情報理論的に安全なタイムリリース暗号化方式とメッセージ認証方式におけるタイトな下界について

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
{watanabe-yohei-xs, takenobu.seito, shikata}@ynu.ac.jp

あらまし 著者らは国際会議 ICITS2012 において，世界で初めて情報理論的に安全なタイムリリース鍵共有方式，暗号化方式，メッセージ認証方式を提案した．上記の論文の中で，鍵共有方式における鍵長等のタイトな下界は既に導出したが，暗号化方式及びメッセージ認証方式における鍵長等の下界は導出していなかった．したがって，本稿では，これらのタイトな下界について示す．

Tight Lower Bounds in Information-Theoretically Secure Timed-Release Encryption and Authentication Codes

Yohei Watanabe　　Takenobu Seito　　Junji Shikata

Graduate School of Environment and Information Sciences,
Yokohama National University,
79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan
{watanabe-yohei-xs, takenobu.seito, shikata}@ynu.ac.jp

Abstract We presented information-theoretically secure timed-release key-agreement, encryption and authentication-codes at ICITS2012, and we derived several tight lower bounds in timed-release key-agreement in our paper. In this paper, we derive several tight lower bounds in timed-release encryption and authentication-codes.

1 はじめに

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 Public Key Encryption (TR-PKE) が知られている．1996 年，Rivest ら [1] によって時刻情報を鍵として復号するモデルの TR-PKE が提案された．TR-PKE 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．TR-PKE 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．

一方で，著者らは国際会議 6th International Conference on Information Theoretic Security (ICITS2012) にて世界で初めて情報理論的に安全なタイムリリース鍵共有方式，暗号化方式，メッセージ認証方式を提案した [3]．[3] において，鍵共有方式における鍵長等のタイトな下界は既に導出したが，暗号化方式及びメッセージ認証方式における鍵長等の下界は導出していなかった．本稿では，これらのタイトな下界について示す．

2 Timed-Release Encryption

本節では，[3] に従い, 情報理論的安全性を有する Timed-Release Encryption (TRE) のモデルと安全性定義を述べる．そして, 本稿の主結果である鍵長等のタイトな下界について示す.

2.1 モデルと安全性定義

本稿の方式では，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．このモデルでは，TI と n 人の利用者，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，TI が各利用者，Time Server の秘密鍵を生成，各エンティティに安全な通信路を用いて配布する．Time Server は，自身の秘密鍵と時刻を使い，各時刻に対応した時刻情報を生成，改ざん不可な通信路を用いて時刻情報を放送する．送信者 U_{i_1} は，任意の平文，自身の暗号化鍵，指定時刻 t，相手の ID を用いて，受信者 U_{i_2} に対して，未来の時刻 t に復号できるような暗号文を生成，その指定時刻と共に U_{i_2} に改ざん不可な通信路を用いて送信する．この時点では U_{i_2} は暗号文を復号することはできない．時が過ぎ，時刻 t になれば，受信者 U_{i_2} は，指定時刻 t に放送されてくる時刻情報，自身の復号鍵，相手の ID を用い，暗号文を復号，平文を得ることができる．

ここで，TRE を次のように定義する．紙面の都合上，本稿の定義はインフォーマルなものとなっているので，詳細な定義は [3] を参照.

定義 1 (TRE). Information-Theoretically Secure Timed-Release Encryption (TRE) プロトコル Σ 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 ($EGen$, $EExt$, Enc, Dec)，6 つの空間 $\mathcal{C}$, $\mathcal{M}_E$, $\mathcal{USK}$, $\mathcal{EMK}$, $\mathcal{T}$, $\mathcal{ETI}$ からなる．$EGen$ アルゴリズムは確率的，$EExt$, Enc, Dec 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．記法は以下の通り．エンティティは信頼できる第三者機関 TI，利用者 U_i ($1 \leq i \leq n$)(以下，ID の集合を同一視する)，時刻情報を管理する第三者機関 (Time Server) T である．さらに $U := \{U_1, U_2, \ldots, U_n\}$ を利用者集合とする．空間は次のように定義する．$\mathcal{C}$ は暗号文の集合であり，$\mathcal{M}_E$ は平文の集合であり確率分布 P_M をもつ．$\mathcal{USK}_i$ は U_i の秘密鍵の集合であり，$\mathcal{EMK}$ 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．$\mathcal{ETI}$ は時刻情報の集合である．ここで $\mathcal{ETI} := \bigcup_{i=1}^{\tau} \mathcal{ETI}^{(i)}$ とおく．また, $\mathcal{USK}_i := \mathcal{EK}_i \times \mathcal{DK}_i$ とおく．ただし, $\mathcal{EK}_i$ は U_i の暗号化鍵の集合であり，$\mathcal{DK}_i$ は U_i の復号鍵の集合である．ここで $\mathcal{USK} := \bigcup_{i=1}^{n} \mathcal{USK}_i$，また $\mathcal{EK} := \bigcup_{i=1}^{n} \mathcal{EK}_i$, $\mathcal{DK} := \bigcup_{i=1}^{n} \mathcal{DK}_i$ とする．アルゴリズムは次のように定義する．$EGen$ 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．$EExt : \mathcal{EMK} \times \mathcal{T} \rightarrow \mathcal{ETI}$ は時刻情報生成アルゴリズムである．$Enc : \mathcal{M}_E \times \mathcal{EK} \times \mathcal{T} \times \mathcal{U} \rightarrow \mathcal{C}$ は暗号化アルゴリズム，$Dec : \mathcal{C} \times \mathcal{DK} \times \mathcal{ETI} \times \mathcal{U} \rightarrow \mathcal{M}_E$ は復号アルゴリズムである.

