暗号文長と秘密鍵長間のトレードオフをもつ情報理論的に安全な放送型暗号の構成法

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
‡ 横浜国立大学 先端科学高等研究院
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 情報理論的に安全な放送型暗号（Broadcast Encryption Scheme: BES）のモデルは 2 つのタイプに大別でき，その両方において暗号文長と秘密鍵長の間にはトレードオフが存在することがわかっているが，一方のタイプの BES の構成法は限られた暗号文長の場合におけるものしかなく，具体的にどういったトレードオフが存在するのかは知られていない．本稿ではこれらの構成法を拡張し，より一般的な暗号文長の場合における BES を Key Predistribution System（KPS）を用いて一般的に構成する．しかし，構成の際に様々な KPS の組み合わせが適用可能なため，どのような組み合わせを選べば構成した BES の鍵長を最小化できるかも明らかにする．本成果により一般的な暗号文長における BES の鍵長の上界も示されたといえる．

Unconditionally Secure Broadcast Encryption Schemes with Trade-offs between Communication and Storage

Yohei Watanabe†　　Junji Shikata†‡

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

Abstract The fact there is a trade-off between the secret-key size and the ciphertext size in unconditionally secure broadcast encryption schemes (BESs) is well known. However, there is no concrete analysis of such a trade-off in a certain type of BESs. In this paper, we first show an efficient construction of such a BES with more general ciphertext sizes from key predistribution systems (KPSs). However, there are many possible combinations of the KPSs to realize the BES in our construction methodology, and therefore, we show that which combination is the best one in the sense that secret-key size can be minimized.

1　はじめに

放送型暗号（Broadcast Encryption Scheme: BES）は，暗号化の際にユーザ全体の中の誰に復号を許すのか自由に指定可能な暗号化方式であり（復号が許可されたユーザの集合 $\mathcal{S}$ を “受信者集合” と呼ぶ），Berkovitz によってその概念が提案された [1]．Fiat と Naor によって定式

化がなされて以降 [9]，計算量的安全性の枠組み [14, 8, 6, 10]，情報理論的安全性の枠組み [3, 4, 11, 12, 7, 15] 双方において，BES に関する様々な研究がなされてきており，実際に著作権保護等に利用されている重要な暗号技術のひとつである．本稿では情報理論的に安全な BES を扱い，単に “BES” と呼ぶ．

大きく分けて，BES のモデルは 2 つのタイプに分けられる．ひとつは $(t, \leq \omega)$-one-time secure BES と呼ばれ，送信者は暗号化の際に受信者集合 $\mathcal{S}$ の要素数がちょうど t であるように（すなわち常に $|\mathcal{S}| = t$）指定する BES である [3, 4, 11, 12, 15]．もうひとつは $(\leq n, \leq \omega)$-one-time secure BES と呼ばれ，送信者は**任意の**受信者集合 $\mathcal{S}$ を指定可能な BES である [9, 3]．Blundo と Cresti は *Key Predistribution System* (KPS) [13, 2] の文脈から両者の鍵長の下界を導出し，後者の方が前者に比べてより柔軟な復号権限の制御が行える一方で，後者の方が大幅に鍵長が長くなることを示した [3]．KPS の文脈から鍵長の下界を導出したということはすなわち，あくまで暗号文長が平文長と等しい場合における BES の鍵長の下界を導出したということである．

Blundo らは $(t, \leq \omega)$-one-time secure BES において，秘密鍵長と暗号文長にトレードオフがあることを示し，また任意の暗号文長における鍵長の下界を導出した [4]．後に，Padró ら [15] によってトレードオフに関する研究は進展したものの，[4] で導出された下界がタイトなものかどうかは知られていない．$(\leq n, \leq \omega)$-one-time secure BES に関しても同様のトレードオフは存在するのは間違いないが，これまでに解析は行われてきておらず，任意の暗号文長における秘密鍵長の下界も未だに導出されていない．

本稿の貢献: 上で述べた通り，$(\leq n, \leq \omega)$-one-time secure BES は $(t, \leq \omega)$-one-time secure BES に比べ，より柔軟な復号権限の制御が可能である．しかしながら，これまでに 2 つの構成法しか知られていない．ひとつは Fiat と Naor によって提案された，暗号文長と平文長が常に等しいような構成法 [9] であり，もうひとつは暗号文長が平文の高々 n 倍となるような，one-time pad を用いた自明な構成法である．本稿では，これらの構成法を拡張し，KPS を用いて，より一般的な暗号文長における $(\leq n, \leq \omega)$-one-time secure BES の一般的構成法を提案する．具体的には，暗号文長が平文長の高々 δ 倍である時に，$(\leq n, \leq \omega)$-one-time secure BES を δ 個の KPS から一般的に構成する手法を示す．構成のアイディア自体はシンプルであるものの，n，ω，δ を固定したときに，考えられる KPS の組み合わせは複数存在する構成手法となっている．従って，構成法を提案すると共に，どういった KPS の組み合わせを選べば，構成した BES の鍵長を最小化することができるかを明らかにする．これにより，通信路容量等に応じて δ を選択し，BES を構成することで，必要な秘密鍵長を抑えることができ，比較的実用的な鍵長を有する情報理論的に安全な BES を実現できた．例えば $n = 100$，$\omega = 5$ の時は，今までは $\delta = 1$ または $\delta = 100$ の場合の構成法しか存在せず，前者の各受信者の復号鍵長は平文長の 75,449,320 倍と膨大になり，後者では平文長と等しい復号鍵長を実現できるものの，暗号文長が平文長の 100 倍と極端であった．すなわち，通信路がその暗号文長を許容できない場合，前者を使うしか選択肢がなかった．それに対し，本構成法を用い，かつ最適な KPS の組み合わせを選べば，たとえば $\delta = 10$ を選ぶことによって，復号鍵長は平文長の 382 倍かつ暗号文長は平文長の 10 倍でよく，柔軟なパラメータ設定が可能である．

