時刻情報で制御する情報理論的に安全な鍵共有方式

渡邉 洋平　　清藤 武暢　　四方 順司

横浜国立大学大学院環境情報学府/研究院
240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7

youhei@mlab.jks.ynu.ac.jp, takenobu.seito@ynu.ac.jp, shikata@ynu.ac.jp

あらまし これまでに時刻で復号を制御する暗号化方式として、Timed-Release Encryption (TRE) が知られている。本稿では、情報理論的安全性に基づき、時刻情報を利用して鍵共有を行うための Timed-Release Key-Agreement プロトコルを提案する。具体的には、そのモデル及び安全性の定式化を示す。また、利用者の鍵サイズのタイトな下界と最適構成法も示す。

Information-Theoretically Secure Timed-Release Key-Agreement

Yohei Watanabe　　Takenobu Seito　　Junji Shikata

Graduate School of Environment and Information Sciences,
Yokohama National University,
79-7, Tokiwadai, Hodogaya, Yokohama, Kanagawa 240-8501, Japan

youhei@mlab.jks.ynu.ac.jp, takenobu.seito@ynu.ac.jp, shikata@ynu.ac.jp

Abstract The timed-release encryption (TRE) scheme enables a sender to secretly send a message to a receiver so that even the legitimate receiver knows it only after the time which the sender has specified beforehand. In this paper, we study information-theoretically secure timed-release key-agreement (TR-KA). Specifically, we propose a model and security definition of information-theoretically secure TR-KA, and we show tight lower bounds of users' keys and the optimal construction of TR-KA.

1　はじめに

これまでに多くの暗号技術が提案されているが, それらの安全性は主に計算量的安全性あるいは情報理論的安全性に基づいて保証されている．計算量的安全性は素因数分解問題や離散対数問題などの計算量的な問題を解くことが難しいという仮定に基づいて安全性を保証し，情報理論的安全性は計算量的な仮定を用いずに確率論や情報理論に基づいてその安全性を保証する．情報理論的安全性に基づく暗号技術は計算量的安全性に基づく暗号技術に比べて一般的に必要な記憶容量が多く，また全てのエンティティが自身の鍵を秘密に保持する必要がある．しかし計算量的な仮定を用いないために攻撃者の計算能力に関わらず定量的なセキュリティを長期間保証できるという利点がある．計算機の計算能力の向上やアルゴリズムの進歩を考えると，情報理論的安全性に基づく暗号技術の有用性が増すことが期待され，これらについて議論する意義は大きい．

鍵共有プロトコルとは基礎的な暗号プロトコルの１つである．これまでにも，計算量的安全

性に基づいた方式と情報理論的安全性に基づいた方式，そのどちらについても数多くの論文が発表されている（例えば, [1]-[5], [8]）.

暗号技術の 1 つに，特定の時刻以降にのみ復号可能な暗号化方式として Timed-Release Encryption (TRE) が知られている．これは 1993 年に May によってその概念が提案され [6]，その後 Rivest ら [7] によって時刻情報を鍵として復号するモデルの TRE が提案された．TRE は，正当な受信者であっても送信者に指定された時刻までは復号を行うことができないという特徴を持つ．TRE が Rivest らによって体系づけられてから，計算量的安全性に基づいたものについて今日まで多くの議論が行われてきた．しかし，これまでに情報理論的安全性に基づく TRE は提案されていない．ここで, 本質的に, 情報理論的に安全な暗号化方式は，情報理論的に安全な鍵共有方式と one-time pad を組み合わせることで実現できることに着目すると, “ Timed-Release ”機能を有する情報理論的に安全な鍵共有方式が存在すれば，情報理論的に安全な TRE を構成できると考えられる．したがって, 本稿では，情報理論的に安全な Timed-Release 鍵共有方式のテーマを扱う．情報理論的に安全な TRE については本稿のフルバージョンを参照されたい.

