早稲田大学大学院 基幹理工学研究科

博 士 論 文 概 要

論 文 題 目

情報量的に安全な鍵事前配布方式の
一般化に関する研究
A study of the generalization of unconditionally secure key predistribution systems

申 請 者

吉田	隆弘
Takahiro	Yoshida

2010 年 5 月

大規模なコンピュータネットワークにおいて，不特定多数のユーザからなるグループが秘匿通信を行う場合，通信前にグループ内で鍵と呼ばれる情報を共有する必要が生じる．このような場合に必要となる技術が，鍵配布方式である．

鍵配布方式では，鍵を第 3 者に知られないように安全に共有する必要があるため，ある種の安全性が要求される．鍵配布方式を含む一般の暗号方式に対する安全性とは，不正を行う攻撃者，攻撃対象，攻撃者の利用可能な情報，及び攻撃者の計算能力を仮定した下で保証される安全性の概念で，主に情報量的安全性と計算量的安全性の 2 種類の安全性が考えられている．ある暗号方式 Π に対する攻撃者が存在し，攻撃者の利用可能な情報を z，攻撃対象の情報を k とおく．このとき，$H(K|Z) > 0$ を満たす Π は情報量的に安全であるという．$H(K)$ と $H(K|Z)$ は，それぞれエントロピー，条件付きエントロピーと呼ばれる量で，以下のように定義される．

$$H(K) = -\sum_{k\in\mathcal{K}} \Pr\{K=k\}\log\Pr\{K=k\}, \tag{1}$$

$$H(K|Z) = -\sum_{k\in\mathcal{K}}\sum_{z\in\mathcal{Z}} \Pr\{K=k, Z=z\}\log\Pr\{K=k|Z=z\}. \tag{2}$$

ここで，$\mathcal{K}$，$\mathcal{Z}$ をそれぞれ攻撃対象の情報がとり得る値全体の集合，攻撃者の利用可能な情報がとり得る値全体の集合とし，K と Z をそれぞれ $\mathcal{K}$，$\mathcal{Z}$ 上に値をとる確率変数とした．情報量的安全性の条件 $H(K|Z) > 0$ は，攻撃者の利用可能な情報 z からでは，攻撃対象 k の情報を完全に得ることができないことを意味する．また，条件が $H(K|Z) = H(K)$ のとき，最も強い安全性になる．すなわち，K と Z は互いに独立となるので，攻撃者は攻撃対象に関する情報を全く得ることができないことを意味する．暗号理論では，このような性質を満たすことを情報量的安全性として定義している．また，情報量的安全性は攻撃者の計算能力に対しては何も仮定を置いていない．すなわち，無限の計算能力を持つ攻撃者に対しても安全性が保証される．一方，計算量的安全性は攻撃者の計算能力に現実的な仮定を置いたときに保証される安全性として定義されるため，計算機能力の急速な進展等によって，将来的に攻撃対象の特定が可能となり，計算量的安全性では長期的な安全性が保証できない．すなわち，計算量的安全性では，攻撃者の計算能力が仮定を満たさなくなると $H(K|Z) = 0$ となってしまう．したがって，情報量的安全性は計算量的安全性よりも高い安全性を有し，長期的な安全性が保証できる極めて高度な安全性となる．本研究では，高度な安全性を有する情報量的に安全な鍵配布方式を研究の対象とする．

情報量的に安全な鍵配布方式は，個体識別のための情報である ID 情報 $\mathrm{D}_1, \mathrm{D}_2, \cdots, \mathrm{D}_{n_D}$ をそれぞれ持つ n_D 個のセンターと，ID 情報 $\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_{n_P}$ をそれぞれ持つ n_P 人のユーザで構成されており，鍵逐次配布方式と鍵事前配布方式の 2 方式が存在する．前者は，ユーザが鍵を使用するたびに，センターから鍵をその都度受け取る方式で，後者は，各ユーザが自身の属している全グループの鍵を，センターから事前に受け取る方式である．鍵事前配布方式は，センターとユーザとの通信が 1 回のみであることから，ユーザの利便性の面から考えると鍵逐次配布方式より優れている．本研究では，利用者の利便性に優れた鍵事前配布方式を研究の対象とする．