上記の通り，任意の暗号文長における $(\leq n, \leq \omega)$-one-time secure BES の鍵長のタイトな下界[1]の導出は大きな課題となっている．本研究は，既存構成法を拡張することにより任意の暗号文長における $(\leq n, \leq \omega)$-one-time secure BES の鍵長の上界を示したともいえ，その課題解決の一歩として捉えられる．

2 準備

本節では準備として，BES と KPS それぞれについて記述する．以下，ユーザの集合を $\mathcal{U} :=$

[1] 一般にタイトな下界を示すためには，上界と下界の両方の等号を満たすような BES の存在を示す必要がある．

$\{U_1, U_2, \ldots, U_n\}$ とする．また，任意の $n \in \mathbb{N}$ に対して，$[n] := \{1, 2, \ldots, n\}$ という記法を用いる．

2.1 One-time Secure Broadcast Encryption Scheme

第 1 節で述べたように，本稿ではユーザ集合の**任意の**部分集合を受信者集合として指定可能な BES を扱う．BES は以下のように定義される．$\mathcal{M}$ を平文集合とする．任意の部分集合 $\mathcal{J} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$ に対し，$\mathcal{C}_\mathcal{J}$ を受信者集合 $\mathcal{J}$ の暗号文集合とし，暗号文全体の集合を $\mathcal{C} := \bigcup_{\mathcal{J} \subset \mathcal{U}} \mathcal{C}_\mathcal{J}$ とする．また，$\mathcal{EK}$ を暗号化鍵の集合，$\mathcal{DK}_i$ をユーザ U_i の復号鍵集合とし，$\mathcal{DK} := \bigcup_{i=1}^{n} \mathcal{DK}_i$ とする．

定義 1 (BES)**.** *BES* Π は以下の 3 つのアルゴリズム *(Setup, Enc, Dec)* と 4 つの集合 $\mathcal{M}$, $\mathcal{C}$, $\mathcal{EK}$, $\mathcal{DK}$ からなる．*Setup* は確率的アルゴリズム，*Enc*，*Dec* は確定的アルゴリズムであり，上記空間は全て有限集合である．

1. $(ek, dk_1, \ldots, dk_n) \leftarrow Setup(n)$*:* 受信者数 n を入力にとり，暗号化鍵 $ek \in \mathcal{EK}$ と n 個の復号鍵 $(dk_1, \ldots, dk_n) \in \prod_{i=1}^{n} \mathcal{DK}_i$ を出力する．
2. $c_\mathcal{S} \leftarrow Enc(ek, m, \mathcal{S})$*:* 暗号化鍵 ek，平文 $m \in \mathcal{M}$，また任意の受信者集合 $\mathcal{S} \subset \mathcal{U}$ を入力にとり，暗号文 $c_\mathcal{S}$ を出力する．
3. m *or* $\perp \leftarrow Dec(dk_i, c_\mathcal{S}, \mathcal{S}, U_i)$*:* U_i の復号鍵 dk_i，暗号文 $c_\mathcal{S}$，またその受信者集合 $\mathcal{S}$，自身の *ID* U_i を入力にとり，復号結果の平文 m を出力，または復号失敗を表す $\perp$ を出力する．

本モデルでは，以下の正しさを要求する: 全ての $n \in \mathbb{N}$，全ての $(ek, dk_1, \ldots, dk_n) \leftarrow Setup(n)$，全ての $m \in \mathcal{M}$，全ての $\mathcal{S} \subset \mathcal{U}$，全ての $U_i \in \mathcal{S}$ に対して，$m \leftarrow Dec(dk_i, Enc(ek, m, \mathcal{S}), \mathcal{S}, U_i)$.

上記の BES は one-time model を考える．すなわち，送信者はただ一度だけ暗号文を生成し，それを放送するものとする．

BES では，高々ω 人の受信者の結託に対する完全秘匿性を考える．任意の $\mathcal{J} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$ に対して，$\mathcal{DK}_\mathcal{J} := \mathcal{DK}_{i_1} \times \cdots \times \mathcal{DK}_{i_j}$ を $\mathcal{J}$ の復号鍵の集合とする．M, $C_\mathcal{S}$, EK, DK_i $(1 \le i \le n)$, $DK_\mathcal{J}$ $(\mathcal{J} \subset \mathcal{U})$ をそれぞれ $\mathcal{M}$, $\mathcal{C}_\mathcal{S}$, $\mathcal{EK}$, $\mathcal{DK}_i$ $(1 \le i \le n)$, $\mathcal{DK}_\mathcal{J}$ $(\mathcal{J} \subset \mathcal{U})$ に値をとる確率変数とする．

定義 2 (BES の安全性)**.** Π を *BES* とする．次の条件を満たすとき，Π は $(\le n, \le \omega)$*-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 $|W| \le \omega$ となるような任意の結託者集合 $W \subset \mathcal{U}$ に対して，$H(M \mid C_\mathcal{S}, DK_W) = H(M)$.