本稿の以下の節では，情報理論的安全性に基づいて，Timed-Relaese Key-Agreement (TR-KA) を提案する．2 節でそのモデル，安全性の定式化を行い，3 節で利用者の鍵サイズのタイトな下界を示す．4 節で TR-KA に対する最適構成法を示した後，5 節でまとめと今後の研究について述べる．

2　モデルと安全性定義

本節では，情報理論的安全性を有する TR-KA のモデル，安全性定義を示す.

2.1　モデル

本稿では TI モデルを考える．TI モデルとは，信頼できる第三者機関の存在を仮定するモデルである．TI はプロトコルの開始時のみ起動し，各エンティティに鍵などの情報を配送し，その後は登場しないエンティティである．

提案するモデルでは，TI と n 人の利用者集合 $U := \{U_1, U_2, \ldots, U_n\}$(以下，ID の集合を同一視する)，Time Server と呼ばれる時刻情報を管理する第三者機関が登場する．

まず, モデルの概要を述べる．TR-KA は，n 人の中の任意の二者間で鍵共有を行うプロトコルである．二者のうち一方の利用者は鍵を共有したい時刻を指定したうえで先に共有鍵を得ることができ，もう一方の利用者は指定時刻になると鍵を得ることができる．まず，プロトコルの開始時に TI は各利用者の秘密鍵と Time Server のマスター秘密鍵を生成し，それを安全な通信路を用いて各エンティティに配送した後，自身のメモリから削除する．時刻を指定する側の利用者 U_{i_1} は，自身の秘密と鍵を共有したい利用者 U_{i_2} の ID 情報を用い，共有可能時刻を指定して共有鍵を生成，また指定時刻を U_{i_2} に伝える．Time Server は，各時刻の始めにマスター鍵を用いてその時刻に対応した時刻情報を生成し，全てのエンティティに一斉送信する．そして U_{i_2} は，Time Server から送信された指定時刻の時刻情報，自身の秘密鍵と U_{i_1} の ID 情報を用い，鍵を共有することができる．形式的な TR-KA の定義は次の通りである．

定義 1 Timed-release key-agreement (TR-KA) プロトコル Π は，TI と $U_1, U_2, \ldots, U_n$，Time Server の $n+2$ のエンティティ，4 つのアルゴリズム (*Setup*, *Ext*, *KeyGen*, *KeyDer*)，5 つの空間 $\mathcal{CK}, \mathcal{UK}, \mathcal{MK}, \mathcal{T}, \mathcal{TI}$ からなる．*Setup* アルゴリズムは確率的，*Ext*, *KeyGen*, *KeyDer* アルゴリズムは決定的アルゴリズムであり，すべての空間は有限である．加えて，Π は次に示す 4 つのフェーズを実行する．

記法

- エンティティ: TI は信頼できる第三者機関，U_i $(1 \leq i \leq n)$ は利用者，そして Time Server は時刻情報を管理する第三者機関である．さらに $U := \{U_1, U_2, \ldots, U_n\}$ を利用者集合とする．

- 空間: $\mathcal{CK}$ は共有鍵の集合であり，$\mathcal{MK}$ はマスター鍵の集合である．$\mathcal{T} := \{1,2,\ldots,\tau\}$ を時刻の集合とする．$\mathcal{TI}$ は時刻情報の集合である．また $\mathcal{UK}_i$ は U_i の秘密鍵の集合であり確率分布 P_{UK_i} をもつ．$\mathcal{UK}_i := \mathcal{UK}_i^{(S)} \times \mathcal{UK}_i^{(R)}$ とおく．ただし，$\mathcal{UK}_i^{(S)}$ は U_i の共有鍵生成用の秘密鍵の集合であり，$\mathcal{UK}_i^{(R)}$ は U_i の共有鍵導出用の秘密鍵の集合である．ここで $\mathcal{UK} := \mathcal{UK}_1 \cup \mathcal{UK}_2 \cup \ldots \cup \mathcal{UK}_n$ とおく．
- アルゴリズム: $Setup$ はセキュリティパラメータ 1^k を入力とし，各利用者の秘密鍵と Time Server のマスター秘密鍵を出力する鍵生成アルゴリズムである．$Ext : \mathcal{MK} \times \mathcal{T} \to \mathcal{TI}$ は時刻情報生成アルゴリズムである．$KeyGen : \mathcal{UK} \times \mathcal{T} \times \mathcal{U} \to \mathcal{CK}$ は共有鍵生成アルゴリズム，$KeyDer : \mathcal{UK} \times \mathcal{TI} \times \mathcal{U} \to \mathcal{CK}$ は共有鍵導出アルゴリズムである．