次に，TRE 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 $W := \{U_{l_1}, U_{l_2}, \ldots, U_{l_j} \in \mathcal{P}(\mathcal{U}, \omega)$ とし， $\mathcal{EK}_W := \mathcal{EK}_{l_1} \times \cdots \times \mathcal{EK}_{l_j}$ を W の持つ暗号化鍵の集合， $\mathcal{DK}_W := \mathcal{DK}_{l_1} \times \cdots \times \mathcal{DK}_{l_j}$ を W の持つ復号鍵の集合とする．さらに, $\mathcal{C}_{i_1,i_2}^{(t)}$ を U_{i_1} と U_{i_2} の間での時刻 t で復号可能な暗号文の集合とする．M,$C_{i_1,i_2}^{(t)}$, EMK, EK_W, DK_W, $ETI^{(1)}, \ldots, ETI^{(\tau)}$ を，それぞれ $\mathcal{M}_E$,$\mathcal{C}_{i_1,i_2}^{(t)}$, $\mathcal{EMK}$, $\mathcal{EK}_W$, $\mathcal{DK}_W$, $\mathcal{ETI}^{(1)}, \ldots, \mathcal{ETI}^{(\tau)}$ に値をとる確率変数とする.

TRE 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，受信者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 (TRE の安全性). TRE Σ が以下を満たすとき，Σ 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 msk^* と暗号文から平文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，$H(M \mid C^{(t)}_{i_1,i_2}, EMK) = H(M)$.

(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，平文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，$H(M \mid C^{(t)}_{i_1,i_2}, EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(\tau)}) = H(M)$.

(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，時刻 t に放送される時刻情報がなければ，平文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 $U_{i_1} \notin W, U_{i_2} \in W$，また任意の時刻 $t \in \mathcal{T}$ に対して，$H(M \mid C^{(t)}_{i_1,i_2}, EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(t-1)}, ETI^{(t+1)}, \ldots, ETI^{(\tau)}) = H(M)$.

2.2 鍵長等のタイトな下界

定理 1. (n, ω, τ)-secure TRE において，任意の $i \in \{1, 2, \ldots, n\}$，$t \in \{1, 2, \ldots, \tau\}$ において，以下の不等式が成立する．

$$
\begin{array}{ll}
(i) & H(DK_i) \geq (\omega + 1)H(M), \\
(ii) & H(EK_i) \geq (\tau + \omega)H(M), \\
(iii) & H(ETI^{(t)}) \geq (\omega + 1)H(M), \\
(iv) & H(EMK) \geq \tau(\omega + 1)H(M).
\end{array}
$$

証明は本節の以下の補題から従う．ここで，任意の $i, j \in \{1, 2, \ldots, n\}$，$t \in \{1, 2, \ldots, \tau\}$ において，時刻 t を指定し U_i から U_j に送られる平文の確率変数を $M^{(t)}_{i,j}$ とする．また，$M^{(t)}_{i,j}$ は互いに独立で同一の確率分布 P_M に従う（つまり、i.i.d.）.

まず，TRE Σ において次の条件を考える．

(1)' 任意の $U_i, U_j \in \mathcal{U}$，任意の $t \in \mathcal{T}$ において，$H(C^{(t)}_{i,j} \mid M^{(t)}_{i,j}, EMK) = H(C^{(t)}_{i,j} \mid EMK)$.

(2)' 任意の $W \in \mathcal{P}(\mathcal{U}, \omega)$, $U_i, U_j \in \mathcal{U}$ かつ $U_i, U_j \notin W$, また任意の $t \in \mathcal{T}$ において，$H(C^{(t)}_{i,j} \mid M^{(t)}_{i,j}, EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(\tau)}) = H(C^{(t)}_{i,j} \mid EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(\tau)})$.

(3)' 任意の $W \in \mathcal{P}(\mathcal{U}, \omega)$，$U_i, U_j \in \mathcal{U}$ かつ $U_i \notin W$，$U_j \in W$ また任意の $t \in \mathcal{T}$ において，$H(C^{(t)}_{i,j} \mid M^{(t)}_{i,j}, EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(t-1)}, ETI^{(t+1)}, \ldots, ETI^{(\tau)}) = H(C^{(t)}_{i,j} \mid EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(t-1)}, ETI^{(t+1)}, \ldots, ETI^{(\tau)})$.

この時，上記は定義 2 と同値であることを示す．

補題 1. TRE Σ に対して、Σ が (n, ω, τ)-secure であることと、条件式 (1)', (2)', (3)' を満たすことは同値である．

証明: Z を次の (1), (2), (3) いずれかの任意の確率変数とする．(1) $Z = EMK$, (2) $Z = (EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(\tau)})$ $(U_i, U_j \notin W)$, (3) $Z = (EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(t-1)}, ETI^{(t+1)}, \ldots, ETI^{(\tau)})$ $(U_i \notin W, U_j \in W)$.

まず，$H(M^{(t)}_{i,j}, C^{(t)}_{i,j} \mid Z)$ において，

$$
\begin{aligned}
& H(M^{(t)}_{i,j}, C^{(t)}_{i,j} \mid Z) \\
= \; & H(M^{(t)}_{i,j} \mid Z) + H(C^{(t)}_{i,j} \mid M^{(t)}_{i,j}, Z) \\
= \; & H(M^{(t)}_{i,j}) + H(C^{(t)}_{i,j} \mid M^{(t)}_{i,j}, Z). \qquad (1)
\end{aligned}
$$

(1) は $M^{(t)}_{i,j}$ と Z は独立なことから従う．一方で，

$$
\begin{aligned}
& H(M^{(t)}_{i,j}, C^{(t)}_{i,j} \mid Z) \\
= \; & H(C^{(t)}_{i,j} \mid Z) + H(M^{(t)}_{i,j} \mid C^{(t)}_{i,j}, Z). \qquad (2)
\end{aligned}
$$

(1) と (2) から，この補題は従う． □

補題 2. 任意の $i, j \in \{1, 2, \ldots, n\}$, $t \in \{1, 2, \ldots, \tau\}$ において，$H(C^{(t)}_{i,j} \mid Z) \geq H(M^{(t)}_{i,j})$. Z は補題 1 の証明における確率変数である．