本稿では，その暗号文長が平文の整数倍長であるような $(\le n, \le \omega)$-one-time secure BES を扱う．これまでに研究対象にされた $(\le n, \le \omega)$-one-time secure BES は，暗号文長と平文長が等しい時のものであった．

定義 3. 任意の $(\le n, \le \omega)$*-one-time secure BES* Π において，$\delta := \max_{\mathcal{S} \subset \mathcal{U}} \log |\mathcal{C}_\mathcal{S}| / \log |\mathcal{M}|$ と定義する．このとき，Π は $(\le n, \le \omega; \delta)$*-one-time secure* であるという．

2.2 Key Predistribution System

KPS は以下のように定義される．任意の部分集合 $\mathcal{J} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$ に対し，$\mathcal{K}_\mathcal{J}$ を $\mathcal{J}$ のセッション鍵の集合とし，$\mathcal{K} := \bigcup_{\mathcal{J} \subset \mathcal{U}} \mathcal{K}_\mathcal{J}$ とする．また，ユーザ U_i の秘密鍵集合を $\mathcal{UK}_i$ とし，$\mathcal{UK} := \bigcup_{i=1}^{n} \mathcal{UK}_i$ とする．

定義 4 (KPS)**.** *KPS* Φ は以下の 2 つのアルゴリズム *(Init, Der)* と 2 つの集合 $\mathcal{K}$, $\mathcal{UK}$ からなる．*Init* は確率的アルゴリズム，*Der* は確定的アルゴリズムであり，上記空間は全て有限集合である．

1. $(uk, uk_1, \ldots, uk_n) \leftarrow Init(n)$*:* ユーザ数 n を入力とし，マスター鍵 $uk \in \mathcal{UK}$ と n 個の秘密鍵 $(uk_1, \ldots, uk_n) \in \prod_{i=1}^{n} \mathcal{UK}_i$ を出力する[2].

[2]KPS の既存方式 [2, 13, 5, 11] ではマスター鍵 uk は登場しないが，BES との親和性等を考慮して本稿では uk を明示的に書く．uk は実際に使用するわけではないことに留意する．また，uk は n 個の秘密鍵 $uk_1, \ldots . uk_n$ を導出する確定的アルゴリズムと見ることもできる．

2. $k_{\mathcal{S}} \leftarrow Der(uk_i, \mathcal{S})$: U_i の秘密鍵 uk_i と任意の部分集合 $\mathcal{S} \subset \mathcal{U}$ を入力とし，$\mathcal{S}$ のセッション鍵 $k_{\mathcal{S}} \in \mathcal{K}_{\mathcal{S}}$ を出力する．

本モデルでは，以下の正しさを要求する: 全ての $n \in \mathbb{N}$，全ての $(uk, uk_1, \ldots, uk_n) \leftarrow Init(n)$，また全ての $\mathcal{S} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$ に対して，$Der(uk_{i_1}, \mathcal{S}) = \cdots = Der(uk_{i_j}, \mathcal{S})$.

BES 同様，高々ω 人の結託者に対する完全秘匿性を考える．任意の $\mathcal{J} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$ に対して，$\mathcal{UK}_{\mathcal{J}} := \mathcal{UK}_{i_1} \times \cdots \times \mathcal{UK}_{i_j}$ を $\mathcal{J}$ の秘密鍵の集合とする．$K_{\mathcal{S}}$，UK_i $(1 \le i \le n)$，$UK_{\mathcal{J}}$ $(\mathcal{J} \subset \mathcal{U})$ をそれぞれ $\mathcal{K}_{\mathcal{S}}$，$\mathcal{UK}_i$ $(1 \le i \le n)$，$\mathcal{UK}_{\mathcal{J}}$ $(\mathcal{J} \subset \mathcal{U})$ に値をとる確率変数とする．

定義 5 (KPS の安全性)**.** Φ を *KPS* とする．次の条件を満たすとき，Φ は $(\le n, \le \omega)$-*KPS* であるという*:* 任意の部分集合 $\mathcal{S} \subset \mathcal{U}$ と，$\mathcal{S} \cap W = \emptyset$ かつ $|W| \le \omega$ となるような任意の結託者集合 $W \subset \mathcal{U}$ に対して，$H(K_{\mathcal{S}} \mid UK_W) = H(K_{\mathcal{S}})$.

$(\le n, \le \omega)$-KPS の秘密鍵長の下界は以下のように知られている．以下では，全ての $\mathcal{S}, \mathcal{S}' \subset \mathcal{U}$ に対して $H(K_{\mathcal{S}}) = H(K_{\mathcal{S}'})$ とし，簡単に $H(K)$ と書く．

命題 1 ([3, 11])**.** Φ を $(\le n, \le \omega)$-*KPS* とする．このとき，任意の $i \in \{1, \ldots, n\}$ に対して，$H(UK_i) \ge \sum_{j=0}^{\omega} \binom{n}{j} H(K)$ が成り立つ．

上記下界の等号を満たす（すなわち最適な）$(\le n, \le \omega)$-KPS の構成法は Fiat と Naor によって提案されているが [9]，紙面の都合上省略する．得られる鍵長はそれぞれ，復号鍵長は $\log |\mathcal{UK}_i| = \sum_{j=0}^{\omega} \binom{n-1}{j} \log |\mathcal{K}|$ であり，マスター鍵長は $\log |\mathcal{UK}| = \sum_{j=0}^{\omega} \binom{n}{j} \log |\mathcal{K}|$ となる．