鍵生成・鍵配布フェーズ プロトコルの開始時に，TI は $Setup$ を実行し，Time Server のマスター鍵 $mk^* \in \mathcal{MK}$ と各利用者の秘密鍵 $uk_i \in \mathcal{UK}_i$ $(i = 1,2,\ldots,n)$ を生成する．uk_i は $uk_i^{(S)} \in \mathcal{UK}_i^{(S)}$ と $uk_i^{(R)} \in \mathcal{UK}_i^{(R)}$ の 2 つから構成されるものとする．これらはそれぞれ共有鍵の生成時，導出時に使用する．TI はこれらの鍵をそれぞれ対応するエンティティに安全な通信路を用いて配布した後，自身のメモリから消去し，各エンティティは自身の鍵を秘密に保持する．

時刻情報生成フェーズ 時刻 t の時刻情報を生成するとき，Time Server は自身のマスター鍵 mk^* と時刻 $t \in \mathcal{T}$ を用いて，時刻情報 $mk_t = Ext(mk^*, t)$ を得る．その後 Time Server は改ざん不可な通信路を用いて時刻情報を全てのエンティティに一斉送信する．

共有鍵生成フェーズ 時刻 t に U_{i_2} と鍵を共有したい U_{i_1} は，自身の生成用秘密鍵 $uk_{i_1}^{(S)}$，共有可能時刻 t，U_{i_2} の ID 情報を用いて，共有鍵 $ck_{i_1,i_2}^{(t)} = KeyGen(uk_{i_1}^{(S)}, t, U_{i_2})$ を得る．U_{i_1} は改ざん不可な通信路を用いて U_{i_2} に指定時刻 t を伝えておく．

共有鍵導出フェーズ U_{i_2} は，指定時刻 t になると放送される時刻情報 mk_t と自身の導出用秘密鍵 $uk_{i_2}^{(R)}$，U_{i_1} の ID 情報を用いて，$ck_{i_1,i_2}^{(t)\prime} = KeyDer(uk_{i_2}^{(R)}, mk_t, U_{i_1})$ を得る．

上記の TR-KA のモデルでは，以下の条件を満たすものとする．任意の生成可能な $t \in \mathcal{T}$，$i_1, i_2 \in \{1,2,\ldots,n\}$，$uk_{i_1}^{(S)} \in \mathcal{UK}_{i_1}^{(S)}$，$uk_{i_2}^{(R)} \in \mathcal{UK}_{i_2}^{(R)}$，$mk_t \in \mathcal{MK}_t$ に対して，$KeyGen(uk_{i_1}^{(S)}, t, U_{i_2}) = KeyDer(uk_{i_2}^{(R)}, mk_t, U_{i_1})$．これは，TR-KA を正しく実行すれば，任意の U_{i_1} と U_{i_2} が指定時刻 t で正しく鍵を共有できることを意味する．

