早稲田大学大学院 基幹理工学研究科

博士論文審査報告書

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
YOSHIDA	Takahiro

2010 年　7 月

インターネット環境等で様々な情報通信サービスを提供するためには，通信内容の守秘性を確保する技術が必要不可欠となる．守秘性を確保するための重要な暗号方式の１つに鍵事前配布方式がある．鍵事前配布方式は，利用者間で暗号通信を行う際に使用する鍵と呼ばれる情報を，事前に共有するための方式である．鍵事前配布方式の参加者は，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いる．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 D_j, $1 \leq j \leq n_D$ は独立に，秘密の情報を生成する．
2. 各センター D_j, $1 \leq j \leq n_D$ は他の全てのセンター $\mathrm{D}_{j'}$, $1 \leq j' \leq n_D$ と安全な通信路上で通信を行う．
3. 各センター D_j, $1 \leq j \leq n_D$ は，2. で得た情報から各センター固有の情報 v_j をそれぞれ生成し，安全な記憶領域であるメモリに記憶する．
4. 各ユーザ P_i, $1 \leq i \leq n_P$ は，一部のセンター D_{i_1},$\cdots$,D_{i_L} を選択し，選択されたセンターは，記憶している情報 v_{i_l},$1 \leq l \leq L$ から，ユーザへの送信情報 $u_{i_l,i}$ をそれぞれ安全な通信路上で通信を行う．
5. 各ユーザ P_i, $1 \leq i \leq n_P$ は，4. で得た情報 $u_{i_1,i}$,$\cdots$,$u_{i_L,i}$ から各ユーザ固有の情報 u_i を生成し，メモリに記憶する．
6. 各ユーザ P_i, $1 \leq i \leq n_P$ は，記憶している情報 u_i から任意の $t-1$ 人のユーザとの鍵 k を生成する．

鍵事前配布方式では，鍵を第 3 者に知られないように利用者間で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の概念は，情報量的安全性と計算量的安全性に大別できる．これらの安全性概念は，暗号方式へ攻撃する者 (以下，攻撃者と呼ぶ) が目標を達成するために実行できる計算時間や計算資源等の攻撃能力に関する仮定の置き方によって分類できる．攻撃能力に対して何も仮定を置かずに定義される安全性を，情報量的安全性という．情報量的安全性は，エントロピー等の情報量のみによって定義されるため，無限の計算能力を持つ攻撃者に対しても保証できる安全性となる．一方，計算量的安全性は，攻撃能力に現実的な制限を設けたときに定義される安全性なので，この安全性が満たされていても，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という欠点がある．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持つことになり，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．本論文では，高度な安全性である情報量的安全性を有する鍵事前配布方式を研究の対象としている．

ここで，センターの ID 情報の集合とユーザの ID 情報の集合をそれぞれ，$\mathcal{D} = \{\mathrm{D}_1, \cdots, \mathrm{D}_{n_D}\}$, $\mathcal{P} = \{\mathrm{P}_1, \cdots, \mathrm{P}_{n_P}\}$ とし，任意の t 人のユーザの ID 情報からなる集合 $\mathcal{A} \subset \mathcal{P}$ が共有する鍵を k とする．鍵事前配布方式に要求する従来の安全性は，攻撃者であるセンター $\mathcal{X} \subset \mathcal{D}$ とユーザ $\mathcal{Y} \subset \mathcal{P}$ の数がそれぞれ m_D, m_P 以下であるとき，攻撃者であるユーザが属していない任意のグループ $\mathcal{A}$ の鍵 k に関する情報が全く得られないことを保証する．すなわち，$|\mathcal{X}| \leq m_D$, $|\mathcal{Y}| \leq m_P$, $\mathcal{Y} \cap \mathcal{A} = \emptyset$ を満たす任意の攻撃者 $\mathcal{X} \subset \mathcal{D}$, $\mathcal{Y} \subset \mathcal{P}$，及びグループ $\mathcal{A}$ に対し，$H(K \mid Z(\mathcal{X}, \mathcal{Y})) = H(K)$ を満たす．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，K を鍵 k に対応する確率変数とした．また，$H(\cdot)$ と $H(\cdot \mid \cdot)$ は，エントロピー及び条件付きエントロピーである．