証明の概略: まず，$H(M^{(t)}_{i,j}, C^{(t)}_{i,j}, EK_i, DK_j, ETI^{(t)} \mid Z)$ において，

$$
\begin{aligned}
& H(M^{(t)}_{i,j}, C^{(t)}_{i,j}, EK_i, DK_j, ETI^{(t)} \mid Z) \\
& = H(M^{(t)}_{i,j}, EK_i, DK_j, ETI^{(t)} \mid Z). \qquad (3)
\end{aligned}
$$

一方で，

$$
\begin{aligned}
& H(M^{(t)}_{i,j}, C^{(t)}_{i,j}, EK_i, DK_j, ETI^{(t)} \mid Z) \\
& = H(C^{(t)}_{i,j}, EK_i, DK_j, ETI^{(t)} \mid Z). \qquad (4)
\end{aligned}
$$

更に，

$$\begin{aligned} & H(C_{i,j}^{(t)} \mid Z) + H(EK_i, DK_j, ETI^{(t)} \mid Z) \\ \geq\ & H(C_{i,j}^{(t)}, EK_i, DK_j, ETI^{(t)} \mid Z) \\ =\ & H(M_{i,j}^{(t)}, EK_i, DK_j, ETI^{(t)} \mid Z) \quad (5) \\ =\ & H(M_{i,j}^{(t)}) + H(EK_i, DK_j, ETI^{(t)} \mid Z). \quad (6) \end{aligned}$$

(5) は (3) と (4) から従い，(6) は $M_{i,j}^{(t)}$ が $(Z, EK_i, DK_j, ETI^{(t)})$ と独立であることから従う．従って，$H(C_{i,j}^{(t)} \mid Z) \geq H(M_{i,j}^{(t)})$. □

補題 3. 任意の $i \in \{1, 2, \ldots, n\}$ において，$H(DK_i) \geq (\omega + 1)H(M)$.

証明の概略: 任意の $i \in \{1, 2, \ldots, n\}$ において，$B := \{l_1, l_2, \ldots, l_{\omega+1}\} \subset \{1, 2, \ldots, n\}$ を $i \notin B$ となるような利用者インデックスの部分集合とする．また，$D_k := (l_k, i)$ $(1 \leq k \leq \omega + 1)$ とする．このとき，

$$\begin{aligned} & H(DK_i) \\ \geq\ & H(DK_i \mid ETI^{(t)}, C_{D_1}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}) \\ \geq\ & I(M_{D_1}^{(t)}, \ldots, M_{D_{\omega+1}}^{(t)}; DK_i \\ & \qquad \mid ETI^{(t)}, C_{D_1}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}) \\ =\ & H(M_{D_1}^{(t)}, \ldots, M_{D_{\omega+1}}^{(t)} \\ & \qquad \mid ETI^{(t)}, C_{D_1}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}) \\ =\ & \sum_{k=1}^{\omega+1} H(M_{D_k}^{(t)}) \quad (7) \\ =\ & (\omega + 1)H(M). \end{aligned}$$

(7) は定義 2 の (2) より従う. □

補題 4. 任意の $i \in \{1, 2, \ldots, n\}$ に対して，$H(EK_i) \geq (\tau + \omega)H(M)$.

証明の概略: 任意の $i \in \{1, 2, \ldots, n\}$ において，$B := \{l_1, l_2, \ldots, l_{\omega+1}\} \subset \{1, 2, \ldots, n\}$ を $i \notin B$ となるような利用者インデックスの部分集合とし，$D_k := (l_k, i)$ $(1 \leq k \leq \omega + 1)$ とする．また，任意の $1 \leq k \leq \omega + 1$，$1 \leq t \leq \tau$ において，$F_k^{(t)} := (M_{D_k}^{(1)}, \ldots, M_{D_k}^{(t)})$，$G_k^{(t)} := (M_{D_1}^{(t)}, \ldots, M_{D_k}^{(t)})$，$FC_k^{(t)} := (C_{D_k}^{(1)}, \ldots, C_{D_k}^{(t)})$，$GC_k^{(t)} := (C_{D_1}^{(t)}, \ldots, C_{D_k}^{(t)})$ とする．このとき，

$$\begin{aligned} & H(EK_i) \\ & = H(EK_i, FC_1^{(\tau)}, GC_{\omega+1}^{(\tau)} \mid F_1^{(\tau)}, G_{\omega+1}^{(\tau)}) \\ & \geq H(FC_1^{(\tau)}, GC_{\omega+1}^{(\tau)} \mid F_1^{(\tau)}, G_{\omega+1}^{(\tau)}) \\ & = \sum_{t=1}^{\tau} H(C_{D_1}^{(t)} \mid F_1^{(\tau)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \\ & \quad + \sum_{k=2}^{\omega+1} H(C_{D_k}^{(\tau)} \mid F_1^{(\tau)}, FC_1^{(\tau)}, G_{\omega+1}^{(\tau)}, \\ & \qquad\qquad C_{D_1}^{(\tau)}, \ldots, C_{D_{k-1}}^{(\tau)}) \\ & \geq (\tau + \omega)H(M). \quad (8) \end{aligned}$$

(8) は補題 2 と補題 1，条件 (2)', (3)' から従う. □

補題 5. 任意の $t \in \mathcal{T}$ において，$H(ETI^{(t)} \mid ETI^{(1)}, \ldots, ETI^{(t-1)}) \geq (\omega + 1)H(M)$. 特に，任意の $t \in \mathcal{T}$ において，$H(ETI^{(t)}) \geq (\omega + 1)H(M)$.

