情報理論的に安全なタイムリリース秘密分散法

渡邉 洋平　　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, shikata}@ynu.ac.jp

あらまし 本稿では，情報理論的安全性に基づき，閾値以上の受信者たちでさえ指定時刻が来るまで秘密を復元できない性質を持つ秘密分散法として，タイムリリース秘密分散法を提案する．具体的には，モデル及び安全性を定義し，シェアサイズや秘密鍵長のタイトな下界を導出する．更に，一般的構成法と具体的構成法の 2 種類の構成法を提案し，後者が下界と等号を満たすものであることも示す．興味深い結果として，シェアのサイズに冗長性を加えることなく，タイムリリース機能を実現できることを示す．

Information-Theoretically Secure Timed-Release Secret Sharing Schemes

Yohei Watanabe　　Junji Shikata

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

Abstract In this paper, we propose a timed-release secret sharing scheme (TR-SS) with information-theoretic security. TR-SS is a secret sharing scheme with the property that participants more than a threshold number can reconstruct a secret by using their shares only when the time specified by a dealer has come. Specifically, in this paper we first introduce a model and formalization of security for TR-SS based on the traditional secret sharing scheme and information-theoretic timed-release security. We also derive tight lower bounds on the sizes of shares, time-signals, and entities' secret-keys required for TR-SS. Furthermore, we propose two kinds of constructions, generic and direct ones, for TR-SS. As a result, it is shown that the timed-release security can be realized without any additional redundancy on the share-size.

1　はじめに

Secret Sharing Scheme (秘密分散法) は，Shamir [6] と Blakley [1] によって独立に提案されて以後，様々な研究がなされてきた．k-out-of-n Secret Sharing Scheme [6] では，ディーラは n 人の受信者たちに秘密情報のシェアを配布し，その後，$k-1$ 人未満の受信者は秘密情報を全く得られない一方で，k 人以上の受信者は秘密情報を復元できる．近年では，セキュアデータストレージサービスのようなクラウドコンピューティングへの応用も考えられている．

また，「時刻・時間」は我々の生活と密接に関

わっているといえる．人々は「時刻・時間」に合わせて日々活動しているといえ，そのことからも,「時刻・時間」に関する暗号技術は有用であると考えられる．そのような暗号技術として，タイムリリース方式 [3, 5] がよく知られている．これは，あるユーザが指定した時刻が来ると，別のユーザのある機能が開始するような方式である．たとえば暗号化方式では，送信者が指定した時刻が来て初めて，受信者は暗号文を復号することができるようになる．

上記の議論を基に，それらを組み合わせたタイムリリース秘密分散法 (Timed-Release Secret Sharing Scheme: 以下 TR-SS) を提案する．これは，計算量的安全性のものも含めて世界初の研究である．TR-SS は，指定時刻が来るまではシェアが閾値以上集まっても復元できず，指定時刻になると放送される時刻情報を用いて秘密情報を復元できるというものである．アプリケーションとして，たとえば，ある企業がある重要な情報を全国に点在する各支社に公開したいという状況を考える．その情報は TR-SS で公開予定時刻を指定して分散され，郵送で全シェアが各支社に伝達される．各支社の所在地によって到着時刻にばらつきがあるため，通常の Secret Sharing Scheme では同じタイミングで情報を共有することができない．しかし，TR-SS では指定時刻まで復元が不可能であるため，全支社に情報が到着した後で，同時に情報を共有することができる．また，Secret Sharing Scheme の性質により，郵送中にシェアが漏えいしても，閾値以下であれば，指定時刻以後でもその情報は一切外部に漏れない．これはあくまで一例であり，これ以外にもセキュアデータストレージサービスでの応用など，TR-SS には様々なアプリケーションが考えられる．

本稿では，まず (k, n, τ)-TR-SS のモデル，安全性を定式化する．ここで，k は閾値，n は受信者の数，τ は時刻情報の放送回数である．その後，(k, n, τ)-TR-SS における鍵長等の下界を導出し，また一般的構成法と具体的構成法をそれぞれ提案する．特に，具体的構成法は導出した鍵長等の下界全てと等号を満たすような最適なものとなっている．興味深い結果として，シェアのサイズに冗長性を加えることなく，タイムリリース機能を実現できることを示す．

本稿では，以下の記法を使う．一般的に，X は集合 $\mathcal{X}$ に値をとる確率変数を表す．例えば，A, B, C はそれぞれ集合 $\mathcal{A}, \mathcal{B}, \mathcal{C}$ に値をとる確率変数である．また，任意の有限集合 $\mathcal{Z}$ と任意の非負整数 z に対して，要素数 z 以下の $\mathcal{Z}$ の部分集合族を $\mathcal{PS}(\mathcal{Z}, z) := \{Z \subset \mathcal{Z} || Z| \leq z\}$ とする．また，任意の有限集合 $\mathcal{Z}$ と任意の非負整数 z に対して，$\overline{\mathcal{PS}(\mathcal{Z}, z)}$ を $\mathcal{Z}$ のべき集合における $\mathcal{PS}(\mathcal{Z}, z)$ の補集合とする．つまり要素数 $z+1$ 以上の $\mathcal{Z}$ の部分集合族を表す．