従来の鍵事前配布方式は，任意の t 人のユーザからなるグループの鍵が共有できる方式で，次のようなプロトコルとして定義される．[**1**] 各センターは独立に，秘密の情報を生成する．[**2**] 各センターは他の全てのセンターと盗聴不可能な通信路上で通信を行う．[**3**] 各センターは，[2] で得た情報から各センター固有の情報を生成し，安全な記憶領域であるメモリに記憶する．[**4**] 各ユーザは，一部のセンターとそれぞれ盗聴不可能な通信路上で通信を行う．[**5**] 各ユーザは，[4] で得た情報から各ユーザ固有の情報を生成し，メモリに記憶する．ここで，任意の t 人のユーザ ID からなるグループの集合を $\mathcal{A}(\mathcal{P}, t) = \{\mathcal{A} \mid |\mathcal{A}| = t, \mathcal{A} \subset \mathcal{P}\} = \{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{\binom{n_P}{t}}\}$ とおくと，上記のプロトコルを正しく行うことで，任意のグループ $\mathcal{A}_l = \{\mathrm{P}_{l_1}, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t}\}$ の鍵 k_l $(1 \le l \le \binom{n_P}{t})$ が，グループ内の各ユーザの固有の情報のみによって個別に生成可能となる．

この鍵事前配布方式の性能を測るための評価尺度として，次のような尺度が従来用いられている．1 つ目は，センターとユーザの記憶容量である．これは，各センター及び各ユーザに対する固有の情報を記憶するために必要なメモリ量を測る尺度として用いられる．センターの記憶容量は，センター D_i $(1 \le i \le n_D)$ 固有の情報 v_i に対応する確率変数 V_i のエントロピー $H(V_i)$ として定義され，ユーザの記憶容量は，ユーザ P_j $(1 \le j \le n_P)$ 固有の情報 u_j に対応する確率変数 U_j のエントロピー $H(U_j)$ として定義される．これらの量が小さいほど，性能の良い鍵事前配布方式となる．2 つ目は，鍵の整合性である．これは，グループ内で正しく鍵が共有できるかどうかを測る尺度として用いられ，グループ $\mathcal{A}_l = \{\mathrm{P}_{l_1}, \cdots, \mathrm{P}_{l_t}\}$ 内のユーザの固有情報 u_{l_j} と鍵 k_l に関する条件付きエントロピー $H(K_l|U_{l_j})$ $(1 \le j \le t)$ として定義される．鍵事前配布方式では，任意のグループ内の各ユーザが鍵を一意に生成できることが要求される．これは，$H(K_l|U_{l_j}) = 0$ を満たすことと等価になる．3 つ目は，鍵の安全性である．これは，攻撃者を攻撃対象となる鍵を共有するグループ以外の複数のユーザ及びセンターとし，その攻撃者が利用可能な情報を攻撃者がプロトコル内で得ることができる全ての情報と仮定している．従来の鍵事前配布方式では，センターとユーザの結託数がそれぞれ m_D, m_P 以下であるとき，攻撃対象の鍵 k_l に関する情報が全く得られないことが保証されている．これは，m_D 個以下のセンター集合 $\mathcal{X}$ と，$\mathcal{A}_l \cap \mathcal{Y} = \emptyset$ となる m_P 人以下のユーザ集合 $\mathcal{Y}$ に対し，$H(K_l|Z(\mathcal{X}, \mathcal{Y})) = H(K_l)$ を

満たすことと等価になる．ここで，$Z(\mathcal{X},\mathcal{Y})$ を攻撃者集合 $\mathcal{X}\cup\mathcal{Y}$ が利用可能な全情報に対応する確率変数とした．このようにしきい値以下の攻撃者に対して，最も強い情報量的安全性を保証する基準をしきい値型基準という．