2.2 安全性

ここでは，TR-KA の安全性について述べる．まず，記法として次のように定義する．τ を時刻情報の最大放送回数，$\omega(< n)$ を利用者の最大結託人数とする．任意の集合 $\mathcal{Z}$，任意の非負整数 z に対して $\mathcal{P}(\mathcal{Z}, z) := \{Z \subset \mathcal{Z} \mid |Z| \leq z\}$ とする．また，結託者の集合を $W := \{U_{i_1}, U_{i_2}, \ldots, U_{i_\omega}\} \in \mathcal{P}(\mathcal{U}, \omega)$ とし，$\mathcal{UK}_W^{(S)} := \mathcal{UK}_{i_1}^{(S)} \times \mathcal{UK}_{i_2}^{(S)} \times \ldots \times \mathcal{UK}_{i_\omega}^{(S)}$ を W の持つ生成用秘密鍵の集合，$\mathcal{UK}_W^{(R)} := \mathcal{UK}_{i_1}^{(R)} \times \mathcal{UK}_{i_2}^{(R)} \times \ldots \times \mathcal{UK}_{i_\omega}^{(R)}$ を W の持つ導出用秘密鍵の集合とする．さらに，$\mathcal{CK}_{i_1,i_2}^{(t)}$ を U_{i_1} と U_{i_2} の間での時刻 t で共有可能な共有鍵の集合とする．$CK_{i_1,i_2}^{(t)}$, MK, $UK_W^{(S)}, UK_W^{(R)}, MK_1, \ldots, MK_\tau$ を，それぞれ $\mathcal{CK}_{i_1,i_2}^{(t)}, \mathcal{MK}, \mathcal{UK}_W^{(S)}, \mathcal{UK}_W^{(R)}, \mathcal{MK}_1, \ldots, \mathcal{MK}_\tau$ に値をとる確率変数とする．

TR-KA では，利用者の結託攻撃と Time Server による攻撃を考える．さらに，時刻を指定される側の利用者 (以下，受信者と呼ぶ) が利用者結託に含まれる場合と含まれない場合を考える．

定義 2 (安全性) TR-KA Π が以下を満たすとき，Π は (n, ω, τ)-secure という．

1. **Time Server に対する安全性.** Time Server の持つマスター鍵 mk^* から共有鍵に関する情報が何も得られない．すなわち，任意の $U_{i_1}, U_{i_2} \in U$, 任意の時刻 $t \in \mathcal{T}$ に対して，

$$H(CK_{i_1,i_2}^{(t)} | MK^*) = H(CK_{i_1,i_2}^{(t)}).$$

2. **受信者を含まない結託に対する安全性.** 受信者を含まない利用者が ω 人まで結託しても，ターゲットの共有鍵に関する情報が何も得られない．すなわち，任意の U_{i_1}, $U_{i_2} \in U$ かつ $U_{i_1}, U_{i_2} \notin W$，任意の時刻 $t \in \mathcal{T}$ に対して，

$$H(CK^{(t)}_{i_1,i_2}|UK^{(S)}_W, UK^{(R)}_W, MK_1, \ldots, MK_\tau) = H(CK^{(t)}_{i_1,i_2}).$$

3. **受信者を含む結託に対する安全性.** 利用者が ω 人まで結託し，かつ受信者が結託に含まれていても，共有鍵に関する情報が何も得られない．すなわち，任意の U_{i_1}, $U_{i_2} \in U$, $U_{i_1} \notin W$, $U_{i_2} \in W$，任意の時刻 $t \in \mathcal{T}$ に対して，

$$H(CK^{(t)}_{i_1,i_2}|UK^{(S)}_W, UK^{(R)}_W, MK_1, \ldots, MK_{t-1}, MK_{t+1}, \ldots, MK_\tau) = H(CK^{(t)}_{i_1,i_2}).$$

3 鍵サイズの下界

本節では TR-KA における利用者の鍵サイズのタイトな下界を示す.

定理 1 *(n, ω, τ)-secure TR-KA* において, 共有鍵のエントロピーが全て等しいとする．すなわち, 任意の i_1,$i_2 \in \{1,2,\ldots,n\}$, $t \in \mathcal{T}$ に対して，$H(CK) = H(CK^{(t)}_{i_1,i_2})$ とする．このとき,

(i) $H(UK^{(R)}_i) \geq (\omega+1)H(CK)$,
(ii) $H(UK^{(S)}_i) \geq \tau(\omega+1)H(CK)$,
(iii) $H(MK_i) \geq (\omega+1)H(CK)$,
(iv) $H(MK^*) \geq \tau(\omega+1)H(CK)$.