2 モデルと安全性定義

まず，(k, n, τ)-TR-SS のモデルについて述べる．従来の Secret Sharing Scheme と違い，秘密鍵を生成，安全に配布してくれる信頼できる第三者機関 (Trusted Authority: TA) の存在を仮定する．これを Trusted Initializer model (TI model) という [4]．(k, n, τ)-TR-SS では，ディーラ D，n 人の受信者 $P_1, P_2, \ldots, P_n$，τ 回時刻情報を放送するタイムサーバ TS，そして TA の $n+3$ のエンティティが登場する．以降では，各受信者 P_i の ID も P_i で記述する．

(k, n, τ)-TR-SS は以下の流れで進む．まず，TA は D と TS の代わりに秘密鍵を生成し，安全に配布する．配布後は自身のメモリーからそれらを消去し，以後 TA は登場しない．次に，D は受信者たちに秘密情報を復元を許す任意の（未来の）時刻を指定し，秘密鍵を用いて秘密情報を n 個のシェアに分散する．そして D は安全な通信路を通じて各受信者に各シェアを配布する．タイムサーバ TS は各時刻において，自身の秘密鍵を用いてその時刻の時刻情報を生成し，放送を行う．指定時刻が来たら，k 人以上の受信者はその時刻情報と彼らのシェアを用いて秘密情報を復元できる．(k, n, τ)-TR-SS は次のように定義される．以下では，$\mathcal{P} := \{P_1, P_2, \ldots, P_n\}$ を受信者の集合，$\mathcal{S}$ を確率分布 P_S に従う秘密情報の集合，$\mathcal{SK}$ を D の秘密鍵の集合，$\mathcal{MK}$ を TS の秘密鍵の集合とする．また，$\mathcal{T} := \{1, 2, \ldots, \tau\}$ は時刻の集合であり，$\mathcal{U}_i^{(t)}$ は時刻 $t \in \mathcal{T}$ を指定された P_i のシェアの集合であ

る．$\mathcal{U}_i := \bigcup_{t=1}^{\tau} \mathcal{U}_i^{(t)}$ は各 P_i のシェアの集合であり $(i \in \{1, 2, \ldots, n\})$，シェア全体の集合を $\mathcal{U} := \bigcup_{i=1}^{n} \mathcal{U}_i$ とする．更に，$\mathcal{TI}^{(t)}$ は時刻 t の時刻情報の集合とし，$\mathcal{TI} := \bigcup_{t=1}^{\tau} \mathcal{TI}^{(t)}$ とする．最後に，任意の受信者の部分集合 $\mathcal{J} = \{P_{i_1}, \ldots, P_{i_j}\} \subset \mathcal{P}$ に対して，$\mathcal{U}_{\mathcal{J}}^{(t)} := \mathcal{U}_{i_1}^{(t)} \times \cdots \times \mathcal{U}_{i_j}^{(t)}$ は $\mathcal{J}$ が持つシェアの集合を示す．

定義 1 (TR-SS). (k, n, τ)-*TR-SS* Π は $TA, D, P_1, \ldots, P_n, TS$ の $n+3$ 人のエンティティと，*Initialize, Extract, Share, Reconstruct* の 4 つのフェーズ，$\mathcal{S}, \mathcal{SK}, \mathcal{MK}, \mathcal{U}, \mathcal{T}, \mathcal{TI}$ の 6 つの空間からなる．Π は以下のフェーズで実行される．

1. *Initialize.* TA は D の秘密鍵 $sk \in \mathcal{SK}$ と TS の秘密鍵 $mk^* \in \mathcal{MK}$ を生成する．これらの鍵はそれぞれのエンティティに安全な通信路を通じて配布される．配布後は自身のメモリーからそれらを消去し，以後 TA は登場しない[1]．
2. *Share.* D は確率分布 P_S に従ってランダムに秘密情報 $s \in \mathcal{S}$ を選ぶ．もし D が受信者たちに時刻 $t \in \mathcal{T}$ に秘密情報 s を復元してもらいたいのであれば，秘密情報 s と指定時刻 t，また秘密鍵 sk を用いて，各受信者 $P_i (i = 1, 2, \ldots, n)$ に対するシェア $u_i^{(t)} \in \mathcal{U}_i^{(t)}$ を生成する．ここで，簡単化のために $u_i^{(t)}$ は s, t, sk によって確定的に決まるものとする．その後，D はシェアと指定時刻のペア $(u_i^{(t)}, t)$ を各受信者 P_i $(i = 1, 2, \ldots, n)$ に安全な通信路を用いて配布する．
3. *Extract.* 各時刻 t の時刻情報を放送するために，TS は秘密鍵 mk^* と時刻 $t \in \mathcal{T}$ を用いて時刻情報 $mk^{(t)} \in \mathcal{TI}^{(t)}$ を生成し，全ての受信者に改ざん不可な放送通信路（broadcast channel）を通じて放送する．
4. *Reconstruct.* 指定時刻 t に，任意の受信者の集合 $\mathcal{A} = \{P_{i_1}, \ldots, P_{i_j}\} (k \le j \le n)$ は彼らのシェア $u_{i_1}^{(t)}, \ldots, u_{i_j}^{(t)} (k \le j \le n)$ と指定時刻の時刻情報 $mk^{(t)}$ から秘密情報 s を復元することができる．