証明の概略: 任意の $i \in \{1, 2, \ldots, n\}$ において，$B := \{l_1, l_2, \ldots, l_{\omega+1}\} \subset \{1, 2, \ldots, n\}$ を $i = l_1$ となるような利用者インデックスの部分集合とし，$D_k := (l_k, i)$ $(1 \leq k \leq \omega + 1)$ とする．このとき，

$$\begin{aligned} & H(ETI^{(t)} \mid ETI^{(1)}, \ldots, ETI^{(t-1)}) \\ & \geq H(ETI^{(t)} \mid C_{D_1}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}, DK_i, \\ & \qquad\qquad ETI^{(1)}, \ldots, ETI^{(t-1)}) \\ & \geq I(M_{D_1}^{(t)}, \ldots, M_{D_{\omega+1}}^{(t)}; ETI^{(t)} \mid C_{D_1}^{(t)}, \ldots, \\ & \quad C_{D_{\omega+1}}^{(t)}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)}) \\ & = H(M_{D_1}^{(t)} \ldots, M_{D_{\omega+1}}^{(t)} \mid C_{D_1}^{(t)}, \ldots, \\ & \qquad C_{D_{\omega+1}}^{(t)}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)}) \\ & = \sum_{k=1}^{\omega+1} H(M_{D_k}^{(t)}) \quad (9) \\ & = (\omega + 1)H(M). \end{aligned}$$

(9) は定義 2 の (3) より従う. □

補題 6. $H(EMK) \geq \tau(\omega + 1)H(M)$.

[3] の補題 4 と同様に証明可能である. □

実は, [3] で示されている TRE の一般的構成法における Timed-Release Key-Agreement (TR-KA) の部分に, 同じく [3] で示されている TR-KA の具体的構成法を適用すると，定理 1 における (i)-(iv) の等号成立の場合の TRE の具体的構成法が得られる．したがって，定理 1 の下界はタイトである．

3 Timed-Release Authentication Codes

本節では, [3] に従い, Timed-Release Authentication code (TRA-code) のモデルと安全性定義を述べる. そして，本稿のもう一つの主結果である TRA-code の鍵長等のタイトな下界と最適な構成法を示す.

3.1 モデルと安全性定義

TREと同様のエンティティが登場する．まず，TRE同様，TIが各利用者，Time Serverの秘密鍵を生成，各エンティティに安全な通信路を用いて配布する．Time Serverは，自身の秘密鍵と時刻を使い，各時刻に対応した時刻情報を生成，改ざん不可な通信路を用いて時刻情報を放送する．送信者U_{i_1}は，任意のメッセージ，自身の認証子生成鍵，指定時刻t，相手のIDを用いて，受信者U_{i_2}に対して，未来の時刻tに検証できるような認証子を生成，U_{i_2}にメッセージ，認証子，指定時刻を送信する．この時点ではU_{i_2}は認証子を検証することはできない．時が過ぎ，時刻tになれば，受信者U_{i_2}は，指定時刻tに放送されてくる時刻情報，自身の検証鍵，相手のIDを用い，認証子を検証，正当なものであれば受理し，そうでなければ受理しない．

ここで，TRA-codeを次のように定義する．紙面の都合上，本稿の定義はインフォーマルなものとなっているので，詳細な定義は[3]を参照．

定義 3 (TRA-code). Timed-Release Authentication code (TR-A-code) Λは，TIとU_1, U_2, …, U_n，Time Serverの$n+2$のエンティティ，4つのアルゴリズム($TAGen$, $AExt$, $TAuth$, $TVer$)，6つの空間$\mathcal{M}_A$, $\mathcal{A}$, $\mathcal{E}$, $\mathcal{AMK}$, $\mathcal{T}$, $\mathcal{ATI}$からなる．$TAGen$アルゴリズムは確率的，$AExt$, $TAuth$, $TVer$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．記法は以下の通り．エンティティはTRE同様のものを考える．空間は次のように定義する．$\mathcal{T}$は定義1と同様である．$\mathcal{M}_A$はメッセージの集合，$\mathcal{A}$は認証子の集合，$\mathcal{AMK}$はマスター鍵の集合である．$\mathcal{ATI}$は時刻情報の集合である．ここで$\mathcal{ATI} := \bigcup_{t=1}^{\tau} \mathcal{ATI}^{(t)}$とおく．$\mathcal{E}_i$は$U_i$の秘密鍵の集合であり，$\mathcal{E}_i := \mathcal{E}_i^{(S)} \times \mathcal{E}_i^{(R)}$とおく．ただし，$\mathcal{E}_i^{(S)}$は$U_i$の認証子生成鍵の集合であり，$\mathcal{E}_i^{(R)}$は$U_i$の検証鍵の集合である．ここで$\mathcal{E}^{(S)} := \bigcup_{i=1}^{n} \mathcal{E}_i^{(S)}$，$\mathcal{E}^{(R)} := \bigcup_{i=1}^{n} \mathcal{E}_i^{(R)}$，また$\mathcal{E} := \bigcup_{i=1}^{n} \mathcal{E}_i$とする．アルゴリズムは次のように定義する．$TAGen$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．$Ext : \mathcal{AMK} \times \mathcal{T} \to \mathcal{ATI}$は時刻情報生成アルゴリズムである．$TAuth : \mathcal{M}_A \times \mathcal{E}^{(S)} \times \mathcal{T} \times \mathcal{U} \to \mathcal{A}$は認証子生成アルゴリズム，$TVer : \mathcal{M}_A \times \mathcal{A} \times \mathcal{T} \times \mathcal{E}^{(R)} \times \mathcal{ATI} \times \mathcal{U} \to \{true, false\}$は検証アルゴリズムである．

