CCA 安全な平文一致確認可能属性ベース暗号の一般的構成

浅野 京一[1,2,a)]　江村 恵太[2]　高安 敦[3]　渡邉 洋平[1,2]

概要：平文一致確認可能属性ベース暗号 (Attribute-based Encryption with Equality Test; ABEET) は，属性ベース暗号 (Attribute-based Encryption; ABE) の拡張であり，トラップドアを持つユーザは 2 つの暗号文の平文が同じか否かの確認が可能である．これまで，単調スパンプログラムに対するいくつかの ABEET 方式が提案されているが，いずれも q タイプ仮定のもとで選択的 CCA 安全性しか達成していない．本論文では，Lee らの階層型 ID ベース暗号を用いた CCA 安全な平文一致確認可能 ID ベース暗号の一般的構成を属性ベースに拡張することで，委譲可能性を持つ ABE から CCA 安全な ABEET の一般的構成を提案する．提案構成法を既存の委譲可能性を持つ ABE 方式と組み合わせることで，LWE 仮定や k-linear 仮定，適応的安全性，非単調スパンプログラムなどのより複雑な述語，定数サイズの暗号文や秘密鍵など既存方式では達成していない様々な特性を持つ ABEET 方式を得る．

キーワード：属性ベース暗号, 平文一致確認, CCA 安全性, 一般的構成

A Generic Construction of CCA-secure Attribute-based Encryption with Equality Test from Delegatable Attribute-based Encryption

Kyoichi Asano[1,2,a)]　Keita Emura[2]　Atsushi Takayasu[3]　Yohei Watanabe[1,2]

Abstract: Attribute-based encryption with equality test (ABEET) is an extension of attribute-based encryption (ABE) that can check the plaintext equality of two distinct ciphertexts. There are several CCA-secure ABEET schemes that satisfy selective security under q-type assumptions for monotone span programs. In this paper, we propose a generic method that constructs a CCA-secure ABEET from delegatable ABE. Specifically, we extend the generic construction of Lee et al.'s identity-based encryption with equality test, which uses hierarchical identity-based encryption, to attribute-based. To the best of our knowledge, there are various delegetable ABE schemes. So, we can obtain ABEET schemes that have previously not been achieved, for example, various predicates, adaptive security, standard assumptions, compact ciphertexts/secret keys, and lattice-based constructions.

Keywords: attribute-based encryption, equality test, CCA security, generic construction

1. はじめに

1.1 背景

平文一致確認可能公開鍵暗号 (Public Key Encryption with Equality Test; PKEET) の概念は Yang ら [26] によって提案された．PKEET は検索可能暗号に似た多目的な方式であり，複数の公開鍵と秘密鍵のペア $(\mathsf{pk}_1, \mathsf{sk}_1), \ldots, (\mathsf{pk}_N, \mathsf{sk}_N)$ を持つ．ct_i と ct_j をそれぞれ pk_i と pk_j による平文 M_i と M_j の暗号文とする．標準的な公開鍵暗号の場合と同様に，秘密鍵 sk_i と sk_j はそれぞれ ct_i と ct_j を復号して，M_i と M_j を得られる．その上，PKEET は平文一致確認を行うためのトラップドア td を持つ．td_i と td_j をそれぞれ秘密鍵 sk_i と sk_j で生成されるトラップドアとする．i 番目のユーザが j 番目のトラップドアを入手しても，j 番目の暗号文 ct_j を復号することはできない一方

[1] 電気通信大学
The University of Electro-Communications
[2] 国立研究開発法人情報通信研究機構
NICT
[3] 東京大学
The University of Tokyo
[a)] k.asano@uec.ac.jp

で，トラップドア td_i と td_j を持つユーザは，ct_i と ct_j が同じ平文の暗号化であるかどうか確認可能である．PKEET の応用例として，Yang ら [26] は暗号化データの分割を行う委託データベースについて検討し，データベース管理者がメッセージ所有者の助けを借りずに機密データを収集・分類できることを示した．これまでに，より強い安全性モデルや，効率の改善，追加の特性，及び様々な仮定のもとで，様々な PKEET 方式が提案されている．

PKEET の自然な拡張として，平文一致確認可能属性ベース暗号 (Attribute-based Encryption with Equality Test; ABEET) が研究されてきた．ここで，述語 $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ の ABEET を簡単に説明する．$(\mathsf{mpk}, \mathsf{msk})$ をマスター公開鍵とマスター秘密鍵のペアとする．ct_i と ct_j をそれぞれ暗号文属性 x_i と x_j に対する平文 M_i と M_j の暗号文とする．標準的な属性ベース暗号 (Attribute-based Encryption; ABE) の場合と同様，鍵属性 y_i に対する秘密鍵 sk_{y_i} は $\mathsf{P}(x_i, y_i) = 1$ のとき，ct_i を復号可能である (sk_{y_j} を用いた ct_j の復号も同様)．td_{y_i} と td_{y_j} をそれぞれ秘密鍵 sk_{y_i} と sk_{y_j} で生成されるトラップドアとする．鍵属性 y_i のユーザは，鍵属性 y_j のトラップドア td_{y_j} を入手しても，$\mathsf{P}(x_j, y_i) = 0$ のとき暗号文属性 x_j の暗号文 ct_{x_j} を復号することはできない．一方，トラップドア td_{y_i} と td_{y_j} を持つユーザは，$\mathsf{P}(x_i, y_i) = \mathsf{P}(x_j, y_j) = 1$ が成立するとき，ct_{x_i} と ct_{x_j} が同じ平文の暗号化かどうか確認可能である．