[1] もし TS が信頼でき，鍵生成をし，D に安全な通信路を通じて送信すると仮定すると，TS は TA と同一視できる．しかし，TA と TS の役割は大きく異なる可能性もある（例えば，TA の役割を担うのはセキュアデータストレージサービスのプロバイダで，TS の役割を担うのは時刻情報配信サーバであるかもしれない）．従って，そのような状況をカバーできるように，一般に本モデルでは TS と TA を分けて定義する．

上記のモデルにおいて，Π は次の *Correctness* を満たす: もし D が正しく *Share* フェーズを，TS が *Extract* フェーズを実行するならば，任意の $i \in \{1, 2, \ldots, n\}$ と $t \in \mathcal{T}$, $s \in \mathcal{S}$, $u_i^{(t)} \in \mathcal{U}_i$, $mk^{(t)} \in \mathcal{TI}^{(t)}$ に対して，任意の $\mathcal{A} \in \overline{\mathcal{PS}(\mathcal{P}, k-1)}$ は *Reconstruct* フェーズの最後に正しく秘密情報 s を復元できる．すなわち，$H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(t)}) = 0$.

次に，(k, n, τ)-TR-SS の安全性を定式化する．ここでは，次の 2 つの安全性を考える: (i) 従来の Secret Sharing Scheme と同じく，k 人未満の受信者は秘密情報に関する情報を何も得ることができないという安全性．(ii) タイムリリース性に関する安全性として，k 人以上の受信者が集まっても，指定時刻が来るまでは秘密情報に関する情報を何も得ることができないという安全性．具体的には次のように定義される．

定義 2 (安全性). Π を (k, n, τ)-*TR-SS* とする．次の要件を満たすとき，Π は安全であるという．

(i) 任意の $\mathcal{F} \in \mathcal{PS}(\mathcal{P}, k-1)$ と任意の $t \in \mathcal{T}$ に対して，

$$H(S \mid U_{\mathcal{F}}^{(t)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(S).$$

(ii) 任意の $\mathcal{A} \in \overline{\mathcal{PS}(\mathcal{P}, k-1)}$ と任意の $t \in \mathcal{T}$ に対して，

$$H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(S).$$

3 鍵長等の下界

次に，安全な (k, n, τ)-TR-SS におけるシェア，時刻情報，秘密鍵のサイズの下界について述べる．

定理 1. Π を任意の安全な (k, n, τ)-*TR-SS* とする．この時，任意の $i \in \{1, 2, \ldots, n\}$ と任意の $t \in \mathcal{T}$ に対して，以下の下界を得る．

$$(i)\ H(U_i^{(t)}) \ge H(S),\ (ii)\ H(SK) \ge \tau H(S),$$
$$(iii)\ H(TI^{(t)}) \ge H(S),\ (iv)\ H(MK) \ge \tau H(S).$$

証明．以下の補題から従う．

補題 1. 任意の $i \in \{1,2,\ldots,n\}$，$t \in \mathcal{T}$ に対して，$H(U_i^{(t)}) \geq H(S)$.

証明．[2] の Theorem 1 の証明と同様に証明することができる．紙面の都合上，詳細は割愛する．

補題 2. 任意の $t \in \mathcal{T}$ に対して，$H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \geq H(S)$．特に，任意の $t \in \mathcal{T}$ に対して，$H(TI^{(t)}) \geq H(S)$.

証明．任意の $\mathcal{A} \in \overline{\mathcal{PS}(\mathcal{P}, k-1)}$ と任意の $t \in \mathcal{T}$ に対して，

$$\begin{aligned} & H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \\ \geq\ & H(TI^{(t)} \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\ \geq\ & I(S; TI^{(t)} \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\ =\ & H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) \quad (1) \\ =\ & H(S). \quad (2) \end{aligned}$$

(1) は (k,n,τ)-TR-SS の Correctness から従い，(2) は定義 2 の (ii) から従う．□

補題 3. $H(SK) \geq \tau H(S)$.

