受信者集合を変更可能な情報理論的安全性に基づく放送型暗号

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@ynu.jp, shikata@ynu.ac.jp

あらまし 放送型暗号は，受信者集合を指定することで，復号できるユーザを指定可能な暗号化方式であり，デジタル著作権管理等，幅広く利用されている．本稿では，暗号文の受信者集合を変更可能な情報理論的安全性に基づく放送型暗号を提案する．本方式では，暗号文がクラウドデータストレージのような外部ストレージに保存されていることを想定しており，復号することなく暗号文を更新し，受信者集合を変更可能である．従って，暗号文を復号できるユーザを動的に管理可能であり，クラウドデータストレージを利用したサービスにより適した放送型暗号といえる．本稿では，本方式の数理モデル及び安全性の定式化を行い，鍵長のタイトな下界を導出し，その下界の等号をみたすような構成法を提案する．本稿の下界に関する成果は通常の放送型暗号にも適用可能であり，結果として通常の放送型暗号における新たな結果を示すことにも繋がっている．

Information-Theoretically Secure Revocable-Storage Broadcast Encryption

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@ynu.jp, shikata@ynu.ac.jp

Abstract In broadcast encryption, a sender specifies a subset of a user set, called a privilege set, and encrypts a plaintext in such a way that only each user in the privilege set can decrypt the ciphertext. In this paper, we first propose revocable-storage broadcast encryption (RS-BE) with information-theoretic security. In RS-BE, we assume ciphertexts are stored in an external storage such as a cloud data storage, and a ciphertext can be updated with a new privilege set without decryption (i.e. without leaking any information on the underlying plaintext). Specifically, in this paper we define a mathematical model and security of RS-BE, derive tight lower bounds on secret keys required for RS-BE, and propose an optimal construction of RS-BE.

1 はじめに

現代社会において，多くの情報は電子化され，インターネットを通じて様々な方法で利用されている．このような電子化された情報は文書，画像，音楽等の著作物を多く含んでおり，適切な管理が必要不可欠である．そのための技術として様々な暗号技術が用いられており，なかでも放送型暗号（Broadcast Encryption: BE）は，デジタル著作権管理や有料放送の管理等に幅広く利用されている暗号化方式である．BE は Berkovits [1] によって最初に提案された暗号化

方式であり，暗号文を復号できる受信者を任意に指定することができる暗号化方式である（この “復号できる受信者たちの集合” を受信者集合とよぶ）．BE はそれぞれ，情報理論的安全性に基づくもの，計算量的安全性に基づくものについて様々な研究が進められている．特に，本稿で扱う情報理論的安全性に基づく BE に関しては [3, 4, 7, 1, 6] 等で研究が進められてきた．

また，近年，クラウドコンピューティングの発展が目覚ましく，それらを利用したサービスも急速に普及し始めている．そのような状況の中で，Sahai ら [8] はクラウドデータストレージに暗号文が保存されていることを想定し，動的に暗号文の属性を変更することが可能な属性ベース暗号を提案した．このようなクラウドデータストレージを利用した暗号技術はこれからの情報社会にとって非常に有用であると考えられるが，実社会で広く利用されている BE における同様のコンセプトを持つ方式は未だ存在しない．

本稿では，Berkovits [1] や Fiat，Naor[6] がまず最初に情報理論的安全性に基づく BE から考察を始めたように，情報理論的安全性の枠組みにおいて同様のコンセプトに基づいた BE について考察し，受信者集合を動的に変更可能な BE(Revocable-Storage Broadcast Encryption: RS-BE) を提案する．具体的には，RS-BE の数理モデル，安全性を定式化し，RS-BE に必要な秘密鍵長のタイトな下界を導出し，その下界をみたすような構成法を提案する．特に，本稿の秘密鍵長の下界に関する成果は，通常の情報理論的に安全な BE に適用することが可能である．情報理論的に安全な BE の秘密鍵長の下界に関する研究として，[3, 4, 7] 等が知られているが，このうち [3] は鍵配送方式（Key Predistribution System: KPS）の観点から見た下界であり，[7] は KPS と (one-time secure) BE の同値性を示したうえで [3] の結果から [4] よりタイトな下界を導出することに成功しているが，暗号化鍵に関する下界については触れられていない．一方で，本稿では，暗号化鍵と復号鍵の両方において，タイトな下界を導出することに成功した．このうち，復号鍵の下界は [7] の結果と一致しており，また暗号化鍵の下界については著者の知る限り世界で初の成果である．

RS-BE には多くのアプリケーションが考えられるが，ここでは動画や音楽をストリーミング配信するサービスを例に挙げる．現在，こうしたサービスはパスワード等で利用者が正規の利用者かを判断し，サービスにログインすることでコンテンツが利用可能になるものが多い．コンテンツを通常の BE を用いて暗号化したとしても，このようにサービスの入り口で制御する必要がある．なぜなら，利用者がサービスを退会した後も既存の暗号文の受信者集合には含まれたままのため，退会前の復号鍵を保持していれば再びアクセス，復号できてしまうからである．しかし，RS-BE を用いることで，退会した利用者を受信者集合から取り除くようにコンテンツの暗号文を更新することで，以前は利用できたはずのコンテンツに後からアクセスしても利用できなくさせることが可能となる．すなわち，ログインによる制御が不要となり，パスワード管理等の負担を軽減することができる．更に，復号することなく暗号文を更新可能なため，更新時にコンテンツに関する情報が漏れない．従って，更新管理も第三者に委託することが可能となる．