一方，鍵事前配布方式を含む一般の暗号方式で用いられている従来の安全性基準には，次のような 2 つの基準がある．1 つ目は，上述したような結託数があるしきい値以下であるとき，最も強い情報量的安全性を保証するしきい値型基準である．2 つ目は，情報量的安全性を弱めた形の基準で，結託数があるしきい値以下であるとき，攻撃者は攻撃対象に関する情報が全く得られず，しきい値を超えると結託数の増加に従ってその情報が段階的に得られていくが，一部の情報は全く得られないことを保証する基準である．このような基準を，しきい値ランプ型基準という．しきい値ランプ型基準は，しきい値型基準を特別な場合に含む一般的な安全性基準となり，しきい値ランプ型基準に基づく暗号方式を用いることで記憶容量削減や，参加者が保有するメモリの有効活用が可能となる．従来の鍵事前配布方式において，しきい値ランプ型基準は定式化されていなかったが，この基準を用いることで他の暗号方式と同様に上記のようなメリットが期待できる．本研究では鍵事前配布方式に対して，従来と同様の攻撃者，及び攻撃者の利用可能な情報を仮定し，新たにしきい値ランプ型基準の定式化を行う．また，鍵事前配布方式に対して，従来のしきい値型基準を拡張したしきい値ランプ型基準の概念を導入する場合，ユーザの結託数の増加に従って攻撃対象の情報が段階的に洩れる基準，センターの結託数の増加に従って情報が段階的に洩れる基準，センター及びユーザの結託数の増加に従って情報が段階的に洩れる基準の 3 基準が考えられる．本研究では，これら 3 種類の基準を，従来と同様にエントロピーを用いて定式化する．

本研究のような情報量的安全性を持つ暗号方式に関する研究では，次のような研究が最も重要なアプローチとして考えられている．例えば，従来の鍵事前配布方式に関する研究では，上述したようにしきい値型基準を定式化し，その基準におけるセンターとユーザの記憶容量の理論的限界，及びその限界を達成する最適なプロトコルを示す．このように，情報量的安全性を持つ暗号方式の研究では，ある安全性基準を定式化し，その基準における参加者の記憶容量の理論的限界，及びその限界を達成する最適なプロトコルを示すことが最も重要なアプローチとして考えられている．本研究においても，従来と同様のアプローチで研究を行う．

また，従来示されているしきい値型基準におけるセンターとユーザの記憶容量の理論的限界は，任意のグループ $\mathcal{A}_j\in\mathcal{A}(\mathcal{P},t)$ に対して，鍵のエントロピーが全て等しいという仮定の下で導出されている．本研究でも，同様の仮定を置き，新たに定式化する基準に対するセンターとユーザの記憶容量を導出する．

以下，本論文の構成を示す．

第 1 章では，序論として本研究の背景及び目的について述べる．

第 2 章では，準備として，本研究で用いる情報理論の基本事項，鍵事前配布方式の定義について述べる．また，しきい値型基準としきい値ランプ型基準の定義を，代表的な暗号方式である秘密分散方式を例にとって説明する．

第 3 章では，従来研究である鍵事前配布方式に対するしきい値型基準の定式化と，その基準に対するセンターとユーザの記憶容量の理論的限界及びその限界を達成する最適なプロトコルについて述べる．

第 4 章では，まず従来の鍵事前配布方式を拡張した一般化鍵事前配布方式を提案する．従来の鍵事前配布方式では，全てのセンター間で通信を行うため，センター数 n_D に対し $O(n_D^2)$ の総通信量が必要であった．これに対し，一般化鍵事前配布方式では，総通信量が $O(n_D)$ に削減できる．次に，この一般化鍵事前配布方式に対する安全性基準として，従来と同様のしきい値型基準を次のように定式化する．$|\mathcal{X}|\le m_D, |\mathcal{Y}|\le m_P, \mathcal{Y}\cap\mathcal{A}_l=\emptyset$ を満たす任意のセンター集合 $\mathcal{X}$，ユーザ集合 $\mathcal{Y}$，及びグループ $\mathcal{A}_l$ に対して，$H(K_l|Z(\mathcal{X},\mathcal{Y}))=H(K_l)$ を満たす．ここで，$|\cdot|$ を集合の要素数とした．このように定式化した基準に対し，センターとユーザの記憶容量の理論的限界及びその限界を達成する最適なプロトコルを示す．センターとユーザの記憶容量の理論的限界は，従来の限界と一致するので，ここで提案した最適なプロトコルは，センター間の総通信量を削減しつつ，従来方式と同様の安全性を保証できる最適なプロトコルとなる．