証明．以下では，任意の $t \in \{1,2,\ldots,\tau\}$ に対して，$S^{(t)}$ は時刻 t に復元される（時刻 t を指定された）秘密情報の確率変数を表し，$S^{(t)}$ は互いに独立で同一の確率分布 P_S に従う（つまり，i.i.d.）とする．また，任意の $1 \leq t \leq \tau$ において，$U_{All}^{(t)} := (U_1^{(t)}, \ldots, U_n^{(t)})$ とする，このとき，

$$\begin{aligned} & H(SK) \\ \geq\ & H(SK \mid S^{(1)}, \ldots, S^{(\tau)}) \\ \geq\ & I(SK; U_{All}^{(1)}, \ldots, U_{All}^{(\tau)} \mid S^{(1)}, \ldots, S^{(\tau)}) \\ =\ & H(U_{All}^{(1)}, \ldots, U_{All}^{(\tau)} \mid S^{(1)}, \ldots, S^{(\tau)}) \\ & -H(U_{All}^{(1)}, \ldots, U_{All}^{(\tau)} \mid S^{(1)}, \ldots, S^{(\tau)}, SK) \\ =\ & H(U_{All}^{(1)}, \ldots, U_{All}^{(\tau)} \mid S^{(1)}, \ldots, S^{(\tau)}) \quad (3) \\ =\ & \sum_{t=1}^{\tau} H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(\tau)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ \geq\ & \tau H(S). \quad (4) \end{aligned}$$

(3) は定義 1 の *Share* フェーズから従い（つまり，$H(U_{All}^{(1)}, \ldots, U_{All}^{(\tau)} \mid S^{(1)}, \ldots, S^{(\tau)}, SK) = 0$），(4) は次の事実が成立することから従う：任意の $t \in \mathcal{T}$ に対して，

$$\begin{aligned} & H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(\tau)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ \geq\ & H(S^{(t)}). \quad (5) \end{aligned}$$

ここで，(5) を以下のように示す．まず，

$$\begin{aligned} & H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(\tau)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ =\ & H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(t)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}). \quad (6) \end{aligned}$$

等号は $(S^{(t+1)}, \ldots, S^{(\tau)})$ が $(S^{(1)}, \ldots, S^{(t)}, U_{All}^{(1)}, \ldots, U_{All}^{(t)})$ と独立であることから従う．

次に，$H(U_{All}^{(t)}, S^{(1)}, \ldots, S^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)})$ に対して，

$$\begin{aligned} & H(U_{All}^{(t)}, S^{(1)}, \ldots, S^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ =\ & H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ & +H(S^{(1)}, \ldots, S^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t)}) \\ =\ & H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ & +\sum_{j=1}^{t} H(S^{(j)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t)}, S^{(1)}, \ldots, S^{(j-1)}) \\ =\ & H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ & +\sum_{j=1}^{t} H(S^{(j)} \mid U_{All}^{(j)}) \quad (7) \\ =\ & H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) + \sum_{j=1}^{t} H(S^{(j)}) \quad (8) \\ =\ & H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ & +H(S^{(1)}, \ldots, S^{(t)}). \quad (9) \end{aligned}$$

(7) は，$j \neq l$ のとき，$S^{(j)}$ が $(U_{All}^{(l)}, S^{(l)})$ と独立であることから従い，(8) は定義 2 の (ii) から従い，(9) はそれぞれ $S^{(j)}$ が i.i.d. であることから従う．

一方で，

$$\begin{aligned} & H(U_{All}^{(t)}, S^{(1)}, \ldots, S^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ =\ & H(S^{(1)}, \ldots, S^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ & +H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(t)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ =\ & \sum_{j=1}^{t} H(S^{(j)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}, S^{(1)}, \ldots, S^{(j-1)}) \\ & +H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(t)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ =\ & \sum_{j=1}^{t} H(S^{(j)}) \\ & +H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(t)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \quad (10) \\ =\ & H(S^{(1)}, \ldots, S^{(t)}) \\ & +H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(t)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}). \quad (11) \end{aligned}$$

(10) と (11) は，(7)，(8)，(9) と同様の理由で従う．

従って，(9) と (11) から，

$$H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(t)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) = H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}). \quad (12)$$

次に，$H(U_{All}^{(t)}, S^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)})$ に対して，

$$\begin{aligned} & H(U_{All}^{(t)}, S^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ = \; & H(U_{All}^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ & \quad + H(S^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t)}, SK, TI^{(t)}) \\ = \; & H(U_{All}^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}). \quad (13) \end{aligned}$$

(13) は (k, n, τ)-TR-SS の Correctness から従う（つまり，$H(S^{(t)} \mid U_{All}^{(t)}, TI^{(t)}) = 0$）．

一方で，

$$\begin{aligned} & H(U_{All}^{(t)}, S^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ = \; & H(S^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ & + H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}, S^{(t)}, SK, TI^{(t)}) \\ = \; & H(S^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}). \quad (14) \end{aligned}$$

(14) は定義 1 の *Share* フェーズから従う（つまり，$H(U_{All}^{(t)} \mid S^{(t)}, SK) = 0$）．

従って，

$$\begin{aligned} & H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ & \quad + H(SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ \geq \; & H(U_{All}^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \\ = \; & H(S^{(t)}, SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \quad (15) \\ = \; & H(S^{(t)}) \\ & \quad + H(SK, TI^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}). \quad (16) \end{aligned}$$