本方式の関連研究として，上で述べた [8] の他に代理人再暗号化方式（Proxy Re-Encryption: PRE）[2] がある．PRE は，暗号文を復号できるエンティティを復号することなく変更することができる暗号化方式であり，特に放送型 PRE として [5] 等がある．しかし，既存研究はいずれも計算量的安全性の枠組みにおける方式であり，本方式は初の情報理論的安全性に基づく PRE と見ることもできる．

2 RS-BE

本節では，受信者集合を変更可能な情報理論的に安全な放送型暗号 (RS-BE) を提案する．

2.1 モデル

本モデルでは，送信者 E，n 人の受信者 $U_1, \ldots, U_n$，ストレージ管理者 SM が登場する．プロ

トコルの流れは以下の通りである．まず，E は鍵生成を行い，暗号化鍵，n 個の復号鍵，メンテナンス鍵を生成し，各復号鍵，メンテナンス鍵をそれぞれ，$U_1, \ldots, U_n$，SM に安全な通信路を通じて送信する．E は，受信者集合を指定し，暗号化鍵を用いて平文を暗号化，ストレージに保存する．本方式では，各受信者 U_i は暗号文を取得するため，自身でストレージにアクセスする必要がある．U_i が取得した暗号文の受信者集合に含まれていれば暗号文を復号でき，そうでなければ暗号文を復号できない．また，(送信者の依頼等のルールに従い) SM は自身のメンテナンス鍵を用いて暗号文の受信者集合を変更可能である．変更後の受信者集合に含まれていない受信者 U_i は，たとえ自身が変更前の受信者集合に含まれていたとしても，復号することができなくなる．RS-BE Π を次のように定義する．

定義 1 (RS-BE). RS-BE Π は，E，SM，$U_1, \ldots, U_n$ の $n+2$ のエンティティ，$\mathcal{M}$，$\mathcal{C}$，$\mathcal{EK}$，$\mathcal{MK}$，$\mathcal{DK}$ の 5 つの空間が登場し，以下の 4 つのアルゴリズム ($Setup$, Enc, Dec, Upd) から成る:

- エンティティ: E は送信者，SM はストレージ管理者，$U_1, \ldots, U_n$ は n 人の受信者であり，$\mathcal{U} := \{U_1, \ldots, U_n\}$ を受信者全体の集合とする．
- 空間: $\mathcal{M}$ は平文集合である．任意の部分集合 $\mathcal{J} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$ に対して，$\mathcal{C}_\mathcal{J}$ を受信者集合 $\mathcal{J}$ に対する暗号文集合と定義し，$\mathcal{C} := \bigcup_{\mathcal{J} \subset \mathcal{U}} \mathcal{C}_\mathcal{J}$ とする．$\mathcal{EK}$ は暗号化鍵の集合，$\mathcal{MK}$ はメンテナンス鍵の集合である．$\mathcal{DK}_i$ は受信者 U_i の復号鍵の集合であり，$\mathcal{DK} := \bigcup_{i=1}^{n} \mathcal{DK}_i$ とする．

1. $(ek, mk, dk_1, \ldots, dk_n) \leftarrow Setup(1^\lambda, n)$: セキュリティパラメータ λ，受信者の人数 n を入力とし，暗号化鍵 $ek \in \mathcal{EK}$，メンテナンス鍵 $mk \in \mathcal{MK}$，復号鍵 $dk_1, \ldots, dk_n \in \prod_{i=1}^{n} \mathcal{DK}_i$ を生成する確率的アルゴリズム．E が実行し，ek は自身が保持し，$mk, dk_1, \ldots, dk_n$ はそれぞれ $SM, U_1, \ldots, U_n$ に安全な通信路を通じて配布される．
2. $c_\mathcal{S} \leftarrow Enc(ek, m, \mathcal{S})$: 暗号化鍵 ek，平文 $m \in \mathcal{M}$，受信者集合 $\mathcal{S} \subset \mathcal{U}$ を入力とし，暗号文 $c_\mathcal{S}$ を出力する確定的アルゴリズム．S が実行し，出力された暗号文 $c_\mathcal{S}$ をクラウドストレージに保存・公開する．
3. m or $\perp \leftarrow Dec(dk_i, c_\mathcal{S}, \mathcal{S}, U_i)$: ユーザ U_i の復号鍵 dk_i，暗号文 $c_\mathcal{S}$，受信者集合 $\mathcal{S}$，自身の ID U_i を入力し，平文 m または $\perp$ を出力する確定的アルゴリズム．U_i がクラウドストレージから $c_\mathcal{S}$ を取得し，実行する．
4. $c_{\mathcal{S}'}$ or $\perp \leftarrow Upd(mk, c_\mathcal{S}, \mathcal{S}, \mathcal{S}')$: メンテナンス鍵 mk，受信者集合 $\mathcal{S}$ の暗号文 $c_\mathcal{S}$，新たな受信者集合 $\mathcal{S}'$ を入力とし，受信者集合 $\mathcal{S}'$ の暗号文 $c_{\mathcal{S}'}$ または $\perp$ を出力する確定的アルゴリズム．SM が実行し，クラウドストレージ上の暗号文を更新する．