ここで提案したプロトコルは，次のような $t+1$ 変数多項式を利用している．

$$P(x_0,x_1,\cdots,x_t)=\sum_{\substack{0\le r_0\le m_D,\\ 0\le r_1,\cdots,r_t\le m_P}} a_{r_0r_1\cdots r_t}(x_0)^{r_0}(x_1)^{r_1}\cdots(x_t)^{r_t}. \tag{3}$$

この多項式は，素数べき位数 p の有限体 $\mathbb{F}_p$ 上で定義され，$\forall b\in\mathbb{F}_p$ 及び任意の置換 $\sigma:\{1,2,\cdots,t\}\to\{1,2,\cdots,t\}$ に対して，$P(b,x_1,x_2,\cdots,x_t)=P(b,x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(t)})$ を満たす．第 5 章以降で提案する，しきい値ランプ型基準に基づく最適なプロトコルも，上記のような $t+1$ 変数多項式を利用している．また，利用する多項式の数や各多項式の次数は定式化される基準によって異なるが，鍵の整合性及び安全性を保証する仕組みは本質的に同様である．以

下で，第 4 章で提案するプロトコルが鍵の整合性と安全性を保証する仕組みの概要について述べる．

提案プロトコルにおいて，センターとユーザの ID 情報は $\mathbb{F}_p\backslash\{0\}$ の要素となり，グループ $\mathcal{A}_l = \{\mathrm{P}_{l_1}, \cdots, \mathrm{P}_{l_t}\}$ の鍵 k_l は，多項式 P 上の点 $k_l = P(0, \mathrm{P}_{l_1}, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ として定義される．また，全てのグループの鍵のエントロピーは $\log p$ となり，記憶容量の理論的限界を導出する際に置いた仮定を満たす．このプロトコルを正しく実行することで，各センター D_i $(1 \leq i \leq n_D)$ のメモリには，t 変数多項式 $P(\mathrm{D}_i, x_1, \cdots, x_t)$ が，各ユーザ P_j $(1 \leq j \leq n_P)$ のメモリには，$t-1$ 変数多項式 $P(0, \mathrm{P}_j, x_2, \cdots, x_t)$ が固有情報として記憶される．

提案プロトコルが保証する鍵の整合性の仕組みは，次のようになる．グループ $\mathcal{A}_l$ の鍵 k_l をユーザ P_{l_j} $(1 \leq j \leq t)$ が生成する場合，ユーザ P_{l_j} は固有情報 $P(0, \mathrm{P}_{l_j}, x_2, \cdots, x_t)$ と他のユーザの ID 情報 $\mathrm{P}_{l_1}, \cdots, \mathrm{P}_{l_{j-1}}, \mathrm{P}_{l_{j+1}}, \cdots, \mathrm{P}_{l_t}$ から $P(0, \mathrm{P}_{l_j}, \mathrm{P}_{l_1}, \cdots, \mathrm{P}_{l_{j-1}}, \mathrm{P}_{l_{j+1}}, \cdots, \mathrm{P}_{l_t})$ を計算する．多項式 P の性質によって，$1 \leq \forall j \leq t$ に対して，$k_l = P(0, \mathrm{P}_{l_j}, \mathrm{P}_{l_1}, \cdots, \mathrm{P}_{l_{j-1}}, \mathrm{P}_{l_{j+1}}, \cdots, \mathrm{P}_{l_t})$ となるので，任意のグループの鍵はグループ内のユーザの固有情報から一意に生成できる．したがって，提案プロトコルは鍵の整合性の基準である $H(K_l|U_{l_j}) = 0$ を満たす．