(15) は (13) と (14) から従い，(16) は $S^{(t)}$ が $(SK, TI^{(t)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)})$ と独立であることから従う．

従って，

$$H(U_{All}^{(t)} \mid U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \geq H(S^{(t)}). \quad (17)$$

最後に，(6)，(12)，(17) から，任意の $t \in \mathcal{T}$ に対して，$H(U_{All}^{(t)} \mid S^{(1)}, \ldots, S^{(\tau)}, U_{All}^{(1)}, \ldots, U_{All}^{(t-1)}) \geq H(S^{(t)})$．

よって補題 3 は示された． □

補題 4. $H(MK) \geq \tau H(S)$.

証明.

$$\begin{aligned} H(MK) & \geq I(TI^{(1)}, \ldots, TI^{(\tau)}; MK) \\ & = H(TI^{(1)}, \ldots, TI^{(\tau)}) \\ & = \sum_{t=1}^{\tau} H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \\ & \geq \tau H(S). \end{aligned}$$

最後の不等号は補題 2 から従う． □

補題 1-4 から，定理 1 は示された． □

4.2 節で述べる構成法は，上記の不等式の全ての等号を満たす．すなわち，上記の下界はタイトである．従って，次のような (k, n, τ)-TR-SS の構成法の最適性を定義する．

定義 3. 安全な (k, n, τ)-*TR-SS* の構成法が定理 *1* の *(i)-(iv)* の全ての等号を満たすとき，その構成法は最適であるという．

注意 1. 各受信者のシェアサイズが秘密情報のサイズと等しいような秘密分散法は，しばしば *ideal* な秘密分散法と呼ばれる．4.2 節の (k, n, τ)-TR-SS の構成法は最適であり，したがって，その意味で我々は *ideal* なタイムリリース秘密分散法を達成していることになる．ここで，定理 1 の (i) の下界は通常の秘密分散法の下界と等しいことに注意する．このことから，シェアサイズに関して興味深い点は，タイムリリースの性質を実現する上で，シェアサイズに（通常の秘密分散法から）冗長性を持たせる必要がないという点である．

4 構成法

構成法として，(k, n, τ)-TR-SS の一般的構成法と，具体的構成法の 2 つの構成法を提案する．

4.1 一般的構成法

タイムリリース暗号（Timed-Release Encryption: 以下 TRE）と k-out-of-n Secret Sharing Scheme から，(k, n, τ)-TR-SS の一般的構成法を提案する．まず，k-out-of-n Secret Sharing Scheme と情報理論的に安全な TRE [7] について簡単に説明する．

k-out-of-n Secret Sharing Scheme. $\mathcal{P} := \{P_1, \ldots, P_n\}$を受信者の集合とし，$\tilde{\mathcal{S}}$を秘密情報の有限集合とする．また，任意の$i \in \{1, 2. \ldots, n\}$に対して，$\mathcal{V}_i$を$P_i$のシェアの有限集合とする．$k$-out-of-$n$ Secret Sharing Scheme Θは2つのアルゴリズム(f_{Share}, f_{Recon})と上記の有限集合から成る．f_{Share}は全ての受信者のシェアを生成する確率的アルゴリズムであり，ディーラDによって実行される．秘密情報$s \in \tilde{\mathcal{S}}$を入力し，$(v_1, v_2, \ldots, v_n) \in \prod_{i=1}^{n} \mathcal{V}_i$を出力する．$D$は各シェア$v_i$を各受信者$P_i$に安全な通信路を用いて送信する．その後，$k$人以上の受信者たちはアルゴリズム$f_{Recon}$を用いて秘密情報を復元することができる．$k$個以上の$t$個のシェアを入力し，秘密情報$s \in \tilde{\mathcal{S}}$を出力する．また，$D$が正しく$f_{Share}$を実行したならば，$k$人以上の受信者は必ず$f_{Recon}$を用いて秘密情報を正しく復元できるものとする．$k$-out-of-$n$ Secret Sharing Scheme において, 次の安全性定義を考える．

定義 4 (k-out-of-n Secret Sharing [2]). Θを*k-out-of-n Secret Sharing Scheme*とする．任意の$\mathcal{F} = \{P_{i_1}, \ldots, P_{i_j}\} \in \mathcal{PS}(\mathcal{P}, k-1)$に対して，$H(S \mid V_{\mathcal{F}}) = H(S)$を満たすとき，$\Theta$は安全であるという．$V_{\mathcal{F}}$は$\mathcal{F}$が持つシェアの集合に値をとる確率変数である．