Π は，以下の性質を満たす．

(a) すべての $\lambda, n \in \mathbb{N}$，すべての $(ek, mk, dk_1, \ldots, dk_n) \leftarrow Setup(1^\lambda, n)$，すべての $m \in \mathcal{M}$，すべての $\mathcal{S} \subset \mathcal{U}$，すべての $U_i \in \mathcal{S}$ に対して，$m \leftarrow Dec(dk_i, Enc(ek, m, \mathcal{S}), \mathcal{S}, U_i)$.

(b) すべての $\lambda, n \in \mathbb{N}$，すべての $(ek, mk, dk_1, \ldots, dk_n) \leftarrow Setup(1^\lambda, n)$，すべての $m \in \mathcal{M}$，すべての $\mathcal{S}, \mathcal{S}' \subset \mathcal{U}$ に対して，$Upd(mk, Enc(ek, m, \mathcal{S}), \mathcal{S}') = Enc(ek, m, \mathcal{S}')$.

すなわち，(a) は復号の正しさを，(b) は更新の正しさを示している．

また，上記の RS-BE は one-time モデルであるとする．one-time モデルとは，Enc アルゴリズムを実行し，E がストレージに暗号文を保存するのが高々1 回であるモデルである．

2.2 安全性

RS-BE では，次の安全性を考える: (1) 通常の BE 同様，受信者集合以外の受信者は，暗号文から平文に関する情報を一切得ることはできないという安全性; (2) SM も暗号文から平文に関する情報を一切得ることは出来ないという安全性．高々ω ($< n$) 人の結託した受信者の集合 (以下，結託者集合とよぶ) を W とする．以下では，

任意の部分集合 $\mathcal{J} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$ に対して，$\mathcal{DK}_{\mathcal{J}} := \mathcal{DK}_{i_1} \times \cdots \times \mathcal{DK}_{i_j}$ とし，また，M，$C_{\mathcal{S}}$，EK，DK_i $(1 \leq i \leq n)$，$DK_{\mathcal{J}}$ $(\mathcal{J} \subset \mathcal{U})$，$MK$ は，$\mathcal{M}$，$\mathcal{C}_{\mathcal{S}}$，$\mathcal{EK}$，$\mathcal{DK}_i$ $(1 \leq i \leq n)$，$\mathcal{DK}_{\mathcal{J}}$ $(\mathcal{J} \subset \mathcal{U})$，$\mathcal{MK}$ に値をとる確率変数とする．

定義 2 (RS-BE の安全性). RS-BE Π は，以下の条件をみたすとき，$(\leq n, \leq \omega)$-one-time secure であるという:

(1) 任意の受信者集合 $\mathcal{S} \subset \mathcal{U}$，$\mathcal{S} \cap W = \emptyset$ かつ $|W| \leq \omega$ となるような任意の結託者集合 $W \subset \mathcal{U}$ に対して，

$$H(M \mid C_{\mathcal{S}}, DK_W) = H(M).$$

(2) 任意の受信者集合 $\mathcal{S} \subset \mathcal{U}$ に対して，

$$H(M \mid C_{\mathcal{S}}, MK) = H(M).$$

注意 1. 定義 1 において SM が存在せず（すなわち mk を空の文字列とし，Upd アルゴリズムを考えない），またそれに伴い定義 2 の (2) を考慮しない場合，通常の BE と同様の定義となる．従って，通常の BE の自然な拡張となっていることがわかる．

注意 2. 上記の安全性定義は，結託者集合がストレージにアクセスし，暗号文を取得するのが高々1 回であることを暗に示している．現実的に考えて，結託者たちは自由にストレージにアクセスし，受信者集合が更新された暗号文を複数種類取得できるものとするのが自然である．実は，そのようなより現実的な安全性定義を考えても，上記の定義と同様の鍵長の下界，またその下界と等号をみたすような最適な構成法を得ることができる（詳しくは 5 節参照）．それに加えて，通常の BE の自然な拡張とするために，上記のような弱い安全性から考えている．

3 鍵長の下界

RS-BE に関して，必要な鍵長の下界について述べる．[4] で述べられているように，通常の BE に関して，暗号文長と秘密鍵長にはトレードオフが存在することが知られている[1]．これは RS-BE においても同様である．本稿では，暗号文長が平文長と等しい場合（すべての $\mathcal{S} \subset \mathcal{U}$ に対して $\log_2 |\mathcal{C}_{\mathcal{S}}| = \log_2 |\mathcal{M}|$，すなわち $H(C_{\mathcal{S}}) = H(M)$ の場合）における秘密鍵長の下界を考える．

定理 1. Π を $(\leq n, \leq \omega)$-one-time secure RS-BE とする．このとき，すべての $\mathcal{S} \subset \mathcal{U}$ に対して $H(C_{\mathcal{S}}) = H(M)$ という仮定のもとで，鍵長の下界は以下のようになる:

(i) $H(EK) \geq \sum_{j=0}^{\omega} \binom{n}{j} H(M)$,

(ii) $H(DK_i) \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(M)$,

(iii) $H(MK) \geq \left(\sum_{j=0}^{\omega} \binom{n}{j} - 1 \right) H(M)$.