ここでは，TRA-code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．TREと同様に，結託者の集合を$W \in \mathcal{P}(\mathcal{U}, \omega)$のように選ぶ．$\mathcal{E}_W^{(S)} := \mathcal{E}_{l_1}^{(S)} \times \cdots \times \mathcal{E}_{l_j}^{(S)}$を$W$の持つ認証子生成鍵の集合，$\mathcal{E}_W^{(R)} := \mathcal{E}_{l_1}^{(R)} \times \cdots \times \mathcal{E}_{l_j}^{(R)}$を$W$の持つ検証鍵の集合とする．TRA-codesでは，次のような攻撃を考える．(a) **なりすまし攻撃．**攻撃者が送信者U_{i_1}が作った正規の認証子を見ずに偽造した時刻をtに指定した認証子$(m, \alpha_{i_1,i_2}^{(t)}, t)$を生成し，受信者$U_{i_2}$に受理させようとする攻撃．(b) **改ざん攻撃．**攻撃者は，送信者U_{i_1}が作った時刻をt_1に指定した正規の認証子$(m, \alpha_{i_1,i_2}^{(t_1)}, t_1)$を見た後で，新たに時刻を$t_2$に指定し偽造した認証子$(m', \alpha_{i_1,i_2}^{(t_2)}, t_2)$を生成，受信者$U_{i_2}$に受理させようとする攻撃．ただし，$(m, \alpha_{i_1,i_2}^{(t_1)}, t_1) \neq (m', \alpha_{i_1,i_2}^{(t_2)}, t_2)$とする．

Time Server，または受信者を含まない利用者の結託によるなりすまし攻撃，改ざん攻撃を考える．さらに，受信者が利用者結託に含まれる場合は，指定時刻以前に検証し，受理させようとする攻撃を考える．

定義 4 (TRA-codeの安全性). TRA-codes Λが$P_{Server}, P_1, P_2 \leq \epsilon$を満たすとき，$\Lambda$は$(n, \omega, \tau; \epsilon)$-secureという．$P_{Server}$, P_1, P_2は以下のように定義される．

(1) **Time Serverに対する安全性.** $P_{Server} := \max(P_{I_S}, P_{S_S})$とする．$P_{I_S}$, P_{S_S}は以下のように定義される．

1-1) **なりすまし攻撃．**攻撃成功確率を$P_{I_S} := \max_{U_{i_1}, U_{i_2}, t} P_{I_S}(U_{i_1}, U_{i_2}, t)$と定義し，任意の$U_{i_1}$, $U_{i_2} \in U$, 任意の時刻$t \in \mathcal{T}$に対して，$P_{I_S}(U_{i_1}, U_{i_2}, t)$を次のように定義する．

$$P_{I_S}(U_{i_1}, U_{i_2}, t) := \max_{(m, \alpha_{i_1,i_2}^{(t)}, t)} \max_{amk^*} \max_{amk^{(t)}} \Pr(TVer(m, \alpha_{i_1,i_2}^{(t)}, t, e_{i_2}^{(R)}, amk^{(t)}, U_{i_1}) = true \mid amk^*).$$

1-2) **改ざん攻撃．**攻撃成功確率を $P_{S_S} := \max_{U_{i_1},U_{i_2},t_1,t_2} P_{S_S}(U_{i_1},U_{i_2},t_1,t_2)$ と定義し，任意の $U_{i_1}, U_{i_2} \in U$, 任意の時刻 $t_1, t_2 \in \mathcal{T}$ に対して，$P_{S_S}(U_{i_1},U_{i_2},t_1,t_2)$ を次のように定義する．

$$P_{S_S}(U_{i_1},U_{i_2},t_1,t_2) := \max_{(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{(m,\alpha^{(t_1)}_{i_1,i_2},t_1)\neq(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{amk^*} \max_{amk^{(t_2)}} \Pr(TVer(m',\alpha^{(t_2)}_{i_1,i_2},t_2,e^{(R)}_{i_2},amk^{(t_2)},U_{i_1}) = true \mid (m,\alpha^{(t_1)}_{i_1,i_2},t_1),amk^*).$$

(2) **受信者を含まない結託に対する安全性．**$P_1 := \max(P_{I_1}, P_{S_1})$ とする．P_{I_1}, P_{S_1} は以下のように定義される．

2-1) **なりすまし攻撃．**攻撃成功確率を $P_{I_1} := \max_{U_{i_1},U_{i_2},W,t} P_{I_1}(U_{i_1},U_{i_2},W,t)$ と定義し，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，$P_{I_1}(U_{i_1},U_{i_2},W,t)$ を次のように定義する．

$$P_{I_1}(U_{i_1},U_{i_2},W,t) := \max_{(m,\alpha^{(t)}_{i_1,i_2},t)} \max_{e^{(S)}_W} \max_{e^{(R)}_W} \max_{amk^{(1)},\ldots,amk^{(\tau)}} \Pr(TVer(m,\alpha^{(t)}_{i_1,i_2},t,e^{(R)}_{i_2},amk^{(t)},U_{i_1}) = true \mid e^{(S)}_W,e^{(R)}_W,amk^{(1)},\ldots,amk^{(\tau)}).$$

2-2) **改ざん攻撃．**攻撃成功確率を $P_{S_1} := \max_{U_{i_1},U_{i_2},W,t_1,t_2} P_{S_1}(U_{i_1},U_{i_2},W,t_1,t_2)$ と定義し，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 $t_1, t_2 \in \mathcal{T}$ に対して，$P_{S_1}(U_{i_1},U_{i_2},W,t_1,t_2)$ を次のように定義する．

$$P_{S_1}(U_{i_1},U_{i_2},W,t_1,t_2) := \max_{(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{(m,\alpha^{(t_1)}_{i_1,i_2},t_1)\neq(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{e^{(S)}_W} \max_{e^{(R)}_W} \max_{amk^{(1)},\ldots,amk^{(\tau)}} \Pr(TVer(m',\alpha^{(t_2)}_{i_1,i_2},t_2,e^{(R)}_{i_2},amk^{(t_2)},U_{i_1}) = true \mid (m,\alpha^{(t_1)}_{i_1,i_2},t_1),e^{(S)}_W,e^{(R)}_W,amk^{(1)},\ldots,amk^{(\tau)}).$$