TRE. 信頼できる第三者機関TA，タイムサーバTS，n人のユーザ$U_1, U_2, \ldots, U_n$の$n+2$人のエンティティを考える．各ユーザは送信者にも受信者にもなり得る．Σは4つのアルゴリズム (*Gen, Ext, Enc, Dec*) と，暗号文，平文，秘密鍵，マスター鍵，時刻情報の5つの空間$\mathcal{C}, \mathcal{M}, \mathcal{UK}, \mathcal{TMK}, \mathcal{ETI}$からなる．*Gen*以外のアルゴリズムは確定的である．$\tilde{\mathcal{U}} := \{U_1, \ldots, U_n\}$をユーザ集合，$\tilde{\mathcal{T}} := \{1, 2, \ldots, \tau\}$を時刻の集合とする．*Gen*は$TA$が実行する鍵生成アルゴリズムであり，セキュリティパラメータを入力とし，マスター鍵tmk^*と各ユーザの秘密鍵$uk_i := (ek_i, dk_i)(1 \leq i \leq n)$を出力する．$ek_i$は暗号化鍵，$dk_i$は復号鍵である．*Ext*は$TS$が実行する時刻情報生成アルゴリズムであり，マスター鍵tmk^*と時刻$t \in \tilde{\mathcal{T}}$を入力とし，時刻情報$tmk^{(t)} \in \mathcal{ETI}$を出力する．これを$tmk^{(t)} = Ext(tmk^*, t)$と書く．*Enc*は暗号化アルゴリズムであり，受信者に復号を許可する時刻tを指定し，平文$m \in \mathcal{M}$，暗号化鍵$ek_i \in \mathcal{EK}_i$，と受信者のID U_jを入力として，暗号文$c_{i,j}^{(t)} \in \mathcal{C}$を出力する．これを$c_{i,j}^{(t)} = Enc(m, ek_i, t, U_j)$と書く．$U_j$が$U_i$から$(c_{i,j}^{(t)}, t)$を受け取り，指定時刻$t$の時刻情報$tmk^{(t)}$を受信後，$U_j$は復号アルゴリズム*Dec*を用いて暗号文を復号する．*Dec*は$c_{i,j}^{(t)}$，復号鍵$dk_j \in \mathcal{DK}_j$，指定時刻の時刻情報$tmk^{(t)}$，送信者のID U_iを入力とし，平文mを出力する．これを$m = Dec(c_{i,j}^{(t)}, dk_j, tmk^{(t)}, U_i)$と書く．TREでは，次の3つの安全性を考える．(1) タイムサーバは，通信路上の情報や自身の鍵を用いても，平文に関する情報を何も得られない．(2) 受信者を含まない最大ω人のユーザ結託集合Wは，たとえ全ての時刻情報を知っていたとしても，平文に関する情報は何も得られない．(3) 受信者を含む最大ω人のユーザ結託集合Wでさえも，指定時刻の時刻情報がなければ，平文に関する情報は何も得られない．具体的には，TREの安全性は次のように定義される．

定義 5 (TRE [7]). Σを*TRE*とする．次の条件を満たすとき，Σは(n, ω, τ)-*secure*であるという．

(1) 任意の$U_i, U_j \in \tilde{\mathcal{U}}$と任意の$t \in \mathcal{T}$に対して，$H(M \mid C_{i,j}^{(t)}, EMK) = H(M)$.

(2) 任意の$W \in \mathcal{PS}(\tilde{\mathcal{U}}, \omega)$，$U_i, U_j \notin W$を満たす任意の$U_i, U_j \in \tilde{\mathcal{U}}$，任意の$t \in \mathcal{T}$に対して，$H(M \mid C_{i,j}^{(t)}, EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(\tau)}) = H(M)$.

(3) 任意の$W \in \mathcal{PS}(\tilde{\mathcal{U}}, \omega)$，$U_i \notin W$かつ$U_j \in W$を満たす任意の$U_i, U_j \in \tilde{\mathcal{U}}$，任意の$t \in \mathcal{T}$に対して，$H(M \mid C_{i,j}^{(t)}, EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(t-1)}, ETI^{(t+1)}, \ldots, ETI^{(\tau)}) = H(M)$.

上記の定義におけるEK_WとDK_Wは$\mathcal{EK}_W$と$\mathcal{DK}_W$にそれぞれ値をとる確率変数であり，$\mathcal{EK}_W$はWがもつ暗号化鍵の集合，$\mathcal{DK}_W$はWがもつ復号鍵の集合を示す．

(k, n, τ)-TR-SSの構成要素として，以下では$(2, 1, \tau)$-secure TREを用いる．(k, n, τ)-TR-SS

Πは，k-out-of-n Secret Sharing Scheme $\Theta = (f_{Share}, f_{Recon})$ と TRE $\Sigma = (Gen,\ Ext,\ Enc,\ Dec)$ を用いて次のように構成される．

1. *Initialize.* まず，TA はセキュリティパラメータとして 1^k を入力し，Gen を実行する．Gen はユーザ $\hat{P}_i (i = 1, 2)$ に対する秘密鍵 $uk_i = (ek_i, dk_i)(i = 1, 2)$ と tmk^* を出力する．TA は TS のマスター鍵 $mk^* := tmk^*$ と D の秘密鍵 $sk := (ek_1, dk_2)$ を安全な通信路を用いてそれぞれに送信する．