証明．以下の補題に従う．

補題 1. 任意の受信者集合 $\mathcal{S} \subset \mathcal{U}$ と，$W \cap \mathcal{S} = \emptyset$ かつ $|W| \leq \omega$ となるような任意の結託者集合 $W \subset \mathcal{U}$ に対して，Y_i $(1 \leq i \leq k)$ を $Y_i \cap W \neq \emptyset$ となるような受信者集合とする．このとき，すべての $\mathcal{S} \subset \mathcal{U}$ に対して $H(C_{\mathcal{S}}) = H(M)$ ならば，$H(C_{\mathcal{S}} \mid M, C_{Y_1}, \ldots, C_{Y_k}, DK_W) \geq H(M)$.

証明．まず，任意の $\mathcal{S} \subset \mathcal{U}$，$U_i \in \mathcal{S}$ に対して，

$$\begin{aligned} H(C_{\mathcal{S}}) \geq & H(C_{\mathcal{S}} \mid DK_i) && (1) \\ \geq & H(C_{\mathcal{S}} \mid DK_i) - H(C_{\mathcal{S}} \mid DK_i, M) && (2) \\ = & I(C_{\mathcal{S}}; M \mid DK_i) \\ = & H(M \mid DK_i) - H(M \mid DK_i, C_{\mathcal{S}}) \\ = & H(M). \end{aligned}$$

最後の等号は M と DK_i が独立であることと，復号の正しさから従う（すなわち $H(M \mid DK_i, C_{\mathcal{S}}) = 0$）．ここで，$H(C_{\mathcal{S}}) = H(M)$ の仮定より，(1)=(2)，すなわち

$$H(C_{\mathcal{S}} \mid DK_i)$$

[1] 実際，暗号文長に制限を加えない場合，定理 1 より大幅に小さい秘密鍵長で，比較的自明に $(\leq n, \leq \omega)$-one-time secure BE を構成することが可能である．

$$=H(C_{\mathcal{S}} \mid DK_i) - H(C_{\mathcal{S}} \mid DK_i, M),$$

が成り立つ．従って，

$$H(C_{\mathcal{S}} \mid DK_i, M) = 0. \tag{3}$$

ここで，$H(M, C_{\mathcal{S}}, C_{Y_1}, \ldots, C_{Y_k} \mid DK_W)$ に対して，

$$\begin{aligned}
&H(M, C_{\mathcal{S}}, C_{Y_1}, \ldots, C_{Y_k} \mid DK_W) \\
=&H(C_{\mathcal{S}} \mid DK_W) + H(M \mid DK_W, C_{\mathcal{S}}) \\
&+ H(C_{Y_1}, \ldots, C_{Y_k} \mid DK_W, C_{\mathcal{S}}, M) \\
=&H(C_{\mathcal{S}} \mid DK_W) + H(M) \\
&+ H(C_{Y_1}, \ldots, C_{Y_k} \mid DK_W, C_{\mathcal{S}}, M) \quad (4) \\
=&H(C_{\mathcal{S}} \mid DK_W) + H(M). \quad (5)
\end{aligned}$$

(4) は定義2の (1) から従い，(5) は任意の Y_j $(1 \leq j \leq k)$ に対して，$Y_j \cap W \neq \emptyset$ であるため，(3) から従う（すなわち $H(C_{Y_j} \mid DK_W, M) = 0$）．

一方，同様に $H(M, C_{\mathcal{S}}, C_{Y_1}, \ldots, C_{Y_k} \mid DK_W)$ に対して，

$$\begin{aligned}
&H(M, C_{\mathcal{S}}, C_{Y_1}, \ldots, C_{Y_k} \mid DK_W) \\
=&H(M \mid DK_W) + H(C_{Y_1}, \ldots, C_{Y_k} \mid DK_W, M) \\
&+ H(C_{\mathcal{S}} \mid DK_W, M, C_{Y_1}, \ldots, C_{Y_k}) \\
=&H(M) + H(C_{\mathcal{S}} \mid DK_W, M, C_{Y_1}, \ldots, C_{Y_k}). \quad (6)
\end{aligned}$$

(6) は M と DK_W の独立性と (5) と同様の理由から従う．

従って，(5)=(6)，すなわち

$$\begin{aligned}
&H(C_{\mathcal{S}} \mid DK_W, M, C_{Y_1}, \ldots, C_{Y_k}) \\
=&H(C_{\mathcal{S}} \mid DK_W), \quad (7)
\end{aligned}$$