証明は以下の補題から従う.

補題 1 r を自然数とし, $|Z| = \omega$, $Z \cap X = \emptyset$, $Z \cap Y_l \neq \emptyset$, $|X| = |Y_l| = 2$ $(l = 1,2,\ldots,r)$ をみたす集合 X,Y_1,$\ldots$,Y_r,$Z \subseteq \{1,2,\ldots,n\}$ をとる．このとき，(n, ω, τ)-*secure TR-KA* において, 任意の $1,\ldots,t \in \mathcal{T}$ に対して，$H(CK^{(t)}_X \mid CK^{(1)}_{Y_1}, \ldots, CK^{(1)}_{Y_r}, \ldots, CK^{(t)}_{Y_1}, \ldots, CK^{(t)}_{Y_r}, CK^{(1)}_X, \ldots, CK^{(t-1)}_X) = H(CK^{(t)}_X)$.

証明: 定義 2 の 3 番目の条件から，$H(CK^{(t)}_X \mid CK^{(1)}_{Y_1}, \ldots, CK^{(1)}_{Y_r}, \ldots, CK^{(t)}_{Y_1}, \ldots, CK^{(t)}_{Y_r}, CK^{(1)}_X, \ldots, CK^{(t-1)}_X) = H(CK^{(t)}_X \mid CK^{(1)}_{Y_1}, \ldots, CK^{(1)}_{Y_r}, \ldots, CK^{(t)}_{Y_1}, \ldots, CK^{(t)}_{Y_r})$．さらに，$H(CK^{(t)}_X \mid CK^{(1)}_{Y_1}, \ldots, CK^{(1)}_{Y_r}, \ldots, CK^{(t)}_{Y_1}, \ldots, CK^{(t)}_{Y_r}) = H(CK^{(t)}_X)$ が成り立つことは [3] の補題 4.1 と同様の流れで証明できる．□

補題 2 任意の $i \in \{1,2,\ldots,n\}$ に対して，$H(UK^{(R)}_i) \geq (\omega+1)H(CK)$.

証明: $i \notin B$ となるような利用者の集合を $B := \{l_1, \ldots, l_{\omega+1}\}$ とおく．また $A := \{(i,l_{\omega+1})\}$, $D_k := \{(i,l_k)\}$ $(1 \leq k \leq \omega)$ とする．このとき,

$$\begin{aligned}
&H(UK^{(R)}_i)\\
&\geq H(UK^{(R)}_i \mid MK_t)\\
&\geq I(CK^{(t)}_A, CK^{(t)}_{D_1}, \ldots, CK^{(t)}_{D_k}; UK^{(R)}_i \mid MK_t)\\
&= H(CK^{(t)}_A, CK^{(t)}_{D_1}, \ldots, CK^{(t)}_{D_k} \mid MK_t)\\
&\quad - H(CK^{(t)}_A, CK^{(t)}_{D_1}, \ldots, CK^{(t)}_{D_k} \mid MK_t, UK^{(R)}_i)\\
&= H(CK^{(t)}_A, CK^{(t)}_{D_1}, \ldots, CK^{(t)}_{D_k} \mid MK_t)\\
&= H(CK^{(t)}_A \mid MK_t) + H(CK^{(t)}_{D_1} \mid MK_t) + \\
&\qquad \cdots + H(CK^{(t)}_{D_k} \mid MK_t) \quad (1)\\
&= (\omega+1)H(CK).
\end{aligned}$$

最後の等号は定義 2 から従い，(1) は本質的に補題 1 から従う．□

補題 3 任意の $i \in \{1,2,\ldots,n\}$ において，$H(UK^{(S)}_i) \geq \tau(\omega+1)H(CK)$ である.

