匿名放送型暗号における下界再考と匿名放送型認証への応用

小林 大航[1,a)]　渡邉 洋平[2,b)]　四方 順司[1,c)]

概要：放送型暗号（Broadcast Encryption; BE）は, 複数人の受信者の中から送信者が指定した受信者のみが復号できる方式である. BE に望まれる安全性の一つとして, 暗号文から指定された受信者の情報が漏れないことを保証する匿名性が考えられており, これまでにいくつかの匿名性を満たす BE 方式（匿名 BE）が提案されている. Kiayias と Samari（IH 2013）は匿名 BE の暗号文長の下界について解析をおこなっている. 解析の中で, 彼らは匿名 BE に対して暗に特殊な性質を仮定している. しかし, 既存の匿名 BE 方式がその性質を満たすかは明らかでなく, 彼らの解析は既存の匿名 BE 方式が最適な暗号文長を達成していることを示すには不十分である. 本稿では, 既存のほとんどの匿名 BE 方式が満たす性質のみを仮定し, 匿名 BE の暗号文長の下界を導出する. これにより, 匿名 BE の暗号文長について初めてタイトな下界を示す. また, 本稿の解析を匿名放送型認証に適用することで, 小林ら（ISEC 2021-3）の解析で用いられた平文空間への仮定を置くことなく, 認証子サイズの下界を示す.

キーワード：放送型暗号, 匿名性, 下界

Revisiting Lower Bounds in Anonymous Broadcast Encryption and Its Application to Anonymous Broadcast Authentication

Hirokazu KOBAYASHI[1,a)]　Yohei WATANABE[2,b)]　Junji SHIKATA[1,c)]

Abstract: Broadcast Encryption (BE) is a cryptosystem in which a sender can designate a set of recipients so that only the designated recipients can perform decryption. Anonymity, which is one of security requirements of BE, guarantees that ciphertexts never leak information of the specified recipients, and there are several work on BE with anonymity (ANO-BE). Kiayias and Samari (IH 2013) analyzed a lower bound on the ciphertext size required for ANO-BE, assuming a special property for ANO-BE. However, it is unclear whether existing ANO-BE schemes satisfy the special property, i.e., their analysis is insufficient to show that the lower bound is tight. In this paper, we show an asymptotically tight lower bound in ANO-BE, assuming only properties that most existing ANO-BE schemes satisfy. Furthermore, we derive an asymptotically tight lower bound on the authenticator size without an assumption on a message-space considered in Kobayashi et al. (ISEC 2021-3).

Keywords: Broadcast Encryption, Anonymity, Lower Bound

1. はじめに

(匿名) 放送型暗号. 放送型暗号 (BE) は, 送信者が複数人の受信者を指定して平文を暗号化し, 指定された受信者のみがその暗号文を復号できる方式である. BE において, 送信者は N 人の受信者の中から復号権限を与える受信者集合 $\mathcal{S}$ を指定して平文を暗号化する. $\mathcal{S}$ に含まれる受信者のみが暗号文 $\mathsf{ct}_{\mathcal{S}}$ を復号でき, そうでない受信者は復号すること

[1] 横浜国立大学, 〒 240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7, Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa, 240-8501, Japan.
[2] 電気通信大学, 〒 182-8585 東京都調布市調布ヶ丘 1-5-1, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, Japan.
[a)] kobayashi-hirokazu-dr@ynu.jp
[b)] watanabe@uec.ac.jp
[c)] shikata-junji-rb@ynu.ac.jp

ができない. BE はこのような機能をもつことから, 有料放送など様々な適用例が考えられている. 一般に, BE は結託耐性をもつことが望まれており, BE が任意の数の結託者に対して安全であるとき, BE は結託耐性をもつという.

また, BE に望まれる安全性の一つとして, 暗号文 $\mathrm{ct}_{\mathcal{S}}$ から指定された受信者集合 $\mathcal{S}$ の情報が一切漏れないことを保証する匿名性が考えられており, それを満たすいくつかの BE 方式 [3], [10], [11] が提案されている. ここで, 匿名性は BE の実用における観点から重要な安全性となっている. 例えば, 有料放送サービスに BE を適用する際, コンテンツの保護と同様にプライバシーの保護が重要となる場合がある. 匿名性の安全性概念について, 主に匿名性と完全匿名性の二つがそれぞれ Barth ら [3], Kiayias と Samari [9] によって導入されている[*1]. これらの概念は以下のような違いがある: 匿名性は指定された受信者に関する情報のうち, 指定された受信者の人数以外の情報が暗号文から漏れないことを保証する; 完全匿名性は指定された受信者に関する情報がその人数の情報でさえも暗号文から漏れないことを保証する. 本稿では, 匿名性を満たす BE 方式および完全匿名性を満たす BE 方式を, それぞれ匿名 BE, 完全匿名 BE と呼ぶ.

匿名放送型暗号の暗号文長. 既存の匿名性を満たす BE 方式における暗号文長は指定された受信者数, または全ての受信者数に線形に比例している. より詳細には, 既存方式における暗号文長は匿名 BE であれば $O(|\mathcal{S}| \cdot \kappa)$, 完全匿名 BE であれば $O(N \cdot \kappa)$ となっている. ここで, $|\mathcal{S}|$ は指定された受信者集合のサイズ, N はプロトコルに参加している受信者数, κ はセキュリティパラメータを表す. そのため, これらの方式の暗号文長が匿名性を満たす BE 方式の暗号文長の上界となっている.

一方で, Kiayias と Samari [9] は匿名 BE や完全匿名 BE における暗号文長の下界について検討をしている. より正確には, 彼らはある限定されたクラスの BE に対して, 匿名 BE と完全匿名 BE の暗号文長の下界がそれぞれ $\Omega(|\mathcal{S}| \cdot \kappa), \Omega(N \cdot \kappa)$ となることを示しており, そのクラスに該当する匿名 BE 方式として [3], [9], [11] を挙げている[*2]. ここで, 彼らは下界に関する主定理 ([9], 定理 2) において, BE 方式に対し暗に特殊な性質を仮定している. つまり, 実際には彼らは「BE 方式が匿名性およびその特殊な性質を満たしているならば, 下界が成立する」ことを証明している. しかし, その性質が彼らの解析対象である匿名 BE 方式 [3], [9], [11] について成り立つことを検証するのは困難である. そのため, それらの匿名 BE 方式が漸近的に最適な暗号文長を達成していると明確には言えない.

1.1 本稿の貢献

本稿では, 既存のほとんどの匿名 BE 方式が満たす性質のみを仮定し, その性質をもつ BE 方式が匿名性および完全匿名性を満たすための暗号文長の下界について, それぞれ $\Omega(|\mathcal{S}| \cdot \kappa), \Omega(N \cdot \kappa)$ となることを示す. これにより, 初めて既存の匿名 BE 方式が最適な暗号文長を達成していることを示す. 本稿で用いる仮定は既存の BE 方式に対しても成立するため, 暗号文長が我々の下界を達成しない限り, 既存の非匿名な BE を基にした構成を試みても匿名性を得られない.

本稿では解析を容易にするため, Kiayias と Samari [9] と同様に Atomic BE(AtBE) 方式と呼ばれる暗号文と復号鍵をそれぞれ複数個の要素に分割できる BE 方式を考える. AtBE 方式は既存のほとんどの BE 方式を記述可能であり, 広い範囲の BE を捉えることができる方式となっている. そして, 既存のほとんどの匿名 BE 方式がもつ性質を満たす AtBE 方式について, その方式が匿名性を満たすために必要な暗号文の要素数について下界を示すことで, 暗号文長の下界を導出する. 本稿における解析は [9] の解析と比較して以下の点で異なっている.