が得られるので，以下では $H(C_{\mathcal{S}} \mid DK_W) \geq H(M)$ を示す．

$H(M, C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_W, EK)$ に対して，

$$\begin{aligned}
&H(M, C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_W, EK) \\
=&H(C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_W, EK) \\
&+ H(M \mid DK_{\mathcal{S}}, DK_W, EK, C_{\mathcal{S}}) \\
=&H(C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_W, EK). \quad (8)
\end{aligned}$$

(8) は復号の正しさ（$H(M \mid DK_{\mathcal{S}}, C_{\mathcal{S}}) = 0$）から従う．

一方，同様に $H(M, C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_W, EK)$ に対して，

$$\begin{aligned}
&H(M, C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_W, EK) \\
=&H(M \mid DK_{\mathcal{S}}, DK_W, EK) \\
&+ H(C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_W, EK, M) \\
=&H(M \mid DK_{\mathcal{S}}, DK_W, EK). \quad (9)
\end{aligned}$$

(9) は暗号化アルゴリズム Enc（$H(C_{\mathcal{S}} \mid EK, M) = 0$）から従う．

従って，

$$\begin{aligned}
H(C_{\mathcal{S}}|DK_W) \geq&H(C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_W, EK) \\
=&H(M \mid DK_{\mathcal{S}}, DK_W, EK) \quad (10) \\
=&H(M). \quad (11)
\end{aligned}$$

(10) は (8)=(9) から従い，(11) は M と $EK, DK_1, \ldots, DK_n$ が独立であることから従う．

(7)，(11) より，$H(C_{\mathcal{S}} \mid M, C_{Y_1}, \ldots, C_{Y_k}, DK_W) \geq H(M)$． □

補題 2. すべての $\mathcal{S} \subset \mathcal{U}$ に対して $H(C_{\mathcal{S}}) = H(M)$ のとき，$H(EK) \geq \sum_{j=0}^{\omega} \binom{n}{j} H(M)$．

証明．まず，すべての結託者集合 W の集合族を $\mathscr{W} := \{\mathcal{W} \subset \mathcal{U} \mid |W| \leq \omega\}$ と定義する．次に，すべての結託者集合 W に対して，結託者以外の全員が含まれる受信者集合の集合族を $\mathscr{S} := \{\mathcal{S} \subset \mathcal{U} \mid W \in \mathscr{W}, \mathcal{S} = \mathcal{U} \setminus W\} = \{\mathcal{S}_1, \ldots, \mathcal{S}_t\}$ と定義する．一般性を失わずに $|\mathcal{S}_1| \geq \cdots \geq |\mathcal{S}_t|$ とする．$|\mathscr{W}| = \sum_{j=0}^{\omega} \binom{n}{j}$ であるから，$|\mathscr{S}| = t = \sum_{j=0}^{\omega} \binom{n}{j}$ である．また，$\mathcal{S}_j \in \mathscr{S}$ $(1 \leq j \leq t)$ に対応する結託者集合を $W_j \in \mathscr{W}$ とかく．すなわち，$W_j = \mathcal{U} \setminus \mathcal{S}_j$．このとき，

$$\begin{aligned}
&H(EK) \\
=&H(EK \mid M) \quad (12) \\
\geq&I(EK; C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid M) \\
=&H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid M) \\
&- H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid M, EK) \\
=&H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid M) \quad (13)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{j=1}^{t} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}) \\
&\geq \sum_{j=1}^{t} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}, DK_{W_j}) \\
&\geq \sum_{j=0}^{\omega} \binom{n}{j} H(M). \qquad (14)
\end{aligned}
$$

(12) は M と EK の独立性から従い，(13) は暗号化アルゴリズム Enc から従い（すなわち $H(C_{\mathcal{S}_i} \mid EK, M) = 0$ $(1 \leq i \leq t)$），(14) は補題 1 から従う． □

補題 3. すべての $\mathcal{S} \subset \mathcal{U}$ に対して $H(C_{\mathcal{S}}) = H(M)$ のとき，任意の $i \in \{1, \ldots, n\}$ に対して，$H(DK_i) \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(M)$.

証明．まず，U_i が含まれないようなすべての結託者集合 W の集合族を $\mathscr{W}^{(i)} := \{\mathcal{W} \subset \mathcal{U} \setminus \{U_i\} \mid |W| \leq \omega\}$ と定義する．次に，U_i が含まれないようなすべての結託者集合 W に対して，結託者以外の全員が含まれる受信者集合の集合族を $\mathscr{S}^{(i)} := \{\mathcal{S} \subset \mathcal{U} \mid W \in \mathscr{W}^{(i)}, \mathcal{S} = \mathcal{U} \setminus W\} = \{\mathcal{S}_1, \ldots, \mathcal{S}_\ell\}$ 一般性を失わずに $|\mathcal{S}_1| \geq \cdots \geq |\mathcal{S}_\ell|$ とする．$|\mathscr{W}^{(i)}| = \sum_{j=0}^{\omega} \binom{n-1}{j}$ であるから，$|\mathscr{S}^{(i)}| = \ell = \sum_{j=0}^{\omega} \binom{n-1}{j}$ である．ここで，どの $\mathcal{S} \in \mathscr{S}^{(i)}$ に対しても，$U_i \in \mathcal{S}$ であることに留意する．また，$\mathcal{S}_j \in \mathscr{S}^{(i)}$ $(1 \leq j \leq \ell)$ に対応する結託者集合を $W_j \in \mathscr{W}^{(i)}$ とかく．すなわち，$W_j = \mathcal{U} \setminus \mathcal{S}_j$．このとき，