一方，提案プロトコルが保証する安全性の仕組みは，次のようになる．ここで，結託したセンター集合を $\mathcal{X} = \{\mathrm{D}_1, \cdots, \mathrm{D}_{m_D}\}$，ユーザ集合を $\mathcal{Y} = \{\mathrm{P}_1, \cdots, \mathrm{P}_{m_P}\}$ とし，攻撃対象の鍵 k_l を共有するグループを $\mathcal{A}_l = \{\mathrm{P}_{l_1}, \cdots, \mathrm{P}_{l_t}\}$ とする $(\mathcal{Y} \cap \mathcal{A}_l = \emptyset)$．このとき，攻撃者 $\mathcal{X} \cup \mathcal{Y}$ が鍵 $k_l = P(0, \mathrm{P}_{l_1}, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ を得るためには，センターの固有情報から得た m_D 個の値 $P(\mathrm{D}_i, \mathrm{P}_{l_1}, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ $(1 \leq i \leq m_D)$ から 1 変数多項式 $P(x_0, \mathrm{P}_{l_1}, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ を求める，あるいはユーザの固有情報から得た m_P 個の値 $P(0, \mathrm{P}_j, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ $(1 \leq j \leq m_P)$ から 1 変数多項式 $P(0, x_1, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ を求めることで，$k_l = P(0, \mathrm{P}_{l_1}, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ を計算する必要がある．多項式 P は x_0 に関して m_D 次であるので，攻撃者が $P(x_0, \mathrm{P}_{l_1}, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ を求めるには，未知数が $m_D + 1$ 個で方程式が m_D 本の連立方程式を解く必要があるが，方程式の数が足りないため目標の多項式を一意に定めることはできず，p 個の多項式が解の候補となってしまう．$P(0, x_1, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ についても，同様に p 個の多項式が解の候補となる．したがって，それぞれの候補から鍵を計算すると，鍵の候補もまた p 個となるので，安全性の基準 $H(K_l|Z(\mathcal{X}, \mathcal{Y})) = H(K_l) = \log p$ を満たす．

第 5 章から第 7 章では，それぞれ異なる 3 つのしきい値ランプ型基準を定式化し，各基準におけるセンターとユーザの記憶容量の理論的限界及びその限界を達成する最適なプロトコルを示す．

3 つのしきい値ランプ型基準は，それぞれ次のように定式化する．

ユーザの結託数の増加に従って秘密が段階的に洩れるしきい値ランプ型基準 (第 5 章)：

$|\mathcal{X}| \leq m_D$, $|\mathcal{Y}| \leq m_P + c_P$, $\mathcal{Y} \cap \mathcal{A}_l = \emptyset$ を満たす任意のセンター集合 $\mathcal{X}$，ユーザ集合 $\mathcal{Y}$，及びグループ $\mathcal{A}_l$ に対し，

$$H(K_l|Z(\mathcal{X}, \mathcal{Y})) = \frac{c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|)}{c_P + 1} H(K_l), \quad \varphi_{m_P}(i) = \begin{cases} 0 & \text{for } \ i \leq m_P \\ i - m_P & \text{for } \ i > m_P \end{cases} \tag{4}$$

を満たす．

センターの結託数の増加に従って秘密が段階的に洩れるしきい値ランプ型基準 (第 6 章)：

$|\mathcal{X}| \leq m_D + c_D$, $|\mathcal{Y}| \leq m_P$, $\mathcal{Y} \cap \mathcal{A}_l = \emptyset$ を満たす任意の $\mathcal{X}$，$\mathcal{Y}$，$\mathcal{A}_l$ に対して，

$$H(K_l|Z(\mathcal{X}, \mathcal{Y})) = \frac{c_D + 1 - \varphi_{m_D}(|\mathcal{X}|)}{c_D + 1} H(K_l), \quad \varphi_{m_D}(i) = \begin{cases} 0 & \text{for } \ i \leq m_D \\ i - m_D & \text{for } \ i > m_D \end{cases} \tag{5}$$

を満たす．

センター及びユーザの結託数の増加に従って秘密が段階的に洩れるしきい値ランプ型基準 (第 7 章)：

$|\mathcal{X}| \leq m_D + c_D$, $|\mathcal{Y}| \leq m_P + c_P$, $\mathcal{Y} \cap \mathcal{A}_l = \emptyset$ を満たす任意の $\mathcal{X}$，$\mathcal{Y}$，$\mathcal{A}_l$ に対して，

$$H(K_l|Z(\mathcal{X}, \mathcal{Y})) = \frac{(c_D + 1 - \varphi_{m_D}(|\mathcal{X}|))(c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|))}{(c_D + 1)(c_P + 1)} H(K_l) \tag{6}$$