証明: $i \notin B$ となるような利用者の集合を $B := \{l_1, \ldots, l_{\omega+1}\}$ とおく．また $A := \{(i,l_{\omega+1})\}$, $D_k := \{(i,l_k)\}$ $(1 \leq k \leq \omega)$ とし，$C^{(t)} := \{CK^{(t)}_A, CK^{(t)}_{D_1}, \ldots, CK^{(t)}_{D_k}\}$ とする．このとき,

$$\begin{aligned}
&H(UK^{(S)}_i)\\
&\geq I(C^{(1)}, \ldots, C^{(\tau)}; UK^{(S)}_i)\\
&= H(C^{(1)}, \ldots, C^{(\tau)}) - H(C^{(1)}, \ldots, C^{(\tau)} \mid UK^{(S)}_i)\\
&= H(C^{(1)}, \ldots, C^{(\tau)})\\
&= H(CK^{(1)}_A) + H(CK^{(1)}_{D_1}) + \cdots + H(CK^{(1)}_{D_k}) + \ldots\\
&\quad + H(CK^{(\tau)}_A) + H(CK^{(\tau)}_{D_1}) + \cdots + H(CK^{(\tau)}_{D_k}) \quad (2)\\
&= \tau(\omega+1)H(CK).
\end{aligned}$$

(2) は補題 1 から従う．□

補題 4 任意の$t \in \mathcal{T}$に対して，$H(MK_t \mid MK_1, \ldots, MK_{t-1}) \geq (\omega+1)H(CK)$．特に，任意の$t \in \mathcal{T}$に対して，$H(MK_t) \geq (\omega+1)H(CK)$．

証明: 任意の$i \in \{1, 2, \ldots, n\}$に対して，$i \notin B$となるような利用者の集合を$B := \{l_1, \ldots, l_{\omega+1}\}$とする．また$A := \{(i, l_{\omega+1})\}$，$D_k := \{(i, l_k)\}$ $(1 \leq k \leq \omega)$とする．このとき，

$$
\begin{aligned}
&H(MK_t)\\
&\geq H(MK_t \mid MK_1, \ldots, MK_{t-1})\\
&\geq H(MK_t \mid UK_i^{(R)}, MK_1, \ldots, MK_{t-1})\\
&\geq I(CK_A^{(t)}, CK_{D_1}^{(t)}, \ldots, CK_{D_k}^{(t)}; MK_t\\
&\qquad\qquad \mid UK_i^{(R)}, MK_1, \ldots, MK_{t-1})\\
&= H(CK_A^{(t)}, CK_{D_1}^{(t)}, \ldots, CK_{D_k}^{(t)}\\
&\qquad\qquad \mid UK_i^{(R)}, MK_1, \ldots, MK_{t-1})\\
&\quad - H(CK_A^{(t)}, CK_{D_1}^{(t)}, \ldots, CK_{D_k}^{(t)}\\
&\qquad\qquad \mid UK_i^{(R)}, MK_1, \ldots, MK_t)\\
&= H(CK_A^{(t)}, CK_{D_1}^{(t)}, \ldots, CK_{D_k}^{(t)}\\
&\qquad\qquad \mid UK_i^{(R)}, MK_1, \ldots, MK_{t-1})\\
&= H(CK_A^{(t)} \mid UK_i^{(R)}, MK_1, \ldots, MK_{t-1})\\
&\quad + H(CK_{D_1}^{(t)} \mid UK_i^{(R)}, MK_1, \ldots, MK_{t-1})\\
&\qquad + \ldots\\
&\qquad\quad + H(CK_{D_k}^{(t)} \mid UK_i^{(R)}, MK_1, \ldots, MK_{t-1}) \qquad (3)\\
&= (\omega+1)H(CK).
\end{aligned}
$$

最後の等号は定義 2 から従い，(3) は本質的に補題 1 から従う．□

補題 5 $H(MK^*) \geq \tau(\omega+1)H(CK)$.