3 $(\le n, \le \omega; \delta)$-one-time Secure BES の一般的構成法

これまで，$(\le n, \le \omega; \delta)$-one-time Secure BES の構成法は $\delta = 1$ または $\delta = n$ の時のものしか知られていない．前者は $(\le n, \le \omega)$-KPS と one-time pad で構成することができ，後者は n 個の $(\le 1, \le 0)$-KPS から（すなわち n 個の one-time pad から）自明に構成可能である．本節では，これら 2 つの構成法の純粋な拡張として，任意の $\delta \in [n]$ に対する $(\le n, \le \omega; \delta)$-one-time secure BES を δ 個の KPS から一般的に構成する手法を提案する．その際，$(\le n, \le \omega; \delta)$-one-time secure BES を実現可能な KPS の組み合わせは数多く存在するため，秘密鍵長が最も小さくなるような KPS の組み合わせの条件を明らかにする．

3.1 KPS を用いたシンプルな構成法

本構成法は非常にシンプルなアイディアに基づいている．まず，ユーザ集合 $\mathcal{U}$ を δ 個の互いに素な部分集合 $\mathcal{U}_1, \ldots, \mathcal{U}_\delta$ に分割する．次に各部分集合 $\mathcal{U}_i$ に $(\le |\mathcal{U}_i|, \le \omega_i)$-KPS を割り当てる．ここで $\omega_i := \min\{\omega, |\mathcal{U}_i| - 1\}$ であり，これは $\omega \ge |\mathcal{U}_i|$ となるような $(\le |\mathcal{U}_i|, \le \omega)$-KPS は考えても意味がないためである．任意の受信者集合 $\mathcal{S}$ に対して，$\mathcal{S}_i := \mathcal{U}_i \cap \mathcal{S}$ とする．その時，セッション鍵 $k_{\mathcal{S}_i}$ は $(\le |\mathcal{U}_i|, \le \omega_i)$-KPS により生成され，暗号文は $c_{\mathcal{S}} := (m \oplus k_{\mathcal{S}_1}, \ldots, m \oplus k_{\mathcal{S}_\delta})$ となる．しかしながら，合計が n となるような δ 個の自然数の組み合わせ（各 $\mathcal{U}_i$ の要素数の組み合わせ）は複数存在し，それを表すために，任意の自然数 $n \in \mathbb{N}$ と任意の $\delta \in [n]$ に対して，次の集合を定義する:

$$\mathcal{L}(n, \delta) := \left\{ (\ell_1, \ldots, \ell_\delta) \in \mathbb{N}^\delta \;\middle|\; \begin{array}{l} (\ell_1 \ge \cdots \ge \ell_\delta) \\ \wedge \sum_{i=1}^{\delta} \ell_i = n \end{array} \right\}.$$

$\mathcal{L}(n, \delta)$ は，合計が n となるような δ 個の自然数の組み合わせ全ての集合であり，しばしば $\boldsymbol{L} := (\ell_1, \ell_2, \ldots, \ell_\delta) \in \mathcal{L}(n, \delta)$ と書く．従って，ある n，ω，δ に対して，最も秘密鍵長が小さくなるような $\boldsymbol{L}$ を選ばなければならない．そのような最適な $\boldsymbol{L}$ が満たすべき条件に関しては，次節で明らかにする．

δ 個の KPS $\Phi_i = \{Init_i, Der_i\}$ $(1 \le i \le \delta)$ による BES $\Pi = \{Setup, Enc, Dec\}$ の構成法は以下の通りである．

– $(ek, dk_1, \ldots, dk_n) \leftarrow Setup(n)$: $\boldsymbol{L} \in \mathcal{L}(n, \delta)$ を選ぶ．一般性を失わずに，$\mathcal{U}_i := \{U_{\sum_{j=1}^{i-1}\ell_j+1}, \ldots, U_{\sum_{j=1}^{i}\ell_j}\}$ とする[3]．$Init_i(\ell_i, \omega_i) \rightarrow (uk^{(i)}, uk_{\sum_{j=1}^{i-1}\ell_j+1}, \ldots, uk_{\sum_{j=1}^{i}\ell_j})$ $(1 \le i \le \delta)$ を実行し，$ek := (uk^{(1)}, \ldots, uk^{(n)})$ と $dk_i := uk_i$ を出力する．

– $c_{\mathcal{S}} \leftarrow Enc(ek, m, \mathcal{S})$: $\mathcal{S} \subset \mathcal{U}$ を選び，$\mathcal{S}_i := \mathcal{S} \cap \mathcal{U}_i$ $(1 \le i \le \delta)$ とする．もし $\mathcal{S}_i \neq \emptyset$ ならば，ある $U_j \in \mathcal{S}_i$ に対して，$Der_i(uk_j, \mathcal{S}_i) \rightarrow k_{\mathcal{S}_i}$ $(1 \le i \le \delta)$ を実行する．任意の uk_j は $uk^{(i)}$ から導出できることに留意する．$c_{\mathcal{S}} := (m \oplus k_{\mathcal{S}_i})_{\mathcal{S}_i \neq \emptyset}$ を出力する．

– m or $\perp \leftarrow Dec(dk_i, c_{\mathcal{S}}, \mathcal{S}, U_i)$: $c_{\mathcal{S}}$ を $(c_{\mathcal{S}_1}, \ldots, c_{\mathcal{S}_k})$ とし，$U_i \in \mathcal{U}_j$ とする．もし $U_i \in \mathcal{S}_j$ ならば，$k_{\mathcal{S}_j} \leftarrow Der(uk_i, \mathcal{S}_j)$ を計算し，$m = c_{\mathcal{S}_j} \oplus k_{\mathcal{S}_j}$ を得る．

以下の定理を得る．紙面の都合上証明は割愛するが，証明はそれほど難しくはない．

定理 1. *$(\le \ell_i, \le \omega_i)$-one-time secure KPS Φ_i $(1 \le i \le \delta)$ より構成した Π の上記構成法は $(\le n, \le \omega; \delta)$-one-time secure である．*