(3) **受信者を含む結託に対する安全性．**攻撃成功確率を $P_2 := \max_{U_{i_1},U_{i_2},W,t} P_2(U_{i_1},U_{i_2},W,t)$ と定義し，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 $t \in \mathcal{T}$，$msk^*_t \neq msk_t$ に対して，$P_2(U_{i_1},U_{i_2},W,t)$ を次のように定義する．

$$P_2(U_{i_1},U_{i_2},W,t) := \max_{(m,\alpha^{(t)}_{i_1,i_2},t)} \max_{e^{(S)}_W} \max_{e^{(R)}_W} \max_{amk^{(1)},\ldots,amk^{(t-1)},amk^{(t+1)},\ldots,amk^{(\tau)}} \Pr(TVer(m,\alpha^{(t)}_{i_1,i_2},t,e^{(R)}_{i_2},amk^{(t)},U_{i_1}) = true \mid e^{(S)}_W,e^{(R)}_W,amk^{(1)},\ldots,amk^{(t-1)},amk^{(t+1)},\ldots,amk^{(\tau)}).$$

3.2 鍵長等のタイトな下界

TRA-code における攻撃成功確率と利用者の鍵長等のタイトな下界を示す．まず，$A^{(t)}_{1,i_2} := \{\alpha^{(t)}_{1,i_2} \in \mathcal{A} \mid TAuth(m,e^{(S)}_{i_1},t,U_{i_2}) = \alpha^{(t)}_{1,i_2}$ for some $e^{(S)}_{i_1} \in \mathcal{E}^{(S)}_{i_1}\}$ を U_{i_1} から U_{i_2} に送られる時刻を t に指定された認証子の集合とする．また，M,$A^{(t)}_{i_1,i_2}$, AMK, $E^{(S)}_W$, $E^{(R)}_W$, $ATI^{(1)}, \ldots, ATI^{(\tau)}$ を，それぞれ $\mathcal{M}_A$,$\mathcal{A}^{(t)}_{i_1,i_2}$, $\mathcal{AMK}$, $\mathcal{E}^{(S)}_W$, $\mathcal{E}^{(R)}_W$, $\mathcal{ATI}^{(1)}, \ldots, \mathcal{ATI}^{(\tau)}$ に値をとる確率変数とする．加えて，$(M,\tilde{M})$ を $M \neq \tilde{M}$ となるような $\mathcal{M}\times\mathcal{M}$ から値をとる結合確率変数，$(A^{(t)}_{i_1,i_2},\tilde{A}^{(t)}_{i_1,i_2})$ を $A^{(t)}_{i_1,i_2} \neq \tilde{A}^{(t)}_{i_1,i_2}$ となるような $\mathcal{A}^{(t)}_{i_1,i_2}\times\mathcal{A}^{(t)}_{i_1,i_2}$ から値をとる結合確率変数とする．

TRA-code のモデルにおいて，次の写像の存在を仮定する．

$$\begin{aligned}
\pi_j &: \mathcal{E}^{(R)}_j \to \mathcal{E}^{(R)}_{1,j}\times\cdots\times\mathcal{E}^{(R)}_{n,j},\\
f &: \mathcal{ATI}^{(t)} \to \mathcal{ATI}^{(t)}_1\times\cdots\times\mathcal{ATI}^{(t)}_n,\\
g^{(t)} &: \mathcal{AMK} \to \mathcal{ATI}^{(1)}\times\cdots\times\mathcal{ATI}^{(\tau)},\\
g_i &: \mathcal{AMK} \to \mathcal{AMK}_1\times\cdots\times\mathcal{AMK}_n,\\
g^{(t)}_i &: \mathcal{AMK}_i \to \mathcal{ATI}^{(1)}_i\times\cdots\times\mathcal{ATI}^{(\tau)}_i,\\
\rho &: \mathcal{E}^{(S)}_i \to \mathcal{E}^{(R)}_i\times\mathcal{AMK}_i.
\end{aligned}$$

$\mathcal{E}^{(R)}_{i,j}$ は U_j が実際に U_i と通信する際に使用する検証鍵の集合であり，$\mathcal{ATI}^{(t)}_i$ は U_i が時刻 t を指定し送信してきた認証子の検証に実際に使用する時刻情報の集合である．また，利用者はそれぞれのマスター鍵を持っているものとし，U_i のマスター鍵の集合を $\mathcal{AMK}_i$ とする．これらの仮定は自然なものと考えられる．実際, 次節で示すシンプルな多項式による構成法において，これらの仮定をみたすからである．また，$E^{(R)}_{i,j}$, $ATI^{(t)}_i$, AMK_i を $\mathcal{E}^{(R)}_{i,j}$, $\mathcal{ATI}^{(t)}_i$, $\mathcal{AMK}_i$ に値をとる確率変数とする．このとき，攻撃成功確率の下界は以下のようになる．

定理 2. $(n,\omega,\tau;\epsilon)$-secure TRA-code Λ において，任意の $i,j\in\{1,...,n\}$，任意の $t\in\mathcal{T}$，U_{i_1}，$U_{i_2}\notin W$ である任意の結託者集合 W，$U_{i_1}\notin\tilde{W}$ かつ $U_{i_2}\in\tilde{W}$ であるような任意の結託者集合 $\tilde{W}$ に対して，