を満たす．

第 4 章と第 5 章の結果は，それぞれ $c_P = 0$，$c_D = 0$ のとき第 4 章の結果と等価となるので，第 5 章と第 6 章の結果は，それぞれ第 4 章の結果を特別な場合に含む一般的な結果となる．また，第 7 章の結果は，$c_P = 0$，$c_D = 0$，$c_P = c_D = 0$ のとき，それぞれ第 5 章，第 6 章，第 4 章の結果と等価となるので，第 7 章の結果は，全ての結果を含む最も一般的な結果となる．

最後に第 8 章では，以上の結果をまとめ結論と今後の展望について述べる．

早稲田大学　博士（工学）　学位申請　研究業績書

氏 名　　吉田　隆弘　　印

（２０１０年　４月　現在）

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
1. ○論文	複数の鍵配送センターを用いたランプ型鍵事前配布方式 電子情報通信学会論文誌 A, Vol.J93-A, No.4, pp.277-288, (2010-4). 吉田隆弘, 松嶋敏泰, 今井秀樹
2. ○論文	A ramp scheme for key predistribution system against collusion of users and centers Proceeding of 2008 International Symposium on Information Theory and its Applications, (2008-12) Takahiro Yoshida, Toshiyasu Matsushima, and Hideki Imai
3. 論文	Achievable rates of random number generators for an arbitrary prescribed distribution from an arbitrary given distribution Proceedings of IEEE International Symposium on Information Theory, p.155, (2000-6) Takahiro Yoshida, Toshiyasu Matsushima, and Shigeichi Hirasawa
4. 論文	A universal code considering the codeword cost Proceedings of International Symposium on Information Theory and Its Applications, pp.165-168, (1998-10) Takahiro Yoshida, Toshiyasu Matsushima, and Shigeichi Hirasawa
5. 論文	共役勾配法における探索効率向上法に関する一考察 日本経営工学会論文誌, Vol.48, No.5, pp.257-263, (1997-12) 吉田隆弘, 後藤正幸, 俵信彦
6. 論文	KL 情報量を制約とした Resolvability 問題における達成可能条件の評価 電子情報通信学会論文誌 A, Vol.J93-A, No.3, pp.216-221, (2010-3) 野村亮, 吉田隆弘, 松嶋敏泰
7. 論文	Bounds on the number of users for random 2-secure codes Proceedings of 18th Symposium on Applied algebra, Algebraic algorithms and Error Correcting Codes (AAECC-18), Lecture Notes In Computer Science Vol. 5527, pp.239-242, (2009-6) Manabu Hagiwara, Takahiro Yoshida, and Hideki Imai
8. 講演	相互通信可能な情報源符号化に関する一研究 第 29 回情報理論とその応用シンポジウム予稿集, pp.355-358, (2006-12) 吉田隆弘, 松嶋敏泰, 平澤茂一
9. 講演	ID 情報に基づくランプ型分散鍵配送方式について 第 27 回情報理論とその応用シンポジウム予稿集, pp.327-360, (2004-12) 吉田隆弘, 松嶋敏泰, 平澤茂一

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
10. 講演	ランプ型鍵配送方式について 電子情報通信学会技術報告，ISEC2004-11，pp. 69-74，(2004-5) 吉田隆弘，松嶋敏泰，平澤茂一
11. 講演	多端子情報源符号化に基づいた分散協調問題の定式化について 第 25 回情報理論とその応用シンポジウム予稿集，pp. 663-666，(2002-12) 吉田隆弘，松嶋敏泰，平澤茂一
12. 講演	情報システム演習の実績報告 2002 PC カンファレンス論文集，(2002-8) 吉田隆弘，小林学，平澤茂一
13. 講演	多端子情報理論に基づく分散協調問題について 第 24 回情報理論とその応用シンポジウム予稿集，pp. 367-370，(2001-12) 吉田隆弘，松嶋敏泰，平澤茂一
14. 講演	多端子モデルに基づく分散協調問題の定式化について 電子情報通信学会技術報告，IT2001-17，pp. 37-42，(2001-7) 吉田隆弘，松嶋敏泰，平澤茂一
15. 講演	コスト付き情報源符号化定理について 第 22 回情報理論とその応用シンポジウム予稿集，pp. 57-60，(1999-12) 吉田隆弘，松嶋敏泰，平澤茂一
16. 講演	符号語コストを考慮した情報源符号化について 日本経営工学会 平成 10 年度春季大会予稿集，(1998-5) 吉田隆弘，後藤正幸，俵信彦
17. 講演	共役勾配法における探索効率向上法について 日本経営工学会 平成 8 年度春季大会予稿集，(1996-5) 吉田隆弘，後藤正幸，俵信彦
18. 講演	電波伝搬の特性を利用した鍵共有方式の情報量的安全性評価 2010 年暗号と情報セキュリティシンポジウム(SCIS2010)予稿集，(2010-1) 松永雄斗，吉田隆弘，萩原学，古原和邦，今井秀樹
19. 講演	情報理論的に安全なリング署名方式 2010 年暗号と情報セキュリティシンポジウム(SCIS2010)予稿集，(2010-1) 千葉慎平，吉田隆弘，今井秀樹
20. 講演	電力解析攻撃の体系的な分類と比較について 2010 年暗号と情報セキュリティシンポジウム(SCIS2010)予稿集，(2010-1) 野口正俊，堀洋平，吉田隆弘，今井秀樹