3.2 鍵長を最小化する最適なパラメータの導出

鍵長に関して最も効率的な方式を得るためには，どのように $(\le \ell_i, \le \omega)$-KPS を組み合わせるかを慎重に行う必要がある．そこで，どういった $\boldsymbol{L} \in \mathcal{L}(n, \delta)$ を適用すれば秘密鍵長を最小化できるかを以下に示す．

定理 2. *各 $(\le \ell_i, \le \omega_i)$-KPS Φ_i $(1 \le i \le \delta)$ に最適な構成法 [9] を適用した時，構成した $(\le n, \le \omega; \delta)$-one-time secure BES Π の秘密鍵長は以下のようになる．*

(i) $$\log|\mathcal{EK}| = \sum_{i=1}^{\delta}\sum_{j=0}^{\omega_i}\binom{\ell_i}{j}\log|\mathcal{K}|,$$

(ii) $$\sum_{i=1}^{n}\log|\mathcal{DK}_i| = \sum_{i=1}^{\delta}\left(\ell_i\sum_{j=0}^{\omega_i}\binom{\ell_i-1}{j}\right)\log|\mathcal{K}|.$$

更に，以下の条件を満たす $\boldsymbol{L} \in \mathcal{L}(n, \delta)$ によって，暗号化鍵長は最小化される：

$$\begin{cases} {}^{\forall}\boldsymbol{L} & \text{if } \omega = 0, \\ \boldsymbol{L} = (n-(\delta-1), 1, \ldots, 1) & \text{if } \omega = 1, \\ \ell_1 - \ell_\delta = 0 & \text{if } \omega \ge 2 \\ & \quad \wedge n/\delta \in \mathbb{N}, \\ \ell_1 - \ell_\delta = 1 & \text{otherwise.} \end{cases}$$

一方，以下の条件を満たす $\boldsymbol{L} \in \mathcal{L}(n, \delta)$ によって，復号鍵長は最小化される：

$$\begin{cases} {}^{\forall}\boldsymbol{L} & \text{if } \omega = 0, \\ \ell_1 - \ell_\delta = 0 & \text{if } \omega \ge 1 \wedge n/\delta \in \mathbb{N}, \\ \ell_1 - \ell_\delta = 1 & \text{otherwise.} \end{cases}$$

証明．任意の $\boldsymbol{L} \in \mathcal{L}(n, \delta)$ に対して，$F(\boldsymbol{L}, \omega) := \sum_{i=1}^{\delta}\sum_{j=0}^{\omega_i}\binom{\ell_i}{j}$，$G(\boldsymbol{L}, \omega) := \sum_{i=1}^{\delta}\left(\ell_i\sum_{j=0}^{\omega_i}\binom{\ell_i-1}{j}\right)$ とする．$\omega = 0$ のとき，任意の $\boldsymbol{L}$ に対して，明らかに $F(\boldsymbol{L}, 0) = \delta$，また $G(\boldsymbol{L}, 0) = n$ である．

最初に $\omega > 0$ の場合の $F(\boldsymbol{L}, \omega)$ を最小化する条件を導出していく．そのために，以下の補題を示す．紙面の都合上，本証明中に登場する補題の証明は割愛する．詳細な証明は完全版で記述する．

補題 1. 任意の $a, j \in \mathbb{N}$ と任意の $r \in \{0, 1, \ldots, a\}$ に対して，$b_1 \ge \cdots \ge b_j \ge -(a-r)$ かつ $\sum_{i=1}^{j} b_i = 0$ となるような任意の $b_i \in \mathbb{Z}$ $(1 \le i \le j)$ を選ぶ．この時，以下が成り立つ．

$$j\binom{a}{r} \le \binom{a+b_1}{r} + \cdots + \binom{a+b_j}{r}.$$

$r = 0$ または $r = 1$ の時かつその時に限り等号が成り立つ．

これはすなわち，和が等しい j 個の自然数の組み合わせの中で，最も “平らな” 組み合わせが，その j 個の自然数それぞれから r 個を取り出す組み合わせの総和が少なくなるということである．また，以下の系を得る．

[3] 例えば，$n = 9$，$\delta = 3$，$\ell_i = 3$ $(i = 1, 2, 3)$ の場合は，$\mathcal{U}_1 := \{U_1, U_2, U_3\}$，$\mathcal{U}_2 := \{U_4, U_5, U_6\}$，$\mathcal{U}_3 := \{U_7, U_8, U_9\}$ とするということである．

系 1. 任意の $a, j \in \mathbb{N}$ に対して，$b_1 \geq \cdots \geq b_k > -(a-1) \geq b_{k+1} \geq \cdots \geq b_j$ かつ $\sum_{i=1}^{j} b_i = 0$ となるような任意の $b_i \in \mathbb{Z}$ を選ぶ．この時，以下が成り立つ．

$$j\binom{a}{1} > \binom{a+b_1}{1} + \cdots + \binom{a+b_k}{1}.$$

従って，明らかに $k=1$ の時に値は最小化される．すなわち，

$$j\binom{a}{1} > \binom{a+b_1}{1} = \binom{ja-(j-1)}{1}.$$

この系は，$r=1$ の時（すなわち補題 1 において等号が成り立つとき），右辺からいくつか項を削除した時，明らかに左辺が大きくなるということを示している．

ここで，系 1 を用いて $F(\boldsymbol{L}, \omega=1)$ を最小化する条件を示す．$\omega=1$ の時，以下のように書ける．

$$F(\boldsymbol{L},1) = \sum_{i=1}^{k}\binom{\ell_i}{1} + \sum_{i=0}^{\delta}\binom{\ell_i}{0} = \sum_{i=1}^{k}\binom{\ell_i}{1} + \delta.$$