最もシンプルな ABEET は等号述語 $\mathsf{P}_{\mathsf{IBE}} : \mathcal{V} \times \mathcal{V} \to \{0,1\}$，すなわち，$\mathsf{P}_{\mathsf{IBE}}(v, v') = 1 \Leftrightarrow v = v'$ を持つ平文一致確認可能属性ベース暗号 (Identity-based Encryption with Equality Test; IBEET) であり，これまでに [19], [27] などいくつかの IBEET 方式が提案されている．また，より複雑な単調スパンプログラムに対する ABEET 方式も提案されている [14], [15], [20], [23]．ただし，ABE では標準的仮定のもとで適応的安全性を満たす単調スパンプログラムに対する ABE 方式 [1], [7], [8], [12], [13] や，より複雑な非単調スパンプログラムに対する ABE 方式 [3], [21] が提案されている一方で，全ての ABEET 方式 [14], [15], [20], [23] は，単調スパンプログラムに対するもので，q タイプ仮定のもとで選択的安全性を満たす方式のみが提案されている．また，既存の ABEET 方式は全てペアリングを用いているが，Learning with Errors (LWE) 仮定に基づく ABE 方式も提案されている [9]．したがって，最新の ABE 構成手法に基づいて新たな ABEET 方式を構成することは重要な研究課題である．

1.2 本稿の貢献

本稿では IND-CPA 安全な委譲可能性を持つ ABE 方式 (以降，委譲可能 ABE 方式と呼ぶ)，ワンタイム署名方式，暗号学的ハッシュ関数を用いた CCA 安全な ABEET の一般的構成法を提案する．述語 $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ に対する ABEET を構成するために，提案構成では 1 階層目では述語 $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ を，その他の階層では等号述語 $\mathsf{P}_{\mathsf{IBE}} : \mathcal{V} \times \mathcal{V} \to \{0,1\}$ を持つ，3 階層の委譲可能 ABE を用いる．提案構成法を既存の委譲可能 ABE 方式と組み合わせることで，既存方式では達成されていない性質を持つ ABEET 方式を得ることができる．まず，Boneh らの委譲可能 ABE 方式 [9] を用いて，初めての LWE 仮定に基づく ABEET 方式を得る．さらに，Wee [24] と Attrapadung [7] によってそれぞれ提案された複雑な述語の ABE 方式を構成する枠組みである Predicate encoding や Pair encoding を用いることで，様々なペアリングベース方式を得る．[*1]

表 1 で，単調スパンプログラムを含めたいくつかの複雑な述語に対する CCA 安全な ABEET 方式の比較を示す．全ての方式は素数位数の双線形群を用いて構成されている．Pair encoding の枠組みでは膨大な数の ABE 方式が存在するため，Pair encoding と提案構成によって得られる全ての ABEET 方式が表 1 に網羅されていない可能性がある．しかし，表 1 に記載した 14 の方式は，提案構成の効力を明らかにするのには十分であると考えている．Predicate encoding 方式・Pair encoding 方式とそれを ABE 化するための構成法を基となる方式として記載する．例えば提案方式 1 は Wee の Predicate encoding 方式 [24] を Chen-Gay-Wee 構成法 [12] または Chen-Gong 構成法 [13] によって ABE 化することを示している．次に，単調スパンプログラムに対する既知の ABEET 方式 [14], [15], [20], [23] と比較して，我々の結果の様々な利点を説明する．

- 提案方式 4–6，9–12 は非単調スパンプログラムを，提案方式 13，14 は決定性有限オートマトンに対するものである．一方，既存方式は全て単調スパンプログラムに対するものである．
- 提案方式 1，2，4–8，10–14 は適応的安全性を，提案方式 3，9 は準適応的安全性を満たす．一方で，既存方式は全て選択的安全性のみを満たす．
- 提案方式 2–6，8–14 は large universe を扱うことができる．一方で既存の [20] を除いた全ての方式は small universe のみ扱うことができる．
- 提案方式 1–3，7–9 の安全性は標準的な k-linear 仮定に基づいている．一方で，既存の全ての方式の安全性は q タイプ仮定に基づいている．
- 提案方式 3，5，9，11 は暗号文が，提案方式 6，12 は秘密鍵が定数サイズである．一方で，既存方式は全て暗号文と秘密鍵が定数サイズではない．