- 本稿における解析は既存のほとんどの匿名 BE 方式がもついくつかの性質を仮定する. 本稿ではそれらを定式化するため, Kiayias と Samari が形式的に定義していない AtBE 方式のシンタックスを与える.
- 本稿では既存の匿名 BE 方式 [3], [10], [11] が満たす一般的な性質のみを仮定しているため, 導出された下界はこれらの方式に成立する. また, 既存の非匿名な BE 方式の亜種についても本稿の解析は適用できる. 一方で, [9] において仮定されていた性質が既存の匿名 BE 方式に成立するかは明らかではない.

ここで, 本稿で考える AtBE のシンタックスや性質は [9] の結果から自明には導けない内容になっている.

また, 上記と同様な解析を匿名放送型認証 (ABA) におこなうことで, ABA が匿名性および完全匿名性を満たすための認証子サイズの下界がそれぞれ $\Omega(|\mathcal{S}| \cdot \kappa), \Omega(N \cdot \kappa)$ となることを示す. この下界は小林ら [14] の結果とは異なり, 平文空間の大きさが超多項式でない場合にも適用可能である.

1.2 技術的外観

Kiayias と Samari の解析 [9]. Kiayias と Samari は解析を容易にするため, 暗号文と各受信者の復号鍵をそれぞれ atomic 暗号文, atomic 復号鍵と呼ばれる要素に分割できる AtBE 方式を導入している. 彼らの AtBE 方式において, 暗

[*1] 匿名性および完全匿名性と比較して弱い匿名性の安全性概念として, 外部者匿名性 [6] が考えられている. 本稿では, この安全性概念については扱わない.

[*2] Kiayias と Samari は任意の完全匿名 BE についても, 暗号文長の下界が $\Omega(N + \kappa)$ であること ([9], 補題 2) を示している. しかし, その下界を達成する構成は示されていないため, 彼らの下界が漸近的にタイトであるかどうかは不明である. 本稿では, 漸近的にタイトな下界についてのみ議論する.

号文 $\mathsf{ct}_{\mathcal{S}}$ は ρ 個の atomic 暗号文 $\mathsf{ct}_{\mathcal{S}}^{(\theta)}(\theta \in [\rho])$ からなり, 復号鍵 $\mathsf{sk}_{\mathsf{id}}$ は τ 個の atomic 復号鍵 $\mathsf{sk}_{\mathsf{id}}^{(\gamma)}(\gamma \in [\tau])$ からなる. そして, 受信者 id が $\mathcal{S}$ に含まれるならば, 平文 m を生成するような atomic 暗号文 $\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ と復号鍵 $\mathsf{sk}_{\mathsf{id}}^{(\gamma)}$ のペアが少なくとも一つ存在する ($\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ が $\mathsf{sk}_{\mathsf{id}}^{(\gamma)}$ によって復号される).

彼らは匿名性を有する AtBE 方式において, 暗号文に含まれる atomic 暗号文の要素数 ρ の下界を導出することで, 暗号文長の下界を示している. より詳細には, 彼らは [9], 定理 2 において「任意の AtBE 方式について, $\mathsf{ct}_{\mathcal{S}}$ に含まれる atomic 暗号文の要素数が $|\mathcal{S}|$ より小さくなるような集合 $|\mathcal{S}|$ が存在するとき, AtBE 方式は匿名性を満たさない」ことを示している. しかし, 彼らは証明の中で暗に以下のような性質を AtBE 方式に仮定している:

仮定 1: $\mathcal{ID}$ を全ての受信者の集合, 任意の平文 m, 任意の集合 $\mathcal{S} \subseteq \mathcal{ID}$ に対して, $\{\mathsf{ct}_{\mathcal{S}}^{(\theta)}\}_{\theta\in[\rho]} = \mathsf{ct}_{\mathcal{S}} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S})$ とする. もし, 任意の $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ について, $\mathsf{ct}_{\mathcal{S}}$ に含まれる atomic 暗号文 $\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ を復号し m を得られる時, 復号に用いられる atomic 復号鍵 $\mathsf{sk}_{\mathsf{id}}^{(\gamma)}$ と $\mathsf{sk}_{\mathsf{id}'}^{(\gamma')}$ は一致する.

つまり, 彼らが実際に示している定理は「任意の AtBE 方式について, 仮定 1 が成り立ち (AtBE 方式が上記の性質を満たし), かつ $\mathsf{ct}_{\mathcal{S}}$ に含まれる atomic 暗号文の要素数が $|\mathcal{S}|$ より小さくなるような集合 $|\mathcal{S}|$ が存在するとき, AtBE 方式は匿名性を満たさない」となっている. しかし, 任意の匿名性を満たす BE について上記の性質が成立するかを検証するのは困難である. 実際, 既存の全ての匿名 BE について,「任意の $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ について, $\mathsf{ct}_{\mathcal{S}}$ に含まれる atomic 暗号文 $\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ を復号し m を得られる」という状況は起こりえない. ここで, 彼らの定理について対偶をとると「任意の AtBE 方式について, もし AtBE 方式が匿名性を満たすならば, 仮定 1 が成り立たない, または任意の集合 $|\mathcal{S}|$ について, $\mathsf{ct}_{\mathcal{S}}$ に含まれる atomic 暗号文の要素数が $|\mathcal{S}|$ 以上である」となるため, 彼らの下界は AtBE 方式が匿名性を満たし, かつ仮定 1 が成り立つ場合にのみ適用可能である. したがって, 既存の AtBE 方式について仮定 1 が成立するかは不明であることから, 彼らの下界は既存の匿名 BE の暗号文長について最適性を示すには不十分である.

本稿の解析におけるアプローチ. 本稿では, 上記のような特殊な性質ではなく, 既存の BE 方式が満たす性質のみを BE 方式に仮定して暗号文長の下界を導出する.

本稿ではその性質を記述するため, AtBE の形式的な定義を与える. 具体的には, 暗号文と復号鍵に加えて, 公開鍵 pk を複数個の atomic 公開鍵 $\mathsf{pk}^{(\delta)}$ と呼ばれる要素に分割できる AtBE 方式を考える. そして, AtBE 方式の暗号化・復号アルゴリズムとして Enc-at アルゴリズムと Dec-at アルゴリズムを考える. これらのアルゴリズムは, Enc や Dec アルゴリズムの内部でおこなわれる atomic 暗号文ごとの暗号化や復号を表現する. Enc-at では複数個の atomic 公開鍵 $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}$ を用いて, $\mathcal{S}$ 内の受信者 id に対応する atomic 暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ を生成する. Dec-at では atomic 暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ を複数個の atomic 復号鍵 $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}$ を用いて復号する. ここで, 既存のほとんどの BE 方式は上記のアルゴリズムを内部に有している.

本稿では, AtBE 方式のシンタックスに加え, 解析対象の AtBE における以下の 4 つの性質を定式化する.

(1) 任意の集合 $\mathcal{S} \subseteq \mathcal{ID}$ について, 任意の暗号文 $\mathsf{ct}_{\mathcal{S}}$ は atomic 暗号文 $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$ とその他の要素[*3] から構成されており, 任意の受信者 $\mathsf{id} \in \mathcal{S}$ について, $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S}}^{(\theta)})$ となる atomic 復号鍵と atomic 暗号文の組が存在する.

(2) 任意の集合 $\mathcal{S} \subseteq \mathcal{ID}$, 任意の $\mathsf{id} \in \mathcal{S}$, 任意の m について, 正しく atomic 暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}}, \mathcal{S}, \mathsf{m}, \mathsf{id}; \mathsf{r})$ を生成するために必要な要素数が最小の atomic 公開鍵の集合 $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}}$ が $(\mathsf{id}, \mathcal{S}, \mathsf{m})$ の組によって一意に定まる.

(3) 任意の集合 $\mathcal{S} \subseteq \mathcal{ID}$, 任意の $\mathsf{id} \in \mathcal{S}$ について, 正しく生成された atomic 暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ を復号するとき ($\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}}, \mathsf{ct}_{\mathcal{S}}^{(\theta)})$ となるとき), atomic 復号鍵の集合の中で要素数が最小のもの $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}}$ が $(\mathsf{id}, \mathcal{S})$ の組によって一意に定まる.