情報量的安全性を有する鍵事前配布方式に関する研究では，上記の安全性を満たす下で，効率の良い鍵事前配布方式を実現することが重要な目的とされている．この効率を測る評価基準として，従来は利用者間の通信量やセンターとユーザの記憶容量が用いられている．従来研究では，センターの記憶容量を各センターの記憶情報 v_j, $1 \leq j \leq n_D$ に対応する確率変数 V_j のエントロピー $H(V_j)$，ユーザの記憶容量を各ユーザの記憶情報 u_i, $1 \leq i \leq n_P$ に対応する確率変数 U_i のエントロピー $H(U_i)$ と定義しており，これらの理論的限界が導出されている．また，その限界を達成する最適な構成法も提案されている．

本論文では，従来の安全性を一般化した安全性を提案し，従来と同様にセンターとユーザの記憶容量の理論的限界を導出し，その限界を達成する構成法を提案している．また，従来の鍵事前配布方式のセンター間の通信量を削減する新たな鍵事前配布方式も提案している．

第 4 章では，まず従来の鍵事前配布方式におけるセンター間の総通信量を削減する新たな鍵事前配布方式を提案し，従来と同様の安全性を満たす下での記憶容量の理論的限界を導出し，その限界を達成する最適な構成法を提案している．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が，本論文で提案した鍵事前配布方式では，総通信量が $O(n_D)$ に削減できることが示されている．したがって，提案方式は従来方式と同じ安全性と記憶容量を達成し，かつセンター間の総通信量を大幅に削減できるため，実用的価値が高い．

また，上述したように従来の鍵事前配布方式の安全性は，攻撃者であるセンター $\mathcal{X}$ とユーザ $\mathcal{Y}$ の数がそれぞれ m_D, m_P 以下であるとき，攻撃対象とする鍵の情報が全く得られないことを保証するが，m_D, m_P を超える攻撃者数の場合は，何の安全性も保証しない．本論文の第 5 章から第 7 章では，鍵の情報が攻撃者数の増加に伴い段階的に得られるという性質を新たに導入し，各章で次のように一般化した安全性を定義している．

第 5 章： 任意のしきい値 m_D, m_P, c_P に対して，センターとユーザの攻撃者数がそれぞれ m_D, m_P 以下であるとき，攻撃者であるユーザが属していない任意のグループの鍵に関する情報が全く得られず，ユーザの攻撃者数が $m_P + 1$ 以上 $m_P + c_P$ 以下，かつセンターの攻撃者数が m_D 以下の場合には，ユーザの攻撃者数が大きくなるにつれて段階的に情報が得られていくことを保証する，すなわち，$|\mathcal{X}| \leq m_D$, $|\mathcal{Y}| \leq m_P + c_P$, $\mathcal{Y} \cap \mathcal{A} = \emptyset$ を満たす任意の攻撃者 $\mathcal{X} \subset \mathcal{D}$, $\mathcal{Y} \subset \mathcal{P}$，及びグループ $\mathcal{A}$ に対し，

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

を満たす．

第 6 章： 任意のしきい値 m_D, c_D, m_P に対して，センターとユーザの攻撃者数がそれぞれ m_D, m_P 以下であるとき，攻撃者であるユーザが属していない任意のグループの鍵に関する情報が全く得られず，センターの攻撃者数が m_D 以上 $m_D + c_D$ 以下，かつユーザの攻撃者数が m_P 以下の場合には，センターの攻撃者数が大きくなるにつれて段階的に情報が得られていくことを保証する．