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
21. 講演	情報理論的に安全な鍵無効化機能付きメッセージ秘匿・認証方式 電子情報通信学会技術報告, IT2008-90, ISEC2008-148, WBS2008-103, pp.301-306, (2009-3) 千葉慎平, 吉田隆弘, ナッタポンアッタラパドゥン, 今井秀樹
22. 講演	電波の相反性を用いた鍵共有方式における情報量的安全な誤り訂正方式 2009 年暗号と情報セキュリティシンポジウム(SCIS2009)予稿集, (2009-1) 松永雄斗, 萩原学, 吉田隆弘, 古原和邦, 今井秀樹
23. 講演	Set delegation 機能付き階層的 ID ベース暗号方式 2009 年暗号と情報セキュリティシンポジウム(SCIS2009)予稿集, (2009-1) 吉田雅広, ナッタポンアッタラパドゥン, 吉田隆弘, 今井秀樹
24. 講演	ノートパソコンへのパスワード入力過程ののぞき見耐性について 2009 年暗号と情報セキュリティシンポジウム(SCIS2009)予稿集, (2009-1) 佐古武志, 吉田隆弘, 古原和邦, 今井秀樹
25. 講演	積符号化を利用した階層的な秘密分散法の検討 2008 年暗号と情報セキュリティシンポジウム(SCIS2008)予稿集, (2008-1) 川島千種, 吉田隆弘, 松嶋智子
26. 講演	多重符号化を利用した階層的な秘密分散法の検討 電子情報通信学会技術報告, ISEC2007-76, pp.17-23, (2007-9) 川島千種, 吉田隆弘, 松嶋智子
27. 講演	初学者に対する e-learning の試み 平成 16 年度情報処理教育研究集会, (2004-11) 石田則道, 犬伏雄一, 金榮基, 黒澤敦子, 時井聰, 山崎由美子, 吉田隆弘, 和高慶夫, 山田正行, 山内美恵子
28. 講演	ポアソン分布に従う非定常な時系列の予測に関する一考察 電子情報通信学会技術報告, IT2003-39, pp.93-97, (2003-7) 岩田錦弥, 吉田隆弘, 松嶋敏泰
29. 講演	誤り訂正符号を用いた直交計画の構成法に関する一考察 第 25 回情報理論とその応用シンポジウム予稿集, pp.663-666, (2002-12) 斉藤友彦, 吉田隆弘, 松嶋敏泰
30. 講演	ベイズ決定理論に基づくロバストなパターン認識に関する一考察 第 25 回情報理論とその応用シンポジウム予稿集, pp.283-286, (2002-12) 桑田修平, 吉田隆弘, 松嶋敏泰
31. 講演	状態空間モデルを用いた時系列解析に関する一考察 ーモンテカルロフィルタにおけるリサンプリング方法についてー 日本経営工学会 平成 13 年度秋季研究大会予稿集, pp.218-219, (2001-11) 桑田修平, 吉田隆弘, 松嶋敏泰
32. 講演	不確実な知識の演繹推論における二項述語への拡張に関する一考察 人工知能学会全国大会（第 14 回）論文集, (2000-7) 水野洋, 吉田隆弘, 松嶋敏泰