(4) 任意の集合 $\mathcal{S} \subseteq \mathcal{ID}$, 任意の $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$, 任意の暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ について, もし $\mathsf{ct}_{\mathcal{S},\mathsf{id}} = \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ となるならば, それぞれの生成に必要な atomic 公開鍵のうち要素数が最小のもの $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}}, \{\mathsf{pk}^{(\delta')}\}_{\delta'\in\Delta^*_{\mathsf{id}',\mathcal{S},\mathsf{m}}}$ が一致する.

3.2 節において, 既存のほとんどの BE 方式がこの 4 つの性質を満たすことを示す.

下界の導出の概要. 本稿では, まず上記の性質をもつ BE 方式が匿名性を満たすための条件について解析する. 具体的には,「もし AtBE 方式が匿名性と上記の 4 つの性質を満たすならば, 異なる受信者間で復号に用いる atomic 復号鍵を共有していない」こと (4 節, 補題 2) を示す. そして, 匿名性と上記の 4 つの性質を満たす BE 方式に対して, 既存の匿名 BE 方式 [3], [10], [11] がもつ以下の性質を仮定することで下界を導出する:

仮定 2: 任意の集合 $\mathcal{S} \subseteq \mathcal{ID}$, 任意の $\mathsf{id} \in \mathcal{S}$, 任意の m について, pk' を atomic 暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\mathsf{pk}', \mathcal{S}, \mathsf{m}, \mathsf{id}; \mathsf{r})$ を生成する atomic 公開鍵の部分集合とする. このとき, $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ の復号に用いられる atomic 復号鍵の集合の中で, 要素数が最小となるものが pk' によって一意に定まる.

ここで, 仮定 1 とは異なり, 仮定 2 は既存のほとんどの匿名

[*3] その他の要素には, atomic 暗号文への署名 [3], [11] やダミーの暗号文 [11] が該当する.

性を満たす BE 方式に成立することが確認できる.

最終的には, 上記の 4 つの性質と仮定 2 が成り立つ匿名 BE について, 暗号文 $\mathsf{ct}_{\mathcal{S}}$ に含まれる atomic 暗号文の個数が $|\mathcal{S}|$ より小さくなる集合 $\mathcal{S}$ が存在するとき, 補題 2 と矛盾することを示す.

2. 準備

2.1 記法

任意の自然数 $N \in \mathbb{N}$ に対して, $\{1, \ldots, N\}$ を $[N]$ と書く. 有限集合 $\mathcal{X}$ に対して, $|\mathcal{X}|$ は $\mathcal{X}$ の要素数を表す. 任意の集合 $\mathcal{X}, \mathcal{Y}$ に対して, 対称差を $\mathcal{X} \triangle \mathcal{Y} := (\mathcal{X} \setminus \mathcal{Y}) \cup (\mathcal{Y} \setminus \mathcal{X})$ と定義する. 任意の集合 $\mathcal{X}$ 及び自然数 $\ell \in \mathbb{N}$ に対して, $2^{\mathcal{X}}_{\leq \ell} := \{\mathcal{Y} \subset \mathcal{X} \mid |\mathcal{Y}| \leq \ell\}$ は要素数が ℓ 以下であるような $\mathcal{X}$ の部分集合族である. また, 任意の集合 $\mathcal{X}$ に対して, $x \xleftarrow{\cup} \mathcal{X}$ は集合 $\mathcal{X}$ から要素 x を一様ランダムに取り出すことを表す. 任意の $x \in \{0,1\}^*$ に対して, $|x|$ は x のビット長を表す. 関数 $\mathsf{negl}(\cdot)$ は, 任意の多項式 $\mathsf{poly}(\cdot)$ に対してある定数 $\kappa_0 \in \mathbb{N}$ が存在して, 全ての $\kappa \geq \kappa_0$ に対して $\mathsf{negl}(\kappa) < 1/\mathsf{poly}(\kappa)$ が成り立つ時, $\mathsf{negl}(\cdot)$ は無視可能関数であるという. 論文を通して, κ をセキュリティパラメータとし, 確率的多項式時間を PPT と表す.

2.2 放送型暗号

放送型暗号 (BE) のシンタックスと安全性を定義する. 本稿では, セットアップ時に参加する受信者の上限が決まり, また任意の受信者集合を暗号化時に指定できるとする.

モデル. BE Π^{BE} は以下の 4 つのアルゴリズム (Setup, Join, Enc, Dec) からなる.

- $(\mathsf{mk}, \mathsf{pk}) \leftarrow \mathsf{Setup}(1^\kappa, N, \ell)$: セキュリティパラメータ 1^κ, システム内の最大受信者数 $N \in \mathbb{N}$, 最大指定可能受信者数 ℓ を入力に取り, マスター秘密鍵 mk と公開鍵 pk を出力する.
- $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{mk}, \mathsf{id})$: mk 及び生成したい受信者の識別子 $\mathsf{id} \in \mathcal{ID}$ を入力に取り, 復号鍵 $\mathsf{sk}_{\mathsf{id}}$ を出力する. ここで $\mathcal{ID}$ は識別子空間であり, ある多項式 $\mathsf{poly}(\cdot)$ について $|\mathcal{ID}| := \mathsf{poly}(\kappa)$ である.
- $\mathsf{ct}_{\mathcal{S}} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S}; \mathsf{r})$: pk, 平文 $\mathsf{m} \in \mathcal{M}$, $|\mathcal{S}| \leq \ell$ を満たす受信者集合 $\mathcal{S} \subseteq \mathcal{ID}$ を入力に取り, 暗号文 $\mathsf{ct}_{\mathcal{S}}$ を出力する. ここで, $\mathcal{M}$ は平文空間, $\mathcal{R}$ は乱数空間であり, $\mathsf{r} \in \mathcal{R}$ は内部乱数である. また, r を入力から省略することもある.
- $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathcal{S}})$: $\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathcal{S}}$ を入力に取り, $\mathsf{m} \in \mathcal{M} \cup \{\perp\}$ を出力する.

本稿では, 既存の匿名 BE 方式の性質を定式化するため, Join を決定的アルゴリズムとする[*4].

[*4] Join が確率的にふるまう場合についても, 疑似ランダム関数を用いることにより決定的アルゴリズムとして Join を実現できる.

正当性. 全ての $\kappa, N \in \mathbb{N}$, 全ての $1 \leq \ell \leq N$ であるような ℓ, 全ての $\mathsf{mk} \leftarrow \mathsf{Setup}(1^\kappa, N, \ell)$, 全ての $\mathsf{m} \in \mathcal{M}$, 全ての $\mathsf{r} \in \mathcal{R}$, 全ての $|\mathcal{S}| \leq \ell$ であるような $\mathcal{S} \subseteq \mathcal{ID}$, 全ての $\mathsf{id} \in \mathcal{S}$ に対して, 圧倒的な確率で $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{Join}(\mathsf{mk}, \mathsf{id}), \mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S}; \mathsf{r}))$ が成り立つ.

結託耐性. BE の IND-CPA 安全性を定義する. 挑戦者 C と PPT 攻撃者 A の間の試行 $\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ を考える.

$\underline{\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)}$

C はランダムビット $b \in \{0,1\}$ を選ぶ. C は $\mathsf{Setup}(1^\kappa, N, \ell)$ を実行し, mk を得る. 以下で用いる集合 $\mathcal{D}, \mathcal{CD}$ を空集合として初期化する. $\mathcal{D}$ は現在プロトコルに参加している受信者の集合を, $\mathcal{CD}$ は A が復号鍵を得た受信者の識別子の集合を示す. A は以下のクエリを適応的に C に問い合わせることができる.

参加クエリ. A からのクエリ $\mathsf{id} \in \mathcal{ID}$ を受け取り, C は $\mathcal{D}$ に id を追加し, $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{mk}, \mathsf{id})$ を生成する. ただし, このクエリは高々多項式オーダの N 回のみ許される.