証明:

$$
\begin{aligned}
&H(MK^*)\\
&\geq I(MK_1, \ldots, MK_\tau; MK^*)\\
&= H(MK_1, \ldots, MK_\tau) - H(MK_1, \ldots, MK_\tau \mid MK^*)\\
&= H(MK_1, \ldots, MK_\tau)\\
&= H(MK_1) + H(MK_2 \mid MK_1) + \ldots\\
&\qquad + H(MK_t \mid MK_1, \ldots, MK_{t-1}) + \ldots\\
&\qquad\quad + H(MK_\tau \mid MK_1, \ldots, MK_{\tau-1})\\
&= \tau(\omega+1)H(CK).
\end{aligned}
$$

最後の等号は補題 4 から従う．□

実は, 4 節で示す TR-KA の構成法は，定理 1 における (i)-(iv) の等号成立の場合である．したがって，導出した鍵の下界はタイトである．ここで, 下界の等号が成り立つような構成法を以下のように特徴づける．

定義 3 (n, ω, τ)-secure TR-KA II の構成法が定理 1 の (i)-(iv) の等号を全て満たすとき，この構成法は最適 (optimal) であるという．

4 構成法

本節では TR-KA の構成法について述べる．これは有限体上の多項式を用いた構成法である．また，この構成法が最適であることも示す．

鍵生成アルゴリズム *Setup*: セキュリティパラメータ1^kに対して，*Setup* は，$max(n, \tau) < q$となるようなkビットの素数べきqを選び，要素数qの有限体$GF(q)$を構成する．ここで，各利用者の ID 情報は適切な符号化により$U_i \in GF(q)$ $(1 \leq i \leq n)$とし，t $(1 \leq t \leq \tau)$も$GF(q)$の要素とする． 次に，$GF(q)$上の多項式 $f(x, y) := \sum_{i=0}^{\omega}\sum_{j=0}^{\omega} a_{ij}x^i y^j$, $mk^*(x, z) := \sum_{i=0}^{\omega}\sum_{k=1}^{\tau} b_{ik}x^i z^k$ をランダムに選ぶ．さらに，$2n$ 個の多項式 $uk_i^{(S)}(y, z) := f(U_i, y) + mk^*(U_i, z)$ と $uk_i^{(R)}(x) := f(x, U_i)$ $(1 \leq i \leq n)$ をそれぞれ計算する．その後，Time Server のマスター秘密鍵 $mk^* := mk^*(x, z)$ と，各利用者の秘密鍵 $uk_i := \{uk_i^{(S)}(y, z), uk_i^{(R)}(x)\}$ $(1 \leq i \leq n)$ を構成し，出力する．

時刻情報生成アルゴリズム *Ext*: マスター鍵mk^*と時刻tに対して，*Ext* は時刻tの時刻情報$mk_t(x) := mk^*(x, t)$を計算し，出力する．

共有鍵生成アルゴリズム *KeyGen*: 生成用秘密鍵 $uk_{i_1}^{(S)}$，指定する共有可能時刻 t, そして U_{i_2} の ID 情報に対して，*KeyGen* は U_{i_1} と U_{i_2} の共有鍵 $ck_{i_1,i_2}^{(t)} := uk_{i_1}^{(S)}(U_{i_2}, t)$ を出力する．

共有鍵導出アルゴリズム *KeyDer*: 導出用秘密鍵 $uk_{i_2}^{(R)}$，指定された時刻tの時刻情報mk_t, そして U_{i_1} の ID 情報に対して，*KeyDer* は U_{i_1} と U_{i_2} の共有鍵 $ck_{i_1,i_2}^{(t)} := uk_{i_2}^{(R)}(U_{i_1}) + mk_t(U_{i_1})$ を出力する．