ここで，$\ell_1 \geq \cdots \geq \ell_k > 1 = \ell_{k+1} = \cdots = \ell_\delta$ である．従って，$F(\boldsymbol{L},1)$ は $\boldsymbol{L} = (n-(\delta-1), 1, \ldots, 1)$ の時最小化される．

次に，以下の補題を示す．この補題は，$r \geq 2$ の場合は系 1 と逆の結果となることを示している．

補題 2. 任意の $a, j \in \mathbb{N}$ と任意の $r \in \{2, \ldots, a\}$ に対して，$b_1 \geq \cdots \geq b_k \geq -(a-r) > b_{k+1} \geq \cdots \geq b_j$ かつ $\sum_{i=1}^{j} b_i = 0$ となるような任意の $b_i \in \mathbb{Z}$ を選ぶ．この時，以下が成り立つ．

$$j\binom{a}{r} < \binom{a+b_1}{r} + \cdots + \binom{a+b_k}{r}.$$

更に，以下が成り立つ．

$$\binom{a+b_1}{r} + \cdots + \binom{a+b_k}{r} - j\binom{a}{r} > \sum_{m=1}^{\lambda}\binom{a+\alpha_m}{r-1}.$$

ここで，$\lambda := \sum_{i=1}^{k} b_i - (j-k)(a-r)$ であり，$\alpha_m \in \mathbb{N}$ $(1 \leq m \leq \lambda)$ は，$1 \leq \alpha_m \leq b_1$ となるような自然数である．

補題 1，2 を用いて，$\omega \geq 2$ かつ $n/\delta \in \mathbb{N}$ の場合に $F(\boldsymbol{L}, \omega)$ を最小化する条件を示す．ここで，$a := \lfloor n/\delta \rfloor$，$\delta_1 := n \bmod \delta$，$\delta_2 := \delta - \delta_1$ とする．$\omega \geq 2$ かつ $n/\delta \in \mathbb{N}$ の場合は，$\delta_1 = 0$，$\delta_2 = \delta$ となる．この時，$\widehat{\boldsymbol{L}} = (a, \ldots, a)$ に対して，$F(\widehat{\boldsymbol{L}}, \omega)$ を次のように表すことができる:

$$F(\widehat{\boldsymbol{L}}, \omega) = \delta\binom{a}{\hat{\omega}} + \delta\binom{a}{\hat{\omega}-1} + \cdots + \delta\binom{a}{1} + \delta\binom{a}{0}.$$

ここで，$\hat{\omega} := \min\{\omega, a-1\}$ である．

同様に，任意の $\widetilde{\boldsymbol{L}} \in \mathcal{L}(n,\delta) \setminus \{\widehat{\boldsymbol{L}}\}$ に対して，$F(\widetilde{\boldsymbol{L}}, \omega)$ を次のように表すことができる:

$$F(\widetilde{\boldsymbol{L}}, \omega) = \sum_{i=1}^{k_1}\binom{\ell_i}{\tilde{\omega}} + \sum_{i=1}^{k_2}\binom{\ell_i}{\tilde{\omega}-1} + \cdots + \sum_{i=1}^{\delta}\binom{\ell_i}{0}.$$

ここで，$\tilde{\omega} := \min\{\omega, \ell_1 - 1\}$ であり，また $\ell_i > \tilde{\omega} - (m-1) \geq \ell_{i+1}$ としたときに $k_m := i$ $(1 \leq m \leq \tilde{\omega})$ である．すなわち $k_1 \leq \cdots \leq k_{\tilde{\omega}}$ である．

ここで，次の 2 つのケースを考える: (i) $\hat{\omega} = \tilde{\omega}$; (ii) $\hat{\omega} < \tilde{\omega}$. $\ell_1 > a$ であるから，$\hat{\omega} > \tilde{\omega}$ という状況は起こらない．

まず，(i) の場合について示す．

$$\begin{aligned}
&F(\widetilde{\boldsymbol{L}}, \omega) - F(\widehat{\boldsymbol{L}}, \omega) \\
&= \left(\sum_{i=1}^{k_1}\binom{\ell_i}{\hat{\omega}} - \delta\binom{a}{\hat{\omega}}\right) + \cdots + \left(\sum_{i=1}^{k_{\hat{\omega}-1}}\binom{\ell_i}{2} - \delta\binom{a}{2}\right) + \left(\sum_{i=1}^{k_{\hat{\omega}}}\binom{\ell_i}{1} - \delta\binom{a}{1}\right) \\
&= \left(\sum_{i=1}^{k_1}\binom{\ell_i}{\hat{\omega}} - \delta\binom{a}{\hat{\omega}}\right) + \cdots + \left(\sum_{i=1}^{k_{\hat{\omega}-1}}\binom{\ell_i}{2} - \delta\binom{a}{2}\right) + \left(\sum_{i=1}^{k_{\hat{\omega}}}\binom{\ell_i}{1} - \sum_{i=1}^{\delta}\binom{\ell_i}{1}\right) \qquad (1) \\
&> \sum_{m=1}^{\lambda_1}\binom{a+\alpha_m^{(1)}}{\hat{\omega}-1} + \cdots + \sum_{m=1}^{\lambda_{\hat{\omega}-1}}\binom{a+\alpha_m^{(\hat{\omega}-1)}}{1} + \left(\sum_{i=1}^{k_{\hat{\omega}}}\binom{\ell_i}{1} - \sum_{i=1}^{\delta}\binom{\ell_i}{1}\right) \qquad (2)
\end{aligned}$$