$$
\begin{aligned}
&H(DK_i) \\
=&H(DK_i \mid M) \qquad (15) \\
\geq&I(DK_i; C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) \\
=&H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) \\
&\quad - H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M, DK_i) \\
=&H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) \qquad (16) \\
=&\sum_{j=1}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}) \\
\geq&\sum_{j=1}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}, DK_{W_j}) \\
\geq&\sum_{j=0}^{\omega} \binom{n-1}{j} H(M). \qquad (17)
\end{aligned}
$$

(15) は M と DK_i の独立性から従い，(16) は補題 1 の (3) から従い（すなわち $H(C_{\mathcal{S}_j} \mid DK_i, M) = 0$ $(1 \leq j \leq \ell)$），(17) は補題 1 から従う． □

補題 4. 全ての $\mathcal{S} \subset \mathcal{U}$ に対して $H(C_{\mathcal{S}}) = H(M)$ のとき，$H(MK) \geq \left(\sum_{j=0}^{\omega} \binom{n}{j} - 1\right) H(M)$.

証明．$\mathscr{W}, \mathscr{S}$ を補題 2 で定義したものと同様のものとする．このとき，

$$
\begin{aligned}
&H(MK) \\
\geq&H(MK \mid C_{\mathcal{S}_1}) \\
\geq&I(MK; C_{\mathcal{S}_2}, \ldots, C_{\mathcal{S}_t} \mid C_{\mathcal{S}_1}) \\
=&H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid C_{\mathcal{S}_1}) \\
&\quad - H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid C_{\mathcal{S}_1}, MK) \\
=&H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid C_{\mathcal{S}_1}) \qquad (18) \\
=&\sum_{j=2}^{t} H(C_{\mathcal{S}_j} \mid C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}) \\
\geq&\sum_{j=2}^{t} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}, DK_{W_j}) \\
\geq&\left(\sum_{j=0}^{\omega} \binom{n}{j} - 1\right) H(M). \qquad (19)
\end{aligned}
$$

(18) は更新アルゴリズム Upd から従い（すなわち $H(C_{\mathcal{S}_i} \mid C_{\mathcal{S}_1}, MK) = 0$ $(2 \leq i \leq t)$），(19) は補題 1 から従う． □

4 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，次のように $(\leq n, \leq \omega)$-one-time secure RS-BE の構成法の最適性を定義する．

定義 3. $(\leq n, \leq \omega)$-one-time secure RS-BE Π の構成法が定理 1 の (i)-(iii) 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 3. 上記の定理における (i)，(ii) は，通常の BE にも適用可能である．復号鍵の BE の既存のタイトな下界として [7] の成果が知られているが，暗号化鍵のタイトな下界を導出したのは本成果が初である．興味深い点として，上記の定理は，$(\leq n, \leq \omega)$-one-time secure BE における暗号鍵長や復号鍵長を変化させることなく，受信者集合を更新する機能を実現可能であることを示している．

4 最適構成法

本節では，$(\leq n, \leq \omega)$-one-time secure RS-BE の最適構成法について述べる．本構成法は Fiat–Naor KPS 方式 [6] をベースとしている[2]．以下では，各集合族を以下のように定義する．

$$\mathscr{W} := \{\mathcal{W} \subset \mathcal{U} \mid |W| \leq \omega\},$$
$$\mathscr{W}^{(i)} := \{\mathcal{W} \subset \mathcal{U} \setminus \{U_i\} \mid |W| \leq \omega\},$$
$$\mathscr{W}(\mathcal{S}) := \{W \in \mathscr{W} \mid W \cap \mathcal{S} = \emptyset\}.$$

構成法は以下の通りである．

1. $(ek, mk, dk_1, \ldots, dk_n) \leftarrow \mathit{Setup}(1^\lambda, n)$: q を $q > n$ 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．まず，各 $W \in \mathscr{W}$ に対して，一様ランダムに $r_W \in \mathbb{F}_q$ を選ぶ．$ek := \{r_W \mid W \in \mathscr{W}\}$，$dk_i := \{r_W \mid W \in \mathscr{W}^{(i)}\}$ $(1 \leq i \leq n)$，$mk := \{r_W \mid W \in \mathscr{W} \setminus \{\emptyset\}\}$ を出力する．