2. *Share.* まず，D は秘密情報 s を選び，$c_{1,2}^{(t)} = Enc(s, ek_1, t, \hat{P}_2)$ を計算する．次に，D は $(v_1, \ldots, v_n) \leftarrow f_{Share}(c_{1,2}^{(t)})$ を計算する．最後に，$u_i^{(t)} := (v_i, dk_2)(i = 1, 2, \ldots, n)$ とし，D は $(u_i^{(t)}, t)$ を各 $P_i (i = 1, 2, \ldots, n)$ に安全な通信路を用いて送信する．

3. *Extract.* マスター鍵 $mk^* = tmk^*$ と時刻 t を入力して，$tmk^{(t)} = Ext(tmk^*, t)$ を計算する．$mk^{(t)} := tmk^{(t)}$ を時刻 t の時刻情報とし，TS は全ての受信者に（改ざん不可な）放送通信路を用いて放送する．

4. *Reconstruct.* まず，k 人以上の受信者は $c_{1,2}^{(t)} = f_{Recon}(v_{i_1}, \ldots, v_{i_j})(k \le j \le n)$ を計算する．$mk^{(t)} = tmk^{(t)}$ の受信後，$s = Dec(c_{1,2}^{(t)},\ dk_2, tmk^{(t)}, \hat{P}_1)$ を計算し，出力する．

定理 2. 上記の (k, n, τ)-*TR-SS* の構成法で，Σ が $(2, 1, \hat{\tau})$-*secure TRE* であり，Θ が安全な $\tilde{k}$-*out-of-*$\tilde{n}$ *Secret Sharing Scheme* であるとき，Π は (k, n, τ)-*TR-SS* である．ここで，$k = \tilde{k}$，$n = \tilde{n}$，$\tau = \hat{\tau}$．また，上記構成法で必要なシェア，時刻情報，秘密鍵のサイズは以下のようになる．

$$|\mathcal{U}_i^{(t)}| = |\tilde{\mathcal{U}}_i| \cdot |\mathcal{DK}_2|, \quad |\mathcal{SK}| = |\mathcal{EK}_1| \cdot |\mathcal{DK}_2|$$
$$|\mathcal{TI}^{(t)}| = |\mathcal{ETI}^{(t)}|, \quad |\mathcal{MK}| = |\mathcal{TMK}|.$$

証明．まず，定義 2 の (i) を証明する．$k(= \tilde{k})$ 人未満の受信者が，自身の復号鍵 dk_2 と全ての時刻情報 $mk^{(1)}, \ldots, mk^{(\tau)}$ を用いて，$c_{1,2}^{(t)}$ を復元し，その後それを s に復号しようとするものとする．しかし，全ての時刻情報，復号鍵を知っていたとしても，定義 4 から，彼らは $c_{1,2}^{(t)}$ を自身のシェアから復元することができない．従って，任意の $\mathcal{F} \in \mathcal{PS}(\mathcal{P}, k-1)$ と任意の $t \in \mathcal{T}$ に対して，$H(S \mid U_{\mathcal{F}}^{(t)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(S)$．

次に，定義 2 の (ii) を証明する．任意の $\mathcal{A} \in \overline{\mathcal{PS}(\mathcal{P}, k-1)}$ と任意の $t \in \mathcal{T}$ に対して，$\mathcal{A}$ は f_{Recon} と彼らのシェアを用いることで $c_{1,2}^{(t)}$ を復元できる．しかし，定義 5 の 3 番目の条件より，指定時刻 t の時刻情報がない限り，s を $c_{1,2}^{(t)}$ から復号できない．従って，$H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(S)$． □

注意 2. もし，上記構成法において，*ideal* な k-out-of-n Secret Sharing Scheme と TRE の最適構成法を適用したとしても，(k, n, τ)-TR-SS の最適構成法とはならない．特に，シェアサイズが秘密情報のサイズより大きくなってしまう．従って，次節で定義 3 を満たすような具体的構成法を示す．

4.2 具体的構成法

以下では，(k, n, τ)-TR-SS Π の具体的構成法について述べ，その構成法が最適であることを示す．

1. *Initialize.* q を $q > \max(n, \tau)$ となるような素数べきとし，$\mathbb{F}_q$ を要素数 q の有限体とする．また各受信者 P_i の ID は $P_i \in \mathbb{F}_q \backslash \{0\}$ となるように適切に符号化されるものとする．また，適切な符号化により $\mathcal{T} = \{1, 2, \ldots, \tau\} \subset \mathbb{F}_q \backslash \{0\}$ とする．まず，TA は一様ランダムに $\mathbb{F}_q$ 上の多項式 $mk^*(y) := \sum_{i=0}^{\tau-1} b_i y^i$ を選ぶ．y の次数は高々 $\tau - 1$ である．TA は $mk^* := mk^*(y)$，また $sk := mk^*(y)$ とし，それぞれ TS と D に安全な通信路を用いて送信する[2]．

