi:
"Compressed XTR", 5-th International Conference on Applied Cryptography and Network Security, LNCS 4521, 420-431, XTR public key system was introduced at Crypto 2000, which is based on a method to present elements of a subgroup of a multiplicative group of a finite field. Its application in cryptographic protocols leads to substantial savings both in communication and computational overhead without compromising security. It was shown how the use of finite extension fields and subgroups can be combined in such a way that the number of bits to be exchanged is reduced by a factor 3. In this paper we show how to more compress the communication overhead. The compressed XTR leads to a factor 6 reduction in the representation size compared to the traditional representation and achieves as twice compactness as XTR. The computational overhead of it is a little worse than that of XTR, however the compressed XTR requires only about additional 6.
概要: June, 2007

14. Sang Soo Yeo, Kouichi Sakurai, SungEon Cho, KiSung Yang and Sung Kwon Kim:
"Forward Secure Privacy Protection Scheme for RFID System Using Advanced Encryption Standard", ISPA Workshops 2007, Springer LNCS, 245-254, There are many researches related to privacy protection in RFID system. Among them, Ohkubo's hash-based scheme is provably secure and it can protect user 's privacy, prevent location tracking, and guarantee forward security completely. Unfortunately, one-way hash functions, which play important roles in Ohkubo 's schem, can '

t be implemented into the current RFID tag hardware. So we propose a new secure protocol for RFID privacy protection, and it is a modified version of Ohkubo 's scheme using Feldhofer's AES module for RFID tag. Our new scheme has almost all of advantages of Ohkubo 's scheme and moreover it can be embedded into RFID tag hardware easily..
概要: August, 2007

15. Satoshi Hada and Kouichi Sakurai:
"A Note on the (Im)possibility of Using Obfuscators to Transform Private-Key Encryption into Public-Key Encryption", IWSEC 2007, Springer, LNCS, 1-12.
概要: October, 2007 Transforming private-key encryption schemes into public-key encryption schemes is an interesting application of program obfuscation. The idea is that, given a private-key encryption scheme, an obfuscation of an encryption program with a private key embedded is used as a public key and the private key is used for decryption as it is. The security of the resulting public-key encryption scheme would be ensured because obfuscation is unintelligible and the public key is expected to leak no information on the private key. This paper investigates the possibility of general-purpose obfuscators for such a transformation, i.e., obfuscators that can transform an arbitrary private-key encryption scheme into a secure public-key encryption scheme. Barak et al. have shown a negative result, which says that there is a deterministic private-key encryption scheme that is unobfuscatable in the sense that, given any encryption program with a private key embedded, one can efficiently compute the private key. However, it is an open problem whether their result extends to probabilistic encryption schemes, where we should consider a relaxed notion of obfuscators, i.e., sampling obfuscators. Programs obfuscated by sampling obfuscators do not necessarily compute the same function as the original program, but produce the same distribution as the original program. In this paper, we show that there is a probabilistic private-key encryption scheme that can not be transformed into a secure public-key encryption scheme by sampling obfuscators which have a special property regarding input-output dependency of encryption programs. Our intention is not to claim that the required special property is reasonable. Rather, we claim that general-purpose obfuscators for the transformation, if they exist, must be a sampling obfuscator which does NOT have the special property.

研究会等

1. 山田尚志，高木剛，櫻井幸一:
"2 冪算における直接計算法を用いたマルチスカラー倍算の効率性評価,", 電子情報通信学会，情報セキュリティ研究会，信学技報，ISEC2007, 2007.
概要: 楕円曲線に基づくデジタル署名アルゴリズム（ECDSA）を使った署名検証において最も時間を要する演算は，2 つのスカラーを用いるマルチスカラー倍算である．マルチスカラー倍算において，予備計算を必要とせずに高速に計算するクラスとして，Interleave 法と NAF(IL-NAF)，Interleave 法と MOF(IL-MOF) が知られている．IL-NAF/MOF を用いたマルチスカラー倍算では，連続する零桁（ゼロラン）の長さによってマルチスカラー倍算の効率性が評価できるため，IL-NAF/MOF のゼロランの長さ（ゼロラン長）の解析は重要である．本稿では，Markov 鎖を用いた桁の分布解析からゼロランの平均長と発生確率を理論的に解析した．IL-NAF の平均ゼロラン長は 3，IL-MOF の平均ゼロラン長は 256=85 となる．また，ゼロランの分布確率の解析をマルチスカラー倍算の計算量の見積りに適用し，2kP 直接計算法を用いた計算方式が 2 倍算を繰り返し計算

する方式よりも 4.7-4.8 % 高速になることを
証明した