2. $c_\mathcal{S} \leftarrow \mathit{Enc}(ek, m, \mathcal{S})$: 受信者集合 $\mathcal{S}$ に対して，セッション鍵
$$k_\mathcal{S} := \sum_{W \in \mathscr{W}(\mathcal{S})} r_W,$$
を生成し，$c_\mathcal{S} := m + k_\mathcal{S}$ を出力する．

3. m or $\perp \leftarrow \mathit{Dec}(dk_i, c_\mathcal{S}, \mathcal{S}, U_i)$: もし $U_i \in \mathcal{S}$ ならば，$m = c_\mathcal{S} - k_\mathcal{S}$ を計算し，出力する．そうでなければ $\perp$ を出力する．

4. $c_{\mathcal{S}'}$ or $\perp \leftarrow \mathit{Upd}(mk, c_\mathcal{S}, \mathcal{S}, \mathcal{S}')$: 各受信者集合 $\mathcal{S}, \mathcal{S}'$ に対して，更新鍵
$$uk_{\mathcal{S}\to\mathcal{S}'} := \sum_{W \in \mathscr{W}(\mathcal{S}')\setminus\{\emptyset\}} r_W - \sum_{W \in \mathscr{W}(\mathcal{S})\setminus\{\emptyset\}} r_W,$$
を計算し，$c_{\mathcal{S}'} := c_\mathcal{S} + uk_{\mathcal{S}\to\mathcal{S}'}$ を出力する．

以下の定理を得る．

定理 2. 上記の RS-BE Π の構成法は $(\leq n, \leq \omega)$-one-time secure かつ最適である．

[2]定理 1 の (i)，(ii) において等号を満たすような構成法を $(\leq n, \leq \omega)$-one-time secure BE の最適構成法とすると，その最適構成法は Fiat–Naor KPS 方式と one-time pad から得ることができる．

証明. まず定義 2 の (1) が成り立つことの証明を行う．結託者 W は $k_\mathcal{S}$ を推測することを目指す．W が持っている鍵は $\{r_W \mid W \in \bigcup_{U_i \in W} \mathscr{W}^{(i)}\}$ であるが，$\mathscr{W}(\mathcal{S})$ は $\bigcup_{U_i \in W} \mathscr{W}^{(i)}$ の部分集合族ではないため，少なくとも $\{r_W \mid W \in \mathscr{W}(\mathcal{S}) \setminus \mathscr{W}(\mathcal{S}) \cap \bigcup_{U_i \in W} \mathscr{W}^{(i)}\}$ が 1 つは存在し，W はそれらを推測する必要がある．従って，任意の $\mathcal{S} \subset \mathcal{U}$，$\mathcal{S} \cap W = \emptyset$ かつ $|W| \leq \omega$ となるような任意の $W \subset \mathcal{U}$ に対して，$H(M \mid C_\mathcal{S}, DK_W) = H(M)$．

次に定義 2 の (2) が成り立つことを示す．SM は $r_\emptyset$ 以外のすべての鍵を持つが，どんな $\mathcal{S} \subset \mathcal{U}$ に対する暗号文も $r_\emptyset$ が用いられているため，SM はそれをランダムに推測する必要がある．従って，任意の $\mathcal{S} \subset \mathcal{U}$ に対して，$H(M \mid C_\mathcal{S}, MK) = H(M)$．

また，鍵長がそれぞれ定理 1 の (i)-(iii) と等号を満たすのは明らかであるので，この構成法は最適である． □

5 より強い安全性をもつ RS-BE

本節では，定義 2 より強い安全性をもつ RS-BE について議論する．

複数回のストレージアクセスに対して安全な RS-BE. 定義 2 における安全性は，結託者集合 W が自身が含まれない受信者集合 $\mathcal{S}$ の暗号文を “1 つ” 見たときに，平文に関する情報を何も得ることができない，というものであった．本方式は暗号化は 1 度のみ行われるが，更新については回数制限はないため，W が更新された暗号文を複数回取得することできると考えるのが現実的である．従って，より強くかつ自然な安全性定義として，以下のものが考えられる．

定義 4 (RS-BE の強い安全性). RS-BE Π は以下の (1)’ と定義 2 の (2) を満たすとき，strong $(\leq n, \leq \omega)$-one-time secure であるという: (1)’ 任意の受信者集合 $\mathcal{S}_1, \ldots, \mathcal{S}_k \subset \mathcal{U}$ $(1 \leq k \leq \sum_{j=1}^{n} \binom{n}{j})$，$\left(\bigcup_{i=1}^{k} \mathcal{S}_i\right) \cap W = \emptyset$ かつ $|W| \leq \omega$ となるような任意の結託者集合 $W \subset \mathcal{U}$ に対して，$H(M \mid C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_k}, DK_W) = H(M)$．

実は，このような強い安全性を考えても，定理1と同じタイトな下界を得ることができる．これは補題1が複数種の暗号文について成り立っていることからもわかる．また4節の構成法は上記の安全性をみたし，最適である．