$> 0.$ (3)

ここで，$\lambda_i := \sum_{j=1}^{k_i} \ell_j - (\delta - k_i)(a - (\hat{\omega} - i))$，$\alpha_m^{(k)} \in \mathbb{N}$ $(1 \le k \le \hat{\omega} - 1)$ は，$1 \le \alpha_m^{(k)} \le \ell_1 - a$ となるような自然数である．また，(1) は補題 1 から従い，(2) は補題 2 から従い，(3) は以下から従う: $a := \lfloor n/\delta \rfloor$ とする．この時，便宜的に，任意の $\boldsymbol{L}' \in \mathcal{L}(n, \delta)$，$\boldsymbol{L} := (a, \dots, a)$ に対し，$f(\boldsymbol{L}', \boldsymbol{L}, \omega) := \sum_{i=1}^{\hat{\omega}-1} \sum_{m=1}^{\lambda_i} \binom{a + \alpha_m^{(i)}}{\hat{\omega} - i}$，また $g(\boldsymbol{L}', \boldsymbol{L}, \omega) := \left(\sum_{i=1}^{k_{\hat{\omega}}} \binom{\ell_i}{1} - \sum_{i=1}^{\delta} \binom{\ell_i}{1} \right)$ とすると，$F(\boldsymbol{L}', \omega) - F(\boldsymbol{L}, \omega) > f(\boldsymbol{L}', \boldsymbol{L}, \omega) + g(\boldsymbol{L}', \boldsymbol{L}, \omega)$ と表すことができる．次に，次の条件を満たす任意の $\boldsymbol{L}'', \boldsymbol{L}' \in \mathcal{L}(n, \delta)$ を選ぶ: 任意の κ $(1 \le \kappa < \delta)$ と $\boldsymbol{L} := (a, \dots, a)$ に対して，$g(\boldsymbol{L}'', \boldsymbol{L}, \omega) := \left(\sum_{i=1}^{k''_{\hat{\omega}}} \binom{\ell_i}{1} - \sum_{i=1}^{\delta} \binom{\ell_i}{1} \right) = 0$ (すなわち $k''_{\hat{\omega}} = \delta$)，また $g(\boldsymbol{L}', \boldsymbol{L}, \omega) := \left(\sum_{i=1}^{k'_{\hat{\omega}}} \binom{\ell_i}{1} - \sum_{i=1}^{\delta} \binom{\ell_i}{1} \right) = -\kappa$ (すなわち $k'_{\hat{\omega}} = \delta - \kappa$)．$\omega \ge 2$ であるから，$g(\boldsymbol{L}', \boldsymbol{L}, \omega) - g(\boldsymbol{L}'', \boldsymbol{L}, \omega) = -\kappa$ である一方で，明らかに $f(\boldsymbol{L}', \boldsymbol{L}, \omega) - f(\boldsymbol{L}'', \boldsymbol{L}, \omega) \ge \kappa$ を満たす．

(ii) の場合について示す．

$$
\begin{aligned}
&F(\widetilde{\boldsymbol{L}}, \omega) - F(\widehat{\boldsymbol{L}}, \omega) \\
&= \sum_{i=1}^{k_1} \binom{\ell_i}{\tilde{\omega}} + \cdots + \left(\sum_{i=1}^{k_{\omega-1}} \binom{\ell_i}{\hat{\omega}} - \delta \binom{a}{\hat{\omega}} \right) + \cdots \\
&\quad + \left(\sum_{i=1}^{k_{\omega-1}} \binom{\ell_i}{2} - \delta \binom{a}{2} \right) + \left(\sum_{i=1}^{k_\omega} \binom{\ell_i}{1} - \delta \binom{a}{1} \right).
\end{aligned}
$$

従って，(i) の場合と同様に $F(\widetilde{\boldsymbol{L}}, \omega) - F(\widehat{\boldsymbol{L}}, \omega) > 0$ を示すことが可能である．以上より，もし $\omega \ge 2 \wedge n/\delta \in \mathbb{N}$ ならば，$F(\boldsymbol{L}, \omega)$ の最小値は $\ell_1 - \ell_\delta = 0$ を満たす $\boldsymbol{L}$ によって与えられる．

同様に，$\omega \ge 2 \wedge n/\delta \notin \mathbb{N}$ の場合も証明することができ，その時，$F(\boldsymbol{L}, \omega)$ の最小値は $\ell_1 - \ell_\delta = 1$ を満たす $\boldsymbol{L}$ によって与えられる．これは，どんな $a := \lfloor n/\delta \rfloor$，$\delta_1 := n \bmod \delta$，$\delta_2 := \delta - \delta_1$ に対しても，$n = \delta a + \delta_1 = \delta_1(a+1) + \delta_2 a$ と表すことができることによる．

$G(\boldsymbol{L}, \omega)$ においても，以下の補題を用いて，$F(\boldsymbol{L}, \omega)$ の場合と同様の方法で証明可能である．

補題 3. 任意の $a, j \in \mathbb{N}$ と任意の $r \in [a]$ に対して，$b_1 \ge \cdots \ge b_k \ge -(a-r) > b_{k+1} \ge \cdots \ge b_j$ かつ $\sum_{i=1}^{j} b_i = 0$ となるような任意の $b_i \in \mathbb{Z}$ を選ぶ．この時，以下が成り立つ．

$$
\begin{aligned}
&aj\binom{a-1}{r} < \\
&(a+b_1)\binom{a+b_1-1}{r} + \cdots + (a+b_k)\binom{a+b_k-1}{r}.
\end{aligned}
$$