結託クエリ. A からのクエリ $\mathsf{id} \in \mathcal{D}$ を受け取り, C は $\mathcal{CD}$ に id を追加し, $\mathsf{sk}_{\mathsf{id}}$ を A に返す.

チャレンジクエリ. A からのクエリ $(\mathsf{m}_0, \mathsf{m}_1, \mathcal{S}) \in \mathcal{M}^2 \times 2^{\mathcal{D}}_{\leq \ell}$ を受け取り, $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}_b, \mathcal{S})$ を実行し, その出力を A に返す. ただし, このクエリは $\mathcal{S} \cap \mathcal{CD} = \emptyset$ を満たす必要がある. さらに, このクエリは高々 1 回のみ許される.

ある時点で A は b' を出力し, $b = b'$ ならば 1 を, そうでないならば 0 を $\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ の出力とする.

定義 1 (IND-CPA)**.** 任意の PPT アルゴリズム A に対して以下が成り立つならば, Π^{BE} は IND-CPA 安全性を満たすという: 十分大きな $\kappa \in \mathbb{N}$, 任意の $N \in \mathbb{N}$, 任意の ℓ $(\leq N)$ に対して $\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) < \mathsf{negl}(\kappa)$. ここで, $\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) := |\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) \to 1] - \frac{1}{2}|$.

匿名性. BE の匿名性について, 完全匿名性 (full-ANO-CPA 安全性), 匿名性 (ANO-CPA 安全性) を定義する. A を full-ANO-CPA 安全性に対する PPT 攻撃者とする. full-ANO-CPA 安全性は, 試行 $\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ におけるチャレンジクエリを以下のように変更した試行 $\mathsf{Exp}^{\mathsf{full\text{-}ANO}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ によって定義される:

チャレンジクエリ. A からのクエリ $(\mathsf{m}, \mathcal{S}_0, \mathcal{S}_1) \in \mathcal{M} \times \left(2^{\mathcal{D}}_{\leq \ell}\right)^2$ を受け取り, $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S}_b)$ を実行し, その出力を A に返す. ただし, このクエリは $(\mathcal{S}_0 \triangle \mathcal{S}_1) \cap \mathcal{CD} = \emptyset$ を満たす必要がある. さらに, このクエリは高々 1 回のみ許される.

同様に, ANO-CPA 安全性を試行 $\mathsf{Exp}^{\mathsf{full\text{-}ANO}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ におけるチャレンジクエリに以下のような制約を追加した試行 $\mathsf{Exp}^{\mathsf{ANO}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ によって定義する: $|\mathcal{S}_0| = |\mathcal{S}_1|$.

定義 2 (匿名性)**.** 任意の PPT アルゴリズム A に対して以下が成り立つならば, Π^{BE} は X-CPA (X $\in$ {full-ANO, ANO})

安全性を満たすという: 十分大きな $\kappa \in \mathbb{N}$, 任意の $N \in \mathbb{N}$, 任意の $\ell\,(\leq N)$ に対して $\mathsf{Adv}^{X}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) < \mathsf{negl}(\kappa)$. ここで, $\mathsf{Adv}^{X}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) := |\Pr[\mathsf{Exp}^{X}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) \to 1] - \frac{1}{2}|$.

3. Atomic Broadcast Encryption

既存の BE 方式が満たす性質を形式的に記述するため, AtBE のシンタックスを示す. これらの性質は既存の匿名 BE の性質を記述するとき, および暗号文長の下界を導出する際に用いられる. そして, AtBE によって表現される BE について匿名性および完全匿名性を定義する.

3.1 AtBE のシンタックス

AtBE は BE の Enc アルゴリズムや Dec アルゴリズムの内部でおこなわれる, atomic 暗号文ごとの暗号化や復号を記述するモデルである. 以下に AtBE $\Pi^{\mathsf{At\text{-}BE}}$ = (Setup-at, Join-at, Enc-at, Dec-at) のモデルを定義する.

- $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup\text{-}at}(1^\kappa, N, \ell)$: セキュリティパラメータ 1^κ, システム内の最大受信者数 $N \in \mathbb{N}$, 最大指定可能受信者数 ℓ を入力に取り, マスター秘密鍵 mk と $|\Delta|$ 個の atomic 公開鍵からなる公開鍵 $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}$ を出力する.
- $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$: マスター秘密鍵 mk, 生成したい受信者の識別子 $\mathsf{id} \in \mathcal{ID}$ を入力に取り, $|\Gamma_{\mathsf{id}}|$ 個の atomic 復号鍵からなる復号鍵 $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}}$ を出力する.
- $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}, \mathcal{S}, \mathsf{m}, \mathsf{id}; \mathsf{r})$: atomic 公開鍵の集合 $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}$ $(\Delta' \subseteq \Delta)$, $|\mathcal{S}| \leq \ell$ を満たす受信者集合 $\mathcal{S} \subseteq \mathcal{ID}$, 平文 $\mathsf{m} \in \mathcal{M}$, 受信者の識別子 $\mathsf{id} \in \mathcal{ID}$, 乱数 r を入力に取り, atomic 暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ を出力する.
- $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$: 復号鍵の部分集合 $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}$ $(\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}})$, $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ を入力に取り, 平文 $\mathsf{m} \in \mathcal{M} \cup \{\perp\}$ を出力する.

Setup-at と Join-at は公開鍵と復号鍵が明示的に複数個の要素に分割できることを除いて, それぞれ Setup と Join と同等なアルゴリズムである. ここで, Π^{BE} の Join アルゴリズムと同様に, Join-at を決定的アルゴリズムとする. また, 暗号文 $\mathsf{ct}_{\mathcal{S}}$ に含まれる atomic 暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ について, $\mathsf{id} \in \mathcal{S}$ ならば, 受信者 id の復号鍵 $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}}$ によって正しく復号されるという自然な性質を AtBE に要求する:

Atomic Correctness. 全ての $\kappa, N \in \mathbb{N}$, 全ての $1 \leq \ell \leq N$ であるような ℓ, 全ての $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup\text{-}at}(1^\kappa, N, \ell)$, 全ての $\mathsf{m} \in \mathcal{M}$, 全ての $|\mathcal{S}| \leq \ell$ であるような $\mathcal{S} \subseteq \mathcal{ID}$, 全ての $\mathsf{id} \in \mathcal{S}$, 全ての $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$, 全ての $\mathsf{r} \xleftarrow{\cup} \mathcal{R}$ について, ある $\Delta' \subseteq \Delta, \Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$ が存在し, 全ての $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}, \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r})$ に対して, 圧倒的な確率で $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ が成り立つ.

3.2 既存の BE がもつ性質

本節では, Kiayias と Samari らが匿名 BE に対し仮定していた特殊な性質を既存の匿名 BE 方式が明確に満たす性質に変更するため, 既存のほとんどの BE 方式がもつ 4 つの性質を考える. 特に, Boneh ら [4] の構成がそれらの性質をもつことを示す. 以下にその 4 つの性質を示す.