第 7 章： 任意のしきい値 m_D, c_D, m_P，c_P に対して，センターとユーザの攻撃者数がそれぞれ m_D, m_P 以下であるとき，攻撃者であるユーザが属していない任意のグループの鍵に関する情報が全く得られず，ユーザの攻撃者数が $m_P + 1$ 以上 $m_P + c_P$ 以下，かつセンターの攻撃者数が $m_D + 1$ 以上 $m_D + c_D$ 以下の場合には，ユーザとセンターの攻撃者数が大きくなるにつれて段階的に情報が得られていくことを保証する，すなわち，第 5 章と第 6 章を組み合わせた安全性の定義となる．

本論文では，従来研究と同様のアプローチをとるので，上記のような安全性を満たすもとで，センターとユーザの記憶容量の理論的限界を導出している．例えば，第 5 章では，提案した安全性に対する理論的限界が，それぞれ

$$H(V_j) \geq \sum_{\zeta=0}^{c_P} \binom{m_P+t+\zeta}{t} \frac{H(K)}{c_P+1},\ 1 \leq j \leq n_D, \tag{1}$$

$$H(U_i) \geq \sum_{\zeta=0}^{c_P} \binom{m_P+t-1+\zeta}{t-1} \frac{H(K)}{c_P+1},\ 1 \leq i \leq n_P \tag{2}$$

となることを示している．

更に，本論文では，導出した記憶容量の理論的限界を達成する最適な構成法を提案している．例えば，第 4 章で提案した構成法では，次のような $t+1$ 変数多項式を利用している．

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

この多項式は，素数べき位数 q の有限体 $\mathbb{F}_q$ 上で定義され，任意の $b \in \mathbb{F}_q$ 及び任意の置換 $\sigma : \{1, 2, \cdots, t\} \to \{1, 2, \cdots, t\}$ に対して，$Q(b, x_1, x_2, \cdots, x_t) = Q(b, x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(t)})$ を満たす．提案構成法において，センターとユーザの ID 情報は $\mathbb{F}_q \backslash \{0\}$ 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，多項式の値 $k_l = Q(0, \mathrm{P}_{l_1}, \mathrm{P}_{l_2}, \cdots, \mathrm{P}_{l_t})$ として定義され，多項式 Q が上記のような対称性を持つことにより鍵の共有が保証できる，また，多項式が x_0 に関して m_D 次で x_1,$\cdots$,x_t に関して m_P 次であることから，要求する安全性が満たされる．第 5 章以降で提案する構成法も，上記のような $t+1$ 変数多項式を利用しているが，利用する多項式の数や各多項式の次数は各章で提案している構成法によって異なるが，それぞれの安全性を満たす仕組みは本質的に同様である．

第 5 章と第 6 章で示した安全性，理論的限界，及び構成法は，それぞれ $c_P = 0$，$c_D = 0$ のとき第 4 章で示した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ことが示されている．また，第 7 章で示した安全性，理論的限界，及び構成法は，$c_D = 0$，$c_P = 0$，$c_P = c_D = 0$ のとき，それぞれ第 5 章，第 6 章，第 4 章で示した結果と等価となるので，第 7 章で示した結果は，全ての結果を含む最も一般的な結果となることが示されている．

また本論文では，第 5 章から第 7 章で提案した各鍵事前配布方式の安全性を弱めることで，従来の方式における記憶容量を削減することができ，利用者が保有するメモリ等のリソースに制限が設けられている場合でも，リソースの有効な活用が可能となり，柔軟な設計ができることが述べられている．

以上を総括すると，本論文は情報量的安全性を有する鍵事前配布方式に対して，センター間の通信量を削減した新たな方式の提案と，安全性の一般化を行い，その安全性を満たす下での各記憶容量の理論的限界の導出，及びその理論的限界を達成する構成法の提案を行っている．これらの結果は実用的かつ理論的な価値があり，重要な成果であると言える．よって本論文は博士（工学）の学位論文として価値のあるものと認める．

2010 年 7 月

審査員（主査）早稲田大学教授　博士（工学）早稲田大学　松嶋 敏泰

早稲田大学教授　工学博士（早稲田大学）　大石 進一

早稲田大学名誉教授　工学博士（大阪大学）　平澤 茂一