2. *Share.* まず，D は秘密情報 $s \in \mathbb{F}_q$ を選ぶ．また，D は受信者たちが復元できる時刻 t を指定し，$mk^{(t)} := mk^*(t)$ を計算する．次に，$c^{(t)} := s + mk^{(t)}$ とし，D はランダムに $\mathbb{F}_q$ 上の多項式 $f(x) := c^{(t)} +$

[2]本構成法では，定理 1 で見られるように，mk^* と sk の下界は等しいことから，mk^* と sk を同じものとして考える．

$\sum_{i=1}^{k-1} a_i x^i$ を選ぶ．各係数 a_i は $\mathbb{F}_q$ から一様ランダムに選ばれる．最後に，D は $u_i^{(t)} := f(P_i)(i = 1, 2, \ldots, n)$ を計算し，$(u_i^{(t)}, t)$ を $P_i(i = 1, 2, \ldots, n)$ に安全な通信路を通じて送信する．

3. *Extract.* $mk^* = mk^*(y)$ と時刻 $t \in \mathcal{T}$ を用いて，TS は時刻 t の時刻情報 $mk^{(t)} := mk^*(t)$ を計算する．その後，TS は全ての受信者に改ざん不可な放送通信路を通じてその時刻情報を放送する．

4. *Reconstruct.* まず，$\mathcal{A} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_k}\} \in \overline{\mathcal{PS}(\mathcal{P}, k-1)}$ は k 個のシェアとラグランジュ補間を用いて $c^{(t)}$ を次のように計算する．

$$c^{(t)} = \sum_{j=1}^{k} (\prod_{l \neq j} \frac{P_{i_j}}{P_{i_j} - P_{i_l}}) f(P_{i_j}).$$

指定時刻の時刻情報 $mk^{(t)} = mk^*(t)$ を受信後，彼らは $s = c^{(t)} - mk^{(t)}$ を得ることができる．

定理 3. 上記の (k, n, τ)-*TR-SS* Π の構成法は安全かつ最適である．

証明. まず，定義 2 の (i) を証明する．$k-1$ 人の受信者 $\mathcal{F} = \{P_{i_1}, \ldots, P_{i_{k-1}}\}$ が，自身のシェアを用いて，$c_{1,2}^{(t)}$ を知ろうとするものとする．彼らは $mk^*(t) = c^{(t)} - s$ を知っているが，$f(x)$ の次数は $k-1$ のため，$k-1$ 個のシェアからは $f(x)$ を知ることができない．従って，任意の $\mathcal{F} \in \mathcal{PS}(\mathcal{P}, k-1)$ と任意の $t \in \mathcal{T}$ に対して，$H(S \mid U_{\mathcal{F}}^{(t)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(S)$.

次に，定義 2 の (ii) を証明する．任意の $\mathcal{A} \in \overline{\mathcal{PS}(\mathcal{P}, k-1)}$ と任意の $t \in \mathcal{T}$ に対して，まず $\mathcal{A}$ は彼らのシェアを復元し，$c^{(t)} = s + mk^*(t)$ を得ることができる．しかし，$mk^*(y)$ の次数は $\tau - 1$ のため，$\tau - 1$ 個の時刻情報からは $mk^*(y)$ を知ることができない．従って，$H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(S)$.

また，本構成法が定理 1 の全ての不等式の等号を満たしていることは容易にわかる． □

5 まとめと今後の課題

世界で初めて情報理論的に安全なタイムリリース秘密分散法（TR-SS）について提案した．具体的には，(k, n, τ)-TR-SS のモデル，安全性定義を提案し，シェア，時刻情報，秘密鍵のサイズの下界をそれぞれ導出した．更に，一般的構成法と最適な具体的構成法をそれぞれ提案した．

参考文献

[1] Blakley, G.R.: Safeguarding cryptographic keys. In: AFIPS 1979 National Computer Conference, vol.48, pp.313-317. (1979)

[2] Karnin, E.D., Greene, J.W., Hellman, M.E.: On Secret Sharing Systems. In: IEEE Trans. Information Theory, 29(1), pp.35-41. (1983)

[3] May, T.C.: Timed-release crypto. manuscript. (1993)

[4] Rivest, R.: Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer. manuscript. (1999) Available at `http://people.csail.mit.edu/rivest/Rivest-commitment.pdf`

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

[6] Shamir, A.: How to share a secret. In: Communication of the ACM 22, pp.612-613. (1979)

[7] Watanabe, Y., Seito, T., Shikata, J.: Information-Theoretic Timed-Release Security: Key-Agreement, Encryption, and Authentication Codes. In: Smith, A. (ed.) ICITS2012, LNCS 7412, pp. 167-186. Springer, Heidelberg(2012). A full version is available at `http://eprint.iacr.org/2012/460`