性質 1. Enc アルゴリズムから出力される暗号文 $\mathsf{ct}_{\mathcal{S}}$ は, Enc-at アルゴリズムによって得られた atomic 暗号文 $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ 等から構成される. つまり, $\mathsf{ct}_{\mathcal{S}}$ 内に含まれる atomic 暗号文の集合を $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$, $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$ とその他の要素の和集合を $\{\mathsf{ct}^{(\theta)}_{\mathcal{S}}\}_{\theta\in[\beta_{\mathcal{S}}]}$ とすると, $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}} \subseteq \{\mathsf{ct}^{(\theta)}_{\mathcal{S}}\}_{\theta\in[\beta_{\mathcal{S}}]} \subseteq \mathsf{ct}_{\mathcal{S}}$ が成立する. ここで, $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$ をそれぞれ生成する際に, Enc-at に入力される乱数 r は各 id について同一のものである. また, BE の Dec アルゴリズムの内部では, Dec-at アルゴリズムが atomic 暗号文 $\mathsf{ct}^{(\theta)}_{\mathcal{S}}$ と atomic 復号鍵の集合を $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}$ 入力として, 平文 m を出力する. もし, $\mathsf{ct}_{\mathcal{S}}$ が正当な暗号文であるならば, 受信者 $\mathsf{id} \in \mathcal{S}$ の atomic 復号鍵の部分集合を用いて復号される atomic 暗号文 $\mathsf{ct}^{(\theta)}_{\mathcal{S}}$ が $\mathsf{ct}_{\mathcal{S}}$ 内に存在する. 形式的には, BE Π^{BE} に対して以下の性質を要求する:

全ての $\kappa, N \in \mathbb{N}$, 全ての $1 \leq \ell \leq N$ であるような ℓ, 全ての $(\mathsf{mk}, \mathsf{pk}) \leftarrow \Pi^{\mathsf{BE}}.\mathsf{Setup}(1^\kappa, N, \ell)$, 全ての $\mathsf{m} \in \mathcal{M}$, 全ての $|\mathcal{S}| \leq \ell$ であるような $\mathcal{S} \subseteq \mathcal{ID}$, 全ての $\mathsf{id} \in \mathcal{ID}$, 全ての $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \Pi^{\mathsf{At\text{-}BE}}.\mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$, 全ての $\mathsf{r} \xleftarrow{\cup} \mathcal{R}$, 全ての $\{\mathsf{ct}^{(\theta)}_{\mathcal{S}}\}_{\theta\in[\beta_{\mathcal{S}}]} \subseteq \mathsf{ct}_{\mathcal{S}} \leftarrow \Pi^{\mathsf{BE}}.\mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S}; \mathsf{r})$ について, $\mathsf{id} \in \mathcal{S}$ ならば, 圧倒的な確率で, ある $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$ が存在し, $\mathsf{m} \leftarrow \Pi^{\mathsf{At\text{-}BE}}.\mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}^{(\theta)}_{\mathcal{S}})$ となる $\theta \in [\beta_{\mathcal{S}}]$ が存在する. $\mathsf{id} \notin \mathcal{S}$ ならば, 任意の $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$ について, $\mathsf{m} \leftarrow \Pi^{\mathsf{At\text{-}BE}}.\mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}^{(\theta)}_{\mathcal{S}})$ となる $\theta \in [\beta_{\mathcal{S}}]$ が存在する確率が $\mathsf{negl}(\kappa)$ である.

性質 2. $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}, \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r})$ が生成されるとき, Enc-at に入力する atomic 公開鍵の集合の中で要素数が最小のものを $\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}$ とする. このとき, $\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}$ は Enc-at に入力する $(\mathsf{id}, \mathcal{S}, \mathsf{m})$ によって一意に定まる.

性質 3. $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ となるとき, Dec-at に入力する atomic 復号鍵の集合の中で要素数が最小のものを $\Gamma^*_{\mathsf{id},\mathcal{S}}$ とする. このとき, $\Gamma^*_{\mathsf{id},\mathcal{S}}$ は $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ を生成する際, Enc-at へ入力する $(\mathsf{id}, \mathcal{S})$ によって一意に定まる.

性質 4. 任意の $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup\text{-}at}(1^\kappa, N, \ell)$, 任意の $\mathsf{id}, \mathsf{id}' \in \mathcal{ID}$, 任意の $\{\mathsf{id}, \mathsf{id}'\} \subseteq \mathcal{S}$ となるような $\mathcal{S}$, 任意の m, r, 任意の $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}}, \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r}), \mathsf{ct}_{\mathcal{S},\mathsf{id}'} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta')}\}_{\delta'\in\Delta^*_{\mathsf{id}',\mathcal{S},\mathsf{m}}}, \mathsf{id}', \mathsf{m}, \mathcal{S}; \mathsf{r})$ について, $\mathsf{ct}_{\mathcal{S},\mathsf{id}} = \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ ならば, 圧倒的な確率で $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}} = \{\mathsf{pk}^{(\delta')}\}_{\delta'\in\Delta^*_{\mathsf{id}',\mathcal{S},\mathsf{m}}}$ が成り立つ.

以下では Boneh らのペアリングベースの方式 [4] について上記の性質が成り立つことを示す. Boneh らの BE 方式の概

要は以下のとおりである: p を素数, g を位数 p の双線形群 $\mathbb{G}$ からランダムに選んだ生成元, $\mathbb{Z}_p := \{1, \ldots, p-1\}, \alpha, s \xleftarrow{\cup} \mathbb{Z}_p$ とする. Boneh らの方式における公開鍵, 受信者 $\mathsf{id} \in [N]$ の復号鍵, $\mathcal{S}$ を指定した暗号文は以下の通りである. $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta} := \{g, g_1, \ldots, g_N, g_{N+2}, \ldots, g_{2N}, v\}, \{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}} := \{g_{\mathsf{id}}^s\} \cup \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}, \{\mathsf{ct}_{\mathcal{S}}^{(\theta)}\}_{\theta\in[\beta_{\mathcal{S}}]} = \mathsf{ct}_{\mathcal{S}} := \{(g^r, (v \cdot \prod_{j\in\mathcal{S}} g_{N+1-j})^r)\}$. ただし, $g_{\mathsf{id}} := g^{\alpha^{\mathsf{id}}}, v := g^s, r \xleftarrow{\cup} \mathbb{Z}_p$ である.

任意の $\mathsf{id} \in \mathcal{S}$ の atomic 暗号文について,

$$\mathsf{ct}_{\mathcal{S},\mathsf{id}} := \{(g^r, (v \cdot \prod_{j\in\mathcal{S}} g_{N+1-j})^r)\},$$

$$\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}} := \{g_{\mathsf{id}}^s, g, \{g_{N+1-j+\mathsf{id}}\}_{\substack{j\in\mathcal{S},\\ j\neq\mathsf{id}}}, v\},$$

$$\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$$

となるので, 性質 1 を満たしている.

公開鍵について, $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ の生成に用いられる atomic 公開鍵の集合の内, 要素数が最小のものは $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}} := \{g, \{g_{N+1-j}\}_{j\in\mathcal{S}}, v\}$ と一意に定まるため, 性質 2 が成り立つ.

また, $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ の復号に用いられる atomic 復号鍵の集合について, $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}} := \{g_{\mathsf{id}}^s, g, \{g_{N+1-j+\mathsf{id}}\}_{\substack{j\in\mathcal{S},\\ j\neq\mathsf{id}}}, v\}$ と一意に定まる. したがって, 性質 3 を満たしている.

そして, id' を指定した atomic 暗号文は $\mathsf{ct}_{\mathcal{S},\mathsf{id}'} := \{(g^r, (v \cdot \prod_{j\in\mathcal{S}} g_{N+1-j})^r)\}$ であるため, $\mathsf{ct}_{\mathcal{S},\mathsf{id}} = \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ となるならば圧倒的な確率で $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}} = \{\mathsf{pk}^{(\delta')}\}_{\delta'\in\Delta^*_{\mathsf{id}',\mathcal{S},\mathsf{m}}}$ が成立する.

以上より, Boneh らの方式は性質 1~4 を満たしている. ここで, 既存のほとんどの BE 方式 [1], [2], [3], [5], [7], [8], [10], [11], [13] は性質 1~4 を満たしており, 本稿において上記の性質を仮定するのは妥当である.

3.3 AtBE によって表現される BE の安全性定義

AtBE によって表現される BE について, 結託耐性 (INDat-CPA), 完全匿名性 (full-ANOat-CPA), そして匿名性 (ANOat-CPA) を定義する. これらの安全性は, 攻撃者が得られる復号鍵やチャレンジ暗号文が明示的に複数個の要素に分割できることを除いて, BE の安全性と同等なものである.