定理 2 上記の *TR-KA* の構成法は (n, ω, τ)-*secure* であり，最適である．

証明: この構成法が定義 2 の安全性を満たすことを示す. はじめに定義 2 の 1 つめの条件を満たしていることを示す. Time Server は $f(x,y)$ を知ることができないため, $CK^{(t)}_{i_1,i_2}$ に関する情報を何も得られない. このため, $H(CK^{(t)}_{i_1,i_2}|MK^*) = \log q$ である. 一方, $H(CK^{(t)}_{i_1,i_2}) = \log q$ であるから, 任意の U_{i_1}, $U_{i_2} \in U$, 任意の時刻 $t \in \mathcal{T}$ に対して, $H(CK^{(t)}_{i_1,i_2}|\ MK^*) = H(CK^{(t)}_{i_1,i_2})$ である. 次に定義 2 の 2 番目の条件を満たしていることを示す. 多項式 $f(x,y) + mk^*(x,z)$ の x, y, z の次数はそれぞれ ω, ω, τ であり, たとえ U_{i_1}, U_{i_2} 以外の ω 人が結託したとしても, $CK^{(t)}_{i_1,i_2}$ に関する情報を何も得られない. つまり $H(CK^{(t)}_{i_1,i_2}|UK^{(S)}_W, UK^{(R)}_W, MK_1, \ldots, MK_\tau) = \log q$ である. よって, $H(CK^{(t)}_{i_1,i_2}|UK^{(S)}_W, UK^{(R)}_W, MK_1, \ldots, MK_\tau) = H(CK^{(t)}_{i_1,i_2})$ である. 定義 2 の 3 番目の条件についても, 2 番目の条件と同様の流れで証明できるため, ここでは省略する. □

5 まとめと今後の研究

本稿では, 時刻情報で制御する情報理論的に安全な鍵共有方式として, Timed-Release Key-Agreement (TR-KA) を提案した. 具体的には, TR-KA のモデル, 安全性の定式化, および利用者の鍵サイズのタイトな下界を示し, 最適な構成法をも示した.

今後の研究として, 攻撃モデルの拡張と TR-KA のアプリケーションの提案が挙げられる. まず, 今回提案した攻撃モデルの拡張として, Time Server と利用者の結託を想定するものが考えられる. 実は, このような攻撃モデルの下でも同様の鍵サイズの下界を示すことができ, 本稿の構成法は, そのような攻撃モデルに対しても安全であると考えられる. 詳しくは本稿のフルバージョンを参照されたい. また, TR-KA のアプリケーションとして, (TR-KA と one-time pad を組み合わせて) 情報理論的に安全な Timed-Release Encryption や, (TR-KA と Authentication code を組み合わせて) 情報理論的に安全な Timed-Release Authentication Code が実現可能と考えられる. これら, Timed-Release Encryption, Timed-Release Authentication Code のモデルや安全性の定式化、そして TR-KA との関係等の詳細についても、本稿のフルバージョンを参照されたい.

参考文献

[1] R. Blom, “Non-Public Key Distribution”, Proceedings of CRYPTO 1982, pp.231-236, Plenum Press, 1982.

[2] R. Blom, “Optimal Class of Symmetric Key Generation Systems”, Advances in Cryptology - CRYPTO ’85, LNCS 209, pp.335-338, Springer, 1985.

[3] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly Secure Key Distribution for Dynamic Conferences”, Information and Computation, vol.146, pp.1-23, 1998.

[4] T. Matsumoto and H. Imai, “On the Key Predistribution Systems: A Practical Solution to the Key Distribution Problem ”, Advances in Cryptology - CRYPTO ’87, LNCS 293, pp.512-526, Springer, 1987.

[5] U. Maurer, “Secret key agreement by public discussion from common information ”, IEEE Trans. Information Theory, vol.39, no.3, pp.733-742, 1993.

[6] T. C. May, “Timed-release crypto”, 1993.

[7] R. Rivest, A. Shamir, and D. A. Wagner, “Time-lock puzzles and timed-release crypto ”, MIT LCS Tech, Report MIT LCS TR-684, 1996.

[8] S. Wolf, “Strong Security Against Active Attacks in Information-Theoretic Secret-Key Agreement ”, Advances in Cryptology - ASIACRYPT ’98, LNCS 1514, pp.405-419, Springer, 1998.