受信者とストレージ管理者の結託に対して安全な RS-BE. 次に，受信者とストレージ管理者の結託に対して安全な RS-BE を考える．直感的に考えて，mk が与えられた暗号文から任意の暗号文に変換できるような鍵の場合，安全性をみたしようがない．そこで，以下では mk の変換ルールとして，Upd に入力される受信者集合 $\mathcal{S}, \mathcal{S}'$ が $\mathcal{S} \supset \mathcal{S}'$ であるときのみ $c_{\mathcal{S}'}$ を出力し，そうでなければ $\perp$ を出力するものとする．

定義 5 (結託耐性をもつ RS-BE). RS-BE Π は以下の条件を満たすとき，collusion-resilient $(\leq n, \leq \omega)$-one-time secure であるという: 任意の受信者集合 $\mathcal{S} \subset \mathcal{U}$，$\mathcal{S} \cap W = \emptyset$ かつ $|W| \leq \omega$ となるような任意の結託者集合 $W \subset \mathcal{U}$ に対して，$H(M \mid C_{\mathcal{S}}, DK_W, MK) = H(M)$.

定義5をみたす構成法として，次が考えられる．

1. $(ek, mk, dk_1, \ldots, dk_n) \leftarrow Setup(1^\lambda, n)$: 有限体 $\mathbb{F}_q$ 上の多項式 $f^{(h)}(x) := \sum_{i=0}^{\omega} a_i x^i$ $(h = 1, \ldots, n)$ を一様ランダムに選び，$g^{(\ell)}(x) := f^{(\ell)}(x) - f^{(\ell-1)}(x)$ $(2 \leq \ell \leq n)$ とする．$ek := f^{(1)}(x)$，$dk_i := (f^{(1)}(i), \ldots, f^{(n)}(i))$ $(1 \leq i \leq n)$，$mk := (g^{(2)}(x), \ldots, g^{(n)}(x))$ として出力する．

2. $c_{\mathcal{S}} \leftarrow Enc(ek, m, \mathcal{S})$: $\mathcal{S} = \{U_{i_1}, \ldots, U_{i_k}\}$ $(1 \leq k \leq n)$ とする．各 U_{i_j} に対して，$c_{i_j}^{(1)} := m + f^{(1)}(i_j)$ を計算し，カウンタとして $t := 1$ とし，$c_{\mathcal{S}} := (t, c_{i_1}^{(t)}, \ldots, c_{i_k}^{(t)})$ を出力する．

3. m or $\perp \leftarrow Dec(dk_i, c_{\mathcal{S}}, \mathcal{S}, U_i)$: もし $U_i \in \mathcal{S}$ ならば，$m = c_i^{(t)} - f^{(t)}(i)$ を計算，出力する．そうでなければ $\perp$ を出力する．

4. $c_{\mathcal{S}'}$ or $\perp \leftarrow Upd(mk, c_{\mathcal{S}}, \mathcal{S}, \mathcal{S}')$: $\mathcal{S}' = \{U_{i_1}, \ldots, U_{i_k}\}$ とする．$\mathcal{S}' \subset \mathcal{S}$ でなければ $\perp$ を出力する．そうでなければ，各 $U_i \in \mathcal{S}' \subset \mathcal{S}$ に対して，$c_i^{(t+1)} := c_i^{(t)} + g^{(t+1)}(i)$ を計算する．最終的に，$t := t + 1$ とし，$c_{\mathcal{S}'} := (t, c_{i_1}^{(t)}, \ldots, c_{i_k}^{(t)})$ を出力する．

構成法の安全性に関して，以下の定理を示すことができる．紙面の都合上，証明は省略する．

定理 3. 上記の RS-BE Π の構成法は collusion-resilient $(\leq n, \leq \omega)$-one-time secure である．

また，定義5のもとで，暗号化鍵と復号鍵に関しては定理1と同じタイトな下界（すなわち定理1の (i)，(ii)）が成り立つ．メンテナンス鍵のタイトな下界に関しては，完全版で示す．

参考文献

[1] S. Berkovits. How to broadcast a secret. In *EUROCRYPT '91*, volume 547, pages 535–541. Springer, 1991.

[2] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In *EUROCRYPT'98*, volume 1403, pages 127–144. Springer, 1998.

[3] C. Blundo and A. Cresti. Space requirements for broadcast encryption. In *EUROCRYPT'94*, volume 950, pages 287–298. Springer, 1995.

[4] C. Blundo, L. Mattos, and D. Stinson. Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. In *CRYPTO '96*, volume 1109, pages 387–400. Springer, 1996.

[5] C.-K. Chu, J. Weng, S. Chow, J. Zhou, and R. Deng. Conditional proxy broadcast re-encryption. In *Information Security and Privacy*, volume 5594, pages 327–342. Springer, 2009.

[6] A. Fiat and M. Naor. Broadcast encryption. In *CRYPTO' 93*, volume 773, pages 480–491. Springer, 1994.

[7] K. Kurosawa, T. Yoshida, Y. Desmedt, and M. Burmester. Some bounds and a construction for secure broadcast encryption. In *ASIACRYPT'98*, volume 1514, pages 420–433. Springer, 1998.

[8] A. Sahai, H. Seyalioglu, and B. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In *CRYPTO 2012*, volume 7417, pages 199–217. Springer, 2012.