INDat-CPA 安全性 INDat-CPA 安全性に対する PPT 攻撃者を A とする. INDat-CPA 安全性は試行 $\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ の参加クエリと結託クエリに対して, 以下のような変更を加えた試行 $\mathsf{Exp}^{\mathsf{INDat\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ によって定義される.

参加クエリ. A からのクエリ $\mathsf{id} \in \mathcal{ID}$ に対して挑戦者 C は $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{mk}, \mathsf{id})$ ではなく, $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$ を生成する.

結託クエリ. A からのクエリ $\mathsf{id} \in \mathcal{D}$ に対して挑戦者 C は $\mathsf{sk}_{\mathsf{id}}$ ではなく, $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}}$ を返す.

定義 3 (INDat-CPA)**.** 任意の PPT アルゴリズム A に対して以下が成り立つならば, Π^{BE} は INDat-CPA 安全性を満たすという: 十分大きな $\kappa \in \mathbb{N}$, 任意の $N \in \mathbb{N}$, 任意の $\ell\ (\leq N)$ に対して $\mathsf{Adv}^{\mathsf{INDat\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) < \mathsf{negl}(\kappa)$. ここで, $\mathsf{Adv}^{\mathsf{INDat\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) := |\Pr[\mathsf{Exp}^{\mathsf{INDat\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) \to 1] - \frac{1}{2}|$.

匿名性 full-ANOat-CPA 安全性に対する PPT 攻撃者を A とする. full-ANOat-CPA 安全性は試行 $\mathsf{Exp}^{\mathsf{INDat\text{-}CPA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ のチャレンジクエリに対して, 以下のような変更を加えた試行 $\mathsf{Exp}^{\mathsf{full\text{-}ANOat}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ によって定義される.

チャレンジクエリ. A からのクエリ $(\mathsf{m}, \mathcal{S}_0, \mathcal{S}_1) \in \mathcal{M} \times \left(2^{\mathcal{D}}_{\leq\ell}\right)^2$ を受け取り, $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S}_b)$ を実行し, その出力を A に返す. ただし, このクエリは $(\mathcal{S}_0 \triangle \mathcal{S}_1) \cap \mathcal{CD} = \emptyset$ を満たす必要がある. さらに, このクエリは高々 1 回のみ許される.

同様に, ANOat-CPA 安全性を試行 $\mathsf{Exp}^{\mathsf{full\text{-}ANOat}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ におけるチャレンジクエリに以下のような制約を追加した試行 $\mathsf{Exp}^{\mathsf{ANOat}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell)$ によって定義する: $|\mathcal{S}_0| = |\mathcal{S}_1|$.

定義 4 (匿名性)**.** 任意の PPT アルゴリズム A に対して以下が成り立つならば, Π^{BE} は X-CPA ($\mathsf{X} \in \{\text{full-ANOat}, \text{ANOat}\}$) 安全性を満たすという: 十分大きな $\kappa \in \mathbb{N}$, 任意の $N \in \mathbb{N}$, 任意の $\ell\ (\leq N)$ に対して $\mathsf{Adv}^{X}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) < \mathsf{negl}(\kappa)$. ここで, $\mathsf{Adv}^{X}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) := |\Pr[\mathsf{Exp}^{X}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N, \ell) \to 1] - \frac{1}{2}|$.

4. (完全) 匿名 BE における暗号文長の下界

本節では, ANOat-CPA 安全性および full-ANOat-CPA 安全性をもつ BE 方式について暗号文長の下界を導出する. まず, BE 方式に追加で仮定する性質について述べ, Libert ら [11] の匿名 BE 方式がその性質を満たすことを示す. その後, 4.2 節において, その性質を満たす匿名 BE および完全匿名 BE について暗号文長の下界を導出する. 以降の解析では, BE 方式に対して INDat-CPA 安全性を仮定する.

4.1 匿名 BE 方式の性質

本稿では, 3.2 節に示した性質 1~4 をもつ BE に対し,「ある暗号文の復号に用いる鍵の中で最小の構成要素からなるものは, その暗号化に用いた鍵によって一意に定まる」という性質を追加で仮定することにより下界の導出をおこなう. 具体的には以下のような性質を考える:

仮定 2. 任意の $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup\text{-}at}(1^\kappa, N, \ell)$ について, $\mathcal{PK}^* := \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}$ とする. 任意の $\mathsf{id} \in \mathcal{ID}, \{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$ について, 復号時に Dec-at へ入力する atomic 復号鍵の集合の中で要素数が最小となる集合は $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}}$ ($\Gamma^*_{\mathsf{id},\mathcal{S}} \subseteq \Gamma_{\mathsf{id}}$) であり, この集合を要素とする集合族 $\{\{\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}}\}_{\mathsf{id}\in\mathcal{ID},\mathcal{S}\subseteq\mathcal{ID}}$ を $\mathcal{SK}^*$ とする. ここで, Join-at は決定的アルゴリズムなので $\mathcal{SK}^*$ は一意に定まる. このとき, 任意の $\mathsf{id} \in \mathcal{ID}, \mathcal{S} \subseteq \mathcal{ID}, \mathsf{m} \in \mathcal{M}, \mathsf{r} \in \mathcal{R}, \mathsf{pk}' \in 2^{\mathcal{PK}^*}, \mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\mathsf{pk}', \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r})$ について, $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\mathsf{sk}', \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ となる atomic 復号鍵の集合 $\mathsf{sk}' \in \mathcal{SK}^* \cup \{\perp\}$ が atomic 公開鍵の集合 pk' によって一意に定まる.

上記の性質を満たす BE 方式として, 公開鍵暗号 PKE とワンタイム署名 OTS を用いた一般的な構成である Libert らの方式 [11] が挙げられる. その概要を以下に示す.

Π^{BE}.Setup$(1^\kappa, N, \ell)$: 全ての $\mathsf{id} \in [N]$ について, $(\mathsf{pke.pk_{id}}, \mathsf{pke.sk_{id}}) \leftarrow \mathsf{PKE.KGen}(1^\kappa)$ を実行し, $\mathsf{pk} := \{\mathsf{pke.pk_{id}}\}_{\mathsf{id}\in[N]}$, $\mathsf{mk} := \{\mathsf{pke.sk_{id}}\}_{\mathsf{id}\in[N]}$ を出力する.

Π^{BE}.Join(mk, id): $\mathsf{pke.sk_{id}}$ を出力する.

Π^{BE}.Enc(pk, m, $\mathcal{S}$): $(\mathsf{ots.sk}, \mathsf{ots.vk}) \leftarrow \mathsf{OTS.KGen}(1^\kappa)$ を実行する. 全ての $\mathsf{id} \in \mathcal{S}$ について, $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{PKE.Enc}(\mathsf{pke.pk_{id}}, \mathsf{m}||\mathsf{ots.vk})$ を計算し, $\sigma \leftarrow \mathsf{OTS.Sign}(\mathsf{ots.sk}, \{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}})$ を実行した後, $\mathsf{ct}_{\mathcal{S}} := (\sigma, \{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}})$ を出力する.

Π^{BE}.Dec($\mathsf{sk_{id}}, \mathsf{ct}_{\mathcal{S}}$): $\mathsf{ct}_{\mathcal{S}} = (\sigma, \{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}})$ とする. 任意の $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \in \{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$ について, $\mathsf{m}' \leftarrow \mathsf{PKE.Dec}(\mathsf{pke.sk_{id}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ を計算する. $\mathsf{m}||\mathsf{ots.vk} \leftarrow \mathsf{m}'$ とし, $1 \leftarrow \mathsf{OTS.Vrfy}(\mathsf{ots.vk}, \sigma, \{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}})$ ならば m を出力する.