1. $\log P_{I_S}(U_{i_1},U_{i_2},t)\geq -I(MA^{(t)}_{i_1,i_2};E^{(R)}_{i_1,i_2}\mid AMK)$
2. $\log P_{S_S}(U_{i_1},U_{i_2},t_1,t_2)$
   $\geq -I(\tilde{MA}^{(t_2)}_{i_1,i_2};E^{(R)}_{i_1,i_2}\mid AMK,MA^{(t_1)}_{i_1,i_2})$
3. $\log P_{I_1}(U_{i_1},U_{i_2},W,t)$
   $\geq -I(MA^{(t)}_{i_1,i_2};E^{(R)}_{i_1,i_2}\mid E^{(S)}_{W},E^{(R)}_{W},$
   $ATI^{(1)},\dots,ATI^{(\tau)})$
4. $\log P_{S_1}(U_{i_1},U_{i_2},W,t_1,t_2)$
   $\geq -I(\tilde{MA}^{(t_2)}_{i_1,i_2};E^{(R)}_{i_1,i_2}\mid E^{(S)}_{W},E^{(R)}_{W},$
   $ATI^{(1)},\dots,ATI^{(\tau)},MA^{(t_1)}_{i_1,i_2})$
5. $\log P_2(U_{i_1},U_{i_2},\tilde{W},t)$
   $\geq -I(MA^{(t)}_{i_1,i_2};ATI^{(t)}_{i_1}$
   $\mid E^{(S)}_{\tilde{W}},E^{(R)}_{\tilde{W}},ATI^{(1)},\dots,$
   $ATI^{(t-1)},ATI^{(t+1)},\dots,ATI^{(\tau)})$

上記の全ての不等式について，[2] の定理 3.2 の証明と同様の流れで証明することができる．次に，鍵長等の下界について示す．

定理 3. $(n,\omega,\tau;\epsilon)$-secure TRA-code Λ において，$q:=\epsilon^{-1}$ とする．任意の $i_1,i_2\in\{1,2,\dots,n\}$，$t\in\{1,2,\dots,\tau\}$ において，

$$(i)\quad |\mathcal{E}^{(R)}_{i_2}|\geq q^{2(\omega+1)},\quad (ii)\ |\mathcal{E}^{(S)}_{i_1}|\geq q^{2\omega+\tau+1},$$
$$(iii)\quad |\mathcal{ATI}^{(t)}|\geq q^{\omega+1},\quad (iv)\ |\mathcal{AMK}|\geq q^{\tau(\omega+1)},$$
$$(v)\quad |\mathcal{A}^{(t)}_{i_1,i_2}|\geq q.$$

証明は以下の補題から従う．

補題 7. 任意の $i_2\in\{1,2,\dots,n\}$ に対して，$|\mathcal{E}^{(R)}_{i_2}|\geq q^{2(\omega+1)}$.

証明の概略: 任意の $i_1,i_2\in\{1,2,\dots,n\}$ において，任意の結託者集合を $W_{i_1}:=\{U_1,\dots,U_{i_1-1},U_{i_1+1},\dots,U_{\omega+1}\}$ とし，$U_{i_2}\notin W_{i_1}$ とする．このとき，定理 2 と写像 π_{i_2} から次の流れで証明することができる．

$$\left(\frac{1}{q}\right)^{2(\omega+1)}$$
$$\geq \prod_{i_1=1}^{\omega+1}P_{I_1}(U_{i_1},U_{i_2},W_{i_1},t_1)P_{S_1}(U_{i_1},U_{i_2},W_{i_1},t_1,t_2)$$
$$\geq 2^{-H(E^{(R)}_{i_2})}\geq 2^{-\log|\mathcal{E}^{(R)}_{i_2}|}=\frac{1}{|\mathcal{E}^{(R)}_{i_2}|}.\quad\square$$

補題 8. 任意の $i_1\in\{1,2,\dots,n\}$ に対して，$|\mathcal{E}^{(S)}_{i_1}|\geq q^{2\omega+\tau+1}$.

証明の概略: 任意の $i_1,i_2\in\{1,2,\dots,n\}$ において，任意の結託者集合を $W_{i_2}:=\{U_1,\dots,U_{i_2-1},U_{i_2+1},\dots,U_{\omega+1}\}$ とし，$U_{i_1}\notin W_{i_2}$ とする．また任意の受信者を含む結託者集合を $\tilde{W}\in\mathcal{P}(\mathcal{U},\omega)$ とし，$U_{i_1}\notin\tilde{W}$ かつ $U_{i_2}\in\tilde{W}$ である．このとき，定理 2 と補題 7，写像 $g^{(t)}_{i_1}$，写像 ρ から以下の流れで証明することができる．

$$\left(\frac{1}{q}\right)^{2\omega+\tau+1}$$
$$\geq \prod_{i_1=1}^{\omega+1}P_{I_1}(U_{i_2},U_{i_1},W_{i_2},t_1)P_{S_1}(U_{i_2},U_{i_1},W_{i_2},t_1,t_2)$$
$$\prod_{t_1=2}^{\tau}P_2(U_{i_1},U_{i_2},\tilde{W},t_1)$$
$$\geq 2^{-H(E^{(S)}_{i_1})}\geq 2^{-\log|\mathcal{E}^{(S)}_{i_1}|}=\frac{1}{|\mathcal{E}^{(S)}_{i_1}|}.\quad\square$$

補題 9. 任意の $t\in\mathcal{T}$ に対して，$|\mathcal{ATI}^{(t)}|\geq q^{\omega+1}$.

証明の概略: 任意の $i_1,i_2\in\{1,2,\dots,n\}$ において，任意の結託者集合を $\tilde{W}$ とし，$U_{i_2}\in\tilde{W}$ とする．このとき，定理 2 と写像 $\rho,g^{(t)}_{i_1},f$ から以下のように証明することができる．

$$\left(\frac{1}{q}\right)^{\omega+1}\geq\prod_{i_1=1}^{\omega+1}P_2(U_{i_1},U_{i_2},\tilde{W},t)$$
$$\geq 2^{-H(ATI^{(t)})}\geq 2^{-\log|\mathcal{ATI}^{(t)}|}=\frac{1}{|\mathcal{ATI}^{(t)}|}.\quad\square$$

補題 10. $|\mathcal{AMK}|\geq q^{\tau(\omega+1)}$.

証明:補題 9 と写像 $g^{(t)}$ から示される． $\square$

補題 11. 任意の $i_1,i_2\in\{1,2,\dots,n\}$，$t\in\mathcal{T}$ に対して，$|\mathcal{A}^{(t)}_{i_1,i_2}|\geq q$.