補題 2 が $r \ge 2$ の場合に成り立つのに対し，上記の補題は $r = 1$ の時も成り立つことに留意する．従って，もし $\omega \ge 1 \wedge n/\delta \in \mathbb{N}$ ならば，$G(\boldsymbol{L}, \omega)$ の最小値は $\ell_1 - \ell_\delta = 0$ の時に与えられ，同様にもし $\omega \ge 1 \wedge n/\delta \notin \mathbb{N}$ ならば，$G(\boldsymbol{L}, \omega)$ の最小値は $\ell_1 - \ell_\delta = 0$ の時に与えられる． □

従って，定理 2 より，最適なパラメータを本構成法に適用した場合の鍵長は以下のようになる．

系 2. Π を本構成法で得られた $(\le n, \le \omega; \delta)$-*one-time secure BES* とする．$a := \lfloor n/\delta \rfloor$, $\delta_1 := n \bmod \delta$，$\delta_2 := \delta - \delta_1$ とする．この時，δ_1 個の $(\le a+1, \le \omega_1)$-*KPS* Φ_i $(1 \le i \le \delta_1)$ と δ_2 個の $(\le a, \le \omega_2)$-*KPS* Φ_i $(\delta_1 + 1 \le i \le \delta)$ を用いて Π を構成すると，秘密鍵長（特に復号鍵長）を最小化することができる．ここで，$\omega_1 := \min\{a, \omega\}$，$\omega_2 := \min\{a-1, \omega\}$ である．具体的には，秘密鍵長は以下のようになる*:*

(i) $\log |\mathcal{EK}| =$
$$
\left(\delta_1 \sum_{j=0}^{\omega_1} \binom{a+1}{j} + \delta_2 \sum_{j=0}^{\omega_2} \binom{a}{j} \right) \log |\mathcal{K}|,
$$

(ii) $\sum_{i=1}^{n} \log |\mathcal{DK}_i| =$
$$
\left(\delta_1 (a+1) \sum_{j=0}^{\omega_1} \binom{a}{j} + \delta_2 a \sum_{j=0}^{\omega_2} \binom{a-1}{j} \right) \log |\mathcal{K}|.
$$

結果として，上記の結果は，任意の $\delta \in [n]$ に対する $(\le n, \le \omega; \delta)$-one-time secure BES に必要な秘密鍵長の非自明な上界を初めて与えたこととなる．

注意 1. 定理 *2* からわかるように，どんな n，ω，δ に対しても，暗号化鍵長と復号鍵長両方を最小化できるわけではない．具体的には，系 *2* で得られた暗号化鍵長は $\omega = 1$ の場合には最小にならない．しかし，そのオーバーヘッドは実際少なく，また従来 *BES* の文脈では暗号化鍵長より復号鍵長の方が重要視されてきたため，系 *2* では，復号鍵長は常に最小であり，暗号化鍵長はできるだけ小さくなるパラメータを選んでいる．実際，多くの既存研究 *[3, 4, 11, 12, 15]* では，復号鍵の下界についてしか扱っていない．

注意 2. 上記の最適なパラメータを適用した $(\leq n, \leq \omega; \delta)$-*one-time secure BES* は，既存の 2 つの構成法（*3* 節冒頭参照）を含んでいる．具体的には，$\delta = 1$ の時には *Fiat* と *Naor* の提案した *BES[9]* の構成法と等しくなり，$\delta = n$ の時には n 個の *one-time pad* から構成した自明な構成法と等しくなる．すなわち，本構成法は既存構成法の純粋な拡張であるということができる．

謝辞． 本研究は，JSPS 科研費 15H02710 の助成，及び文部科学省国立大学改革強化推進事業の支援によるものです．第一著者は，JSPS 科研費 25·3998 の助成を受けています．また本研究の初期段階において有益なコメントを頂きました，山田翔太氏，花岡悟一郎氏に深く感謝いたします．

参考文献

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

[2] R. Blom. An optimal class of symmetric key generation systems. In *EUROCRYPT'84*, volume 209 of *LNCS*, pages 335–338. Springer, 1985.

[3] C. Blundo and A. Cresti. Space requirements for broadcast encryption. In *EUROCRYPT'94*, volume 950 of *LNCS*, 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 of *LNCS*, pages 387–400. Springer, 1996.

[5] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In *CRYPTO' 92*, volume 740 of *LNCS*, pages 471–486. Springer, 1993.

[6] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *CRYPTO 2005*, volume 3621 of *LNCS*, pages 258–275. Springer, 2005.

[7] H. Chen, S. Ling, C. Padró, H. Wang, and C. Xing. Key predistribution schemes and one-time broadcast encryption schemes from algebraic geometry codes. In *Cryptography and Coding*, volume 5921 of *LNCS*, pages 263–277. Springer, 2009.

[8] Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In *Digital Rights Management*, volume 2696 of *LNCS*, pages 61–80. Springer, 2003.

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

[10] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 171–188. Springer, 2009.

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

[12] M. Luby and J. Staddon. Combinatorial bounds for broadcast encryption. In *EUROCRYPT'98*, volume 1403 of *LNCS*, pages 512–526. Springer, 1998.

[13] T. Matsumoto and H. Imai. On the key predistribution system: A practical solution to the key distribution problem. In *CRYPTO '87*, volume 293 of *LNCS*, pages 185–193. Springer, 1988.

[14] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In *CRYPTO 2001*, volume 2139 of *LNCS*, pages 41–62. Springer, 2001.

[15] C. Padró, I. Gracia, and S. Martín. Improving the trade-off between storage and communication in broadcast encryption schemes. *Discrete Applied Mathematics*, 143(1-3):213–220, 2004.