上記の構成について, Enc, Dec の内部で実行される PKE.Enc と PKE.Dec がそれぞれ Enc-at, Dec-at に対応している. また, $\mathcal{PK}^* = \{\mathsf{pke.pk}_1, \ldots, \mathsf{pke.pk}_N\}$, $\mathcal{SK}^* = \{\{\mathsf{pke.sk}_1\}, \ldots, \{\mathsf{pke.sk}_N\}\}$ となっている. ここで, $\mathsf{m}' \leftarrow \mathsf{PKE.Dec}(\mathsf{pke.sk_{id}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ となる $\mathsf{pke.sk_{id}} = \mathsf{sk}' \in \mathcal{SK}^* \cup \{\perp\}$ は $\{\mathsf{pke.pk_{id}}\} \in 2^{\mathcal{PK}^*}$ によって一意に定まるため, 上記の構成について仮定 2 が成り立つ. また, 既存の匿名 BE 方式 [3], [10] についても仮定 2 が成り立つことが, 同様の議論で確認できる.

4.2 ANOat-CPA 安全性を満たす BE における下界の導出

3.2 節の性質 1~4 および ANOat-CPA 安全性を満たす BE について, 二つの補題を示す. 補題 1 では, 「BE が ANOat-CPA を満たすならば, 要素数が等しく異なる集合 $\mathcal{S}_0, \mathcal{S}_1$ を指定された暗号文について, 受信者 id がそれぞれの復号に用いる atomic 復号鍵の集合は等しい」ことを示す. また, 補題 2 では補題 1 を用いて, 「BE が ANOat-CPA を満たすならば, 要素数が 2 以上の集合 $\mathcal{S}$ について, $\mathcal{S}$ に含まれる受信者 $\mathsf{id}, \mathsf{id}'$ は復号に用いる atomic 復号鍵の集合を共有していてはならない」ことを示す.

そして, 性質 1~4 と ANOat-CPA 安全性に加え, 4.1 節の仮定 2 が成り立つ BE について下界を示す. 以下で用いられる記法については, 3.2 節および 4.1 節を参照されたい.

補題 1. BE Π^{BE} が ANOat-CPA 安全性を満たすならば, 任意の $\mathsf{id} \in \mathcal{ID}$, 任意の $\mathsf{id} \in \mathcal{S}_0 \cap \mathcal{S}_1, |\mathcal{S}_0| = |\mathcal{S}_1|$ となるような集合 $\mathcal{S}_0, \mathcal{S}_1$ について, $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}_0}} = \{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}_1}}$ である.

証明. 対偶である「ある $\mathsf{id} \in \mathcal{ID}$, ある $\mathsf{id} \in \mathcal{S}_0 \cap \mathcal{S}_1, |\mathcal{S}_0| = |\mathcal{S}_1|$ を満たす集合 $\mathcal{S}_0, \mathcal{S}_1$ について, $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}_0}} \neq \{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}_1}}$ ならば, BE Π^{BE} の ANOat-CPA 安全性を破る PPT 攻撃者を構成できる」を示す. ここで, 上記のような id を id^* とする. はじめに、攻撃者は上記のような $\mathcal{S}_0, \mathcal{S}_1$ の大きさを $\ell^* \xleftarrow{\cup} [\ell]$ として推測する. 次に, 攻撃者は $\mathsf{id}^*, \mathcal{S}_0, \mathcal{S}_1$ をランダムに選び推測する. このとき, 攻撃者が推測に成功する確率は $\frac{1}{|\mathcal{ID}|} \cdot \frac{1}{\ell} \cdot \binom{|\mathcal{ID}|}{\ell^*-1}^{-1} \cdot \left(\binom{|\mathcal{ID}|}{\ell^*-1} - 1\right)^{-1}$ となる. また, 攻撃者は $\mathcal{S}_0 \cup \mathcal{S}_1$ に含まれる全ての id について参加クエリを, id^* について結託クエリを発行し, 復号鍵 $\{\mathsf{sk}_{\mathsf{id}^*}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}^*}}$ を得る. そして, 攻撃者はチャレンジクエリ $(\mathsf{m}, \mathcal{S}_0, \mathcal{S}_1)$ を発行し, $\{\mathsf{ct}_{\mathcal{S}_b}^{(\theta)}\}_{\theta\in[\beta_{\mathcal{S}_b}]} \subseteq \mathsf{ct}_{\mathcal{S}_b}$ を得る. その後, 攻撃者は $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}^*}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id}^*,\mathcal{S}_0}}, \mathsf{ct}_{\mathcal{S}_b}^{(\theta)})$ となる $\theta \in [\beta_{\mathcal{S}_b}]$ が存在するとき $b' = 0$ を, そうでなければ $b' = 1$ を出力する. このとき, 攻撃者は $\frac{1}{2}\left(\frac{1}{|\mathcal{ID}|} \cdot \frac{1}{\ell} \cdot \binom{|\mathcal{ID}|}{\ell^*-1}^{-1} \cdot \left(\binom{|\mathcal{ID}|}{\ell^*-1} - 1\right)^{-1} + 1\right)$ の確率で $b = b'$ となる b' を出力できる. ここで, $|\mathcal{ID}| = \mathrm{poly}(\kappa)$ および ℓ^* は高々多項式オーダであることから, 上記の攻撃者の優位性は κ に関して無視できない. □

補題 2. BE Π^{BE} が ANOat-CPA 安全性を満たすならば, 任意の $\mathsf{id}, \mathsf{id}' \in \mathcal{ID}$, 任意の $\{\mathsf{id}, \mathsf{id}'\} \subseteq \mathcal{S}, |\mathcal{S}| \geq 2$ となるような集合 $\mathcal{S}$ について, $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}} \neq \{\mathsf{sk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}}}$ である.

証明. ある $\mathsf{id}, \mathsf{id}' \in \mathcal{ID}$, ある $\{\mathsf{id}, \mathsf{id}'\} \subseteq \mathcal{S}$ を満たす集合 $\mathcal{S}$ について, $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}} = \{\mathsf{sk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}}}$ となることを仮定し, Atomic BE の構造をもつ BE の正当性 (3.2 節, 性質 1) に矛盾することを示す. はじめに, $\mathsf{id} \in \mathcal{S}', \mathsf{id}' \notin \mathcal{S}', |\mathcal{S}| = |\mathcal{S}'|$ となるような $\mathcal{S}'$ を選ぶ. このとき, $\mathsf{id} \in \mathcal{S}'$ であることから $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}'}}, \mathsf{ct}_{\mathcal{S}',\mathsf{id}})$; が成立する. また, 補題 1 より $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}'}} = \{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}}$ となることから, $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}}, \mathsf{ct}_{\mathcal{S}',\mathsf{id}})$; が成立する. ここで, 仮定より $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}} = \{\mathsf{sk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}}}$ となるため, $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}}}, \mathsf{ct}_{\mathcal{S}',\mathsf{id}})$; が成立する. しかし, $\mathsf{id}' \notin \mathcal{S}'$ より性質 1 に矛盾が生じる. □

次に, 「暗号文 $\mathsf{ct}_{\mathcal{S}}$ 含まれる atomic 暗号文の個数 $\beta_{\mathcal{S}}$ が $|\mathcal{S}|$ より少なくなるような集合 $\mathcal{S}$ が存在するとき, 補題 2 に対して矛盾が生じる」ことを示す.

定理 1. 4.1 節に示す仮定 2 が成り立つ BE Π^{BE} について, その方式が ANOat-CPA 安全性を満たすならば, 任意の受信者集合 $\mathcal{S} \subseteq \mathcal{ID}$ を指定した暗号文長は $\Omega(|\mathcal{S}| \cdot k)$ である (ただし, $k = \min_{\mathcal{S}\subseteq\mathcal{ID}, \theta\in[\beta_{\mathcal{S}}]} |\mathsf{ct}_{\mathcal{S}}^{(\theta)}|$).