証明の概略:写像 π_{i_2} から証明することができる．

$$\frac{1}{q}\geq P_{I_1}(U_{i_1},U_{i_2},W,t)\geq 2^{-H(A^{(t)}_{i_1,i_2})}\geq\frac{1}{|\mathcal{A}^{(t)}_{i_1,i_2}|}.\quad\square$$

実は, 次節で示す TRA-code の具体的構成法は，定理 3 における (i)-(v) の等号成立の場合である．したがって，定理 3 の下界はタイトである．ここで, 定理 3 の下界の等号が成り立つような構成法を最適な構成法とよぶことにする．

3.3 構成法

本節では，TRA-code の最適な構成法を示す．

***TAGen*:**セキュリティパラメータ 1^k に対して，$TAGen$ 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 $f(x,y) := \sum_{i=0}^{\omega}\sum_{j=0}^{\omega} a_{ij}x^i y^j$, $g(x,y) := \sum_{i=0}^{\omega}\sum_{j=0}^{\omega} b_{ij}x^i y^j$, $amk^*(x,z) := \sum_{i=0}^{\omega}\sum_{k=0}^{\tau-1} c_{ik}x^i z^k$ をランダムに選ぶ．さらに，多項式 $e_i^{(S)}, := (g(U_i,y), f(U_i, y) + mk^*(U_i, z))$ と $e_i^{(R)} := (g(x,U_i), f(x,U_i))$ $(1 \leq i \leq n)$ をそれぞれ計算する．その後，Time Server のマスター秘密鍵 $amk^* := amk^*(x, z)$ と，各利用者の秘密鍵 $e_i := (e_i^{(S)}, e_i^{(R)})$ $(1 \leq i \leq n)$ を構成し，出力する．

***AExt*:** マスター鍵 amk^* と時刻 t に対して $AExt$ は時刻 t の時刻情報 $amk^{(t)} := amk^*(x,t)$ を計算し，出力する．

***TAuth*:** メッセージ m，認証子生成鍵 $e_{i_1}^{(S)}$，指定する検証可能時刻 t, そして U_{i_2} の ID 情報に対して，$TAuth$ は認証子 $\alpha_{i_1,i_2}^{(t)} := g(U_{i_1}, U_{i_2})m + f(U_{i_1}, U_{i_2}) + amk^*(U_{i_1}, t)$ を出力する．

***TVer*:** 送られてきたメッセージ m，指定時刻 t, 検証鍵 $e_{i_2}^{(R)}$，指定時刻の時刻情報 $amk^{(t)}$，U_{i_1} の ID 情報を用いて，$TVer$ は送られてきた認証子 $\alpha_{i_1,i_2}^{(t)}$ が $g(U_{i_1}, U_{i_2})m + f(U_{i_1}, U_{i_2}) + amk^*(U_{i_1}, t)$ と一致するかを検証する．一致していれば $true$ を出力し，そうでなければ $false$ を出力する．

定理 4. 上記の構成で得られる TRA-code は $(n, \omega, \tau; \epsilon)$-secure であり，最適である．

証明の概要: この構成法が定義 4 の安全性を満たすことを示す．はじめに定義 4 の $1-2$) を満たしていることを示す．Time Server は $f(x,y), g(x, y)$ を知ることができないため，$(m, \alpha_{i_1,i_2}^{(t)}, t)$ を見たとしても，認証子を高々$1/q$ の確率でしか偽造することができない．このため，$P_{S_S} = 1/q$. $1-1$) に関しても同様に，$P_{I_S} = 1/q$. よって，$P_{Server} = 1/q$. 次に定義 4 の $2-2$) を満たしていることを示す．$f(x,y), g(x,y)$ の次数はそれぞれ ω, ω であり，たとえ U_{i_1}, U_{i_2} 以外の ω 人が結託し，$(m, \alpha_{i_1,i_2}^{(t)}, t)$ を見たとしても，認証子を高々$1/q$ の確率でしか偽造することができない．このため，$P_{S_1} = 1/q$. $2-1$) に関しても同様に，$P_{I_1} = 1/q$. よって，$P_1 = 1/q$. 最後に，定義 4 の (3) を満たしていることを示す．amk^* の次数はそれぞれ $\omega, \tau - 1$ であり，たとえ U_{i_2} を含む ω 人が結託し，指定時刻以外の $\tau - 1$ 個の時刻情報を得たとしても，認証子を高々$1/q$ の確率でしか偽造することができない．このため，$P_2 = 1/q$. □

4 まとめ

本稿では，情報理論的に安全なタイムリリース暗号化方式 (TRE) とメッセージ認証方式 (TRA-code) に対して、鍵長等のタイトな下界を導出した．また，TRE の最適な構成法は [3] から導くことができるが, TRA-code の最適な構成法は [3] から導けないため、本稿で新たに示した．[3] に本稿の成果をあわせることで, 情報理論的に安全なタイムリリース技術の主要プリミティブ (鍵共有, 暗号化, メッセージ認証) の数理モデル, 安全性定義, タイトな下界, 最適構成法がすべて明らかになったといえる．

参考文献

[1] Rivest, R., Shamir, A., Wagner, D.A.: Time-lock puzzles and timed-release crypto. In: MIT LCS Tech. Report. MIT LCS TR-684 (1996).

[2] Safavi-naini, R., Wang, H.: Multireceiver Authentication Codes: Model, Bounds, Constructions and Extentions. In: Information and Computation, vol.151, pp.148-172.(1999)

[3] Watanabe, Y., Seito, T., Shikata, J.: Information-Theoretic Timed-Release Security: Key-Agreement, Encryption, and Authentication Codes. In: ICITS 2012, LNCS 7412, pp. 167-186 (2012), Springer. Updated version: http://eprint.iacr.org/2012/460.