証明. ある受信者集合 $\mathcal{S}^*$ について $\beta_{\mathcal{S}^*} < |\mathcal{S}^*|$ となると仮定し, 補題 2 に矛盾することを示す. ここで, $\beta_{\mathcal{S}^*} \geq 1$ より, $\mathcal{S}^*$ の要素数について $|\mathcal{S}^*| \geq 2$ であるとする. $\beta_{\mathcal{S}^*} < |\mathcal{S}^*|$ から, atomic 暗号文の集合 $\{\mathsf{ct}_{\mathcal{S}^*}^{(\theta)}\}_{\theta\in[\beta_{\mathcal{S}^*}]}$ において少なくとも一つは二人の受信者 $\mathsf{id}, \mathsf{id}' \in \mathcal{S}^*$ によって復号される atomic 暗号文 $\mathsf{ct}_{\mathcal{S}^*}^{(\theta^*)}$ が存在する. すなわち, $\mathsf{id}, \mathsf{id}' \in \mathcal{ID}, \{\mathsf{id}, \mathsf{id}'\} \subseteq \mathcal{S}^*$ と任意の m, r について, $\mathsf{ct}_{\mathcal{S},\mathsf{id}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ を以下の (1), (2) のように生成したとき, $\mathsf{ct}_{\mathcal{S}^*}^{(\theta^*)} = \mathsf{ct}_{\mathcal{S},\mathsf{id}} = \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ が成立する.

$$\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}}}, \mathsf{id}, \mathsf{m}, \mathcal{S}^*; \mathsf{r}) \quad (1)$$

$$\mathsf{ct}_{\mathcal{S},\mathsf{id}'} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}}}, \mathsf{id}', \mathsf{m}, \mathcal{S}^*; \mathsf{r}) \quad (2)$$

ここで $\mathsf{ct}_{\mathcal{S},\mathsf{id}} = \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ と BE の性質 4 より $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}}} = \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}}}$ が成立する. また, Atomic Correctness から

$$\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}^*}}, \mathsf{ct}^{(\theta^*)}_{\mathcal{S}^*}) \tag{3}$$

$$\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}^*}}, \mathsf{ct}^{(\theta^*)}_{\mathcal{S}^*}) \tag{4}$$

が成立する. このとき, $\mathsf{ct}^{(\theta^*)}_{\mathcal{S}^*}$ の暗号化に用いた atomic 公開鍵の集合は $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}}} = \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}}}$ である. そのため, 4.1 節の仮定 2 から $\mathsf{ct}^{(\theta^*)}_{\mathcal{S}^*}$ の復号に用いられる atomic 復号鍵の集合の中で, 要素数が最小のものは一意に定まる. したがって (3),(4) が成り立つためには, $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}^*}} = \{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}^*}}$ が成立する必要がある. しかし, 上記の等式は補題 2 に矛盾する. したがって, $\beta_{\mathcal{S}^*} < |\mathcal{S}^*|$ となる集合 $\mathcal{S}^*$ の存在を仮定すると, 補題 2 に矛盾する. □

4.3 full-ANOat-CPA 安全性をもつ BE 方式における下界

補題 3 では, 「BE が full-ANOat-CPA 安全ならば, 任意の集合 $\mathcal{S},\mathcal{S}'$ について暗号文に含まれる atomic 暗号文の数について $\beta_{\mathcal{S}} = \beta_{\mathcal{S}'}$ となる」ことを示す. 定理 2 では, full-ANOat-CPA 安全性を満たし仮定 2 が成り立つ BE について, 暗号文長の下界を定理 1 と補題 3 から導出する. 補題 3 と定理 2 はそれぞれ補題 1 および [9], 系 1 と同様な議論で示すことができるため, 本稿において証明は省略する.

補題 3. BE Π^{BE} が full-ANOat-CPA 安全性を満たすならば, 任意の集合 $\mathcal{S},\mathcal{S}'$ について $\beta_{\mathcal{S}} = \beta_{\mathcal{S}'}$ である.

定理 2. 4.1 節に示す仮定 2 が成り立つ BE Π^{BE} について, その方式が full-ANOat-CPA 安全性を満たすならば, 任意の受信者集合 $\mathcal{S} \subseteq \mathcal{ID}$ を指定した暗号文のサイズは $\Omega(N\cdot k)$ である (ただし, $k = \min_{\mathcal{S}\subseteq\mathcal{ID},\theta\in[\beta_{\mathcal{S}}]} |\mathsf{ct}^{(\theta)}_{\mathcal{S}}|$).

5. 匿名放送型認証

匿名放送認証 (ABA)[12] は送信者が複数の受信者の中から認証子を受理できる検証者を指定できる方式である. この機能に加え, ABA は認証子 $\mathsf{cmd}_{\mathcal{S}}$ から指定された検証者の情報が漏れない匿名性を要求される. Watanabe ら [12] は BE と同様な二つの匿名性概念である, 完全匿名性と匿名性を導入している. 小林ら [14] は ABA における認証子サイズの下界について, 完全匿名性を満たす ABA では $\Omega(N\cdot\kappa)$, 匿名性を満たす ABA では $\Omega(|\mathcal{S}|\cdot\kappa)$ となることを示しているが, 平文空間が超多項式であるという仮定を置いている.

紙面の都合上, 詳細な議論はおこなわないが, 本稿の BE に対する解析を ABA に適用することで平文空間へ仮定を置くことなく上記の下界を導出することができる.

謝辞. 本研究は総務省の「電波資源拡大のための研究開発 (JPJ000254)」における委託研究「電波の有効利用のための IoT マルウェア無害化／無機能化技術等に関する研究開発」によって実施した成果を含みます.

参考文献

[1] S. Agrawal, D. Wichs, and S. Yamada. Optimal broadcast encryption from lwe and pairings in the standard model. In R. Pass and K. Pietrzak, editors, *Theory of Cryptography*, pages 149–178, Cham, 2020. Springer International Publishing.

[2] S. Agrawal and S. Yamada. Optimal broadcast encryption from pairings and LWE. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 13–43, Cham, 2020. Springer International Publishing.

[3] W. B. Barth A., Boneh D. Privacy in encrypted content distribution using private broadcast encryption. In R. A. Di Crescenzo G., editor, *Financial Cryptography and Data Security. FC 2006*, volume 4107. Springer Berlin Heidelberg, 2006.

[4] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In V. Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3621, pages 258–275. Springer Berlin Heidelberg, 2005.

[5] D. Boneh, B. Waters, and M. Zhandry. Low overhead broadcast encryption from multilinear maps. In J. A. Garay and R. Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, pages 206–223, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[6] N. Fazio and I. M. Perera. Outsider-anonymous broadcast encryption with sublinear ciphertexts. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *Public Key Cryptography – PKC 2012*, pages 225–242, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[7] R. Gay, L. Kowalczyk, and H. Wee. Tight adaptively secure broadcast encryption with short ciphertexts and keys. In D. Catalano and R. De Prisco, editors, *Security and Cryptography for Networks, SCN 2018*, pages 123–139, Cham, 2018. Springer International Publishing.

[8] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In A. Joux, editor, *Advances in Cryptology - EUROCRYPT 2009*, pages 171–188, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[9] A. Kiayias and K. Samari. Lower bounds for private broadcast encryption. In M. Kirchner and D. Ghosal, editors, *Information Hiding*, pages 176–190, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[10] J. Li and J. Gong. Improved anonymous broadcast encryptions. In B. Preneel and F. Vercauteren, editors, *Applied Cryptography and Network Security, ACNS 2018*, pages 497–515, Cham, 2018. Springer International Publishing.

[11] B. Libert, K. G. Paterson, and E. A. Quaglia. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *Public Key Cryptography – PKC 2012*, pages 206–224, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[12] Y. Watanabe, N. Yanai, and J. Shikata. Anonymous broadcast authentication for securely remote-controlling iot devices. In L. Barolli, I. Woungang, and T. Enokido, editors, *Advanced Information Networking and Applications*, pages 679–690, Cham, 2021. Springer International Publishing.

[13] B. Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In S. Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, pages 619–636, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[14] 小林大航, 渡邉洋平, 四方順司. 匿名放送型認証における安全性概念の関係性と認証子サイズの下界について. In **電子情報通信学会** *WBS・IT・ISEC* **合同研究会**, 2021.