したがって，提案構成法からいくつかの改良された ABEET 方式を得ることができた．ただし，表 1 に記載している提

[*1] これらの枠組みでは基本的に委譲可能性は議論されないが，Ambrona らの変換法 [6] によって所望の委譲可能性を付与することができる．

表 1 複雑な述語に対する CCA 安全な ABEET 方式の比較．MSP と NSP，DFA，CP，KP，ROM，BDHE はそれぞれ単調スパンプログラム，非単調スパンプログラム，決定性有限オートマトン，暗号文ポリシー，鍵ポリシー，ランダムオラクル，双線形 Diffie-Hellman Exponent を表す．

既存方式	述語	安全性	Policy	Universe	モデル	Complexity Assumption	特徴
CHH+18 [14]	MSP	選択的	CP	small	ROM	q-parallel BDHE	
CHH+19 [15]	MSP	選択的	CP	small	ROM	q-parallel BDHE	
WCH+20 [23]	MSP	選択的	CP	small	標準	q-parallel BDHE	
LSX+21 [20]	MSP	選択的	CP	large	標準	q-1	unbounded
提案方式 (基となる方式)	述語	安全性	Policy	Universe	モデル	Complexity Assumption	特徴
提案方式 1 ([12], [13], [24])	MSP	適応的	KP	small	標準	k-Lin	
提案方式 2 ([1], [7], [21])	MSP	適応的	KP	large	標準	k-Lin	
提案方式 3 ([1], [21])	MSP	準適応的	KP	large	標準	k-Lin	定数サイズ ct
提案方式 4 ([3], [8])	NSP	適応的	KP	large	標準	q-ratio	unbounded
提案方式 5 ([3], [8])	NSP	適応的	KP	large	標準	q-ratio	定数サイズ ct
提案方式 6 ([3], [8])	NSP	適応的	KP	large	標準	q-ratio	定数サイズ sk
提案方式 7 ([12], [13], [24])	MSP	適応的	CP	small	標準	k-Lin	
提案方式 8 ([1], [7], [21])	MSP	適応的	CP	large	標準	k-Lin	
提案方式 9 ([1], [21])	NSP	準適応的	CP	large	標準	k-Lin	定数サイズ ct
提案方式 10 ([3], [8])	NSP	適応的	CP	large	標準	q-ratio	unbounded
提案方式 11 ([3], [8])	NSP	適応的	CP	large	標準	q-ratio	定数サイズ ct
提案方式 12 ([3], [8])	NSP	適応的	CP	large	標準	q-ratio	定数サイズ sk
提案方式 13 ([3], [7])	DFA	適応的	KP	large	標準	q-ratio	unbounded
提案方式 14 ([3], [7])	DFA	適応的	CP	large	標準	q-ratio	unbounded

案方式は，提案構成法から得られる方式の一部に過ぎないことに注意されたい．

1.3 技術的概要

提案構成の概要を説明する．まず，既存の ABEET 方式に共通する構造を利用し，述語 $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ に対する任意の IND-CPA 安全な ABE 方式を暗号学的ハッシュ関数と組み合わせることで，同じ述語に対する CPA 安全な ABEET 方式になることを簡単にまとめる．まず，述語 P に対する ABE 方式を 2 つ並列に用い，$\mathsf{ABE.mpk}_0$ と $\mathsf{ABE.mpk}_1$ を 2 つの ABE 方式のマスター公開鍵，H を暗号学的ハッシュ関数とする．そして，$\mathsf{mpk} = (\mathsf{ABE.mpk}_0, \mathsf{ABE.mpk}_1, \mathsf{H})$ を ABEET 方式のマスター公開鍵とする．平文 M の暗号文属性 $x \in \mathcal{X}$ に対する暗号文を $\mathsf{ct}_x = (\mathsf{ABE.ct}_{x,0}, \mathsf{ABE.ct}_{x,1})$ とする．ただし，$\mathsf{ABE.ct}_{x,0}$ と $\mathsf{ABE.ct}_{x,1}$ はそれぞれ $\mathsf{ABE.mpk}_0$ と $\mathsf{ABE.mpk}_1$ による x に対する M と $\mathsf{H}(\mathsf{M})$ の暗号文である．鍵属性 $y \in \mathcal{Y}$ に対する秘密鍵を $\mathsf{sk}_y = (\mathsf{ABE.sk}_{y,0}, \mathsf{ABE.sk}_{y,1})$ とする．ただし，$\mathsf{ABE.sk}_{y,0}$ と $\mathsf{ABE.sk}_{y,1}$ はそれぞれ $(\mathsf{ABE.mpk}_0, \mathsf{ABE.msk}_0)$ と $(\mathsf{ABE.mpk}_1, \mathsf{ABE.msk}_1)$ を用いて計算された y に対する秘密鍵である．$\mathsf{P}(x,y) = 1$ のとき，$\mathsf{ABE.sk}_{y,0}$ で $\mathsf{ABE.ct}_{x,0}$ を復号して M を得られるので，秘密鍵 sk_y で暗号文 ct_x を復号できる．$y \in \mathcal{Y}$ に対するトラップドアを $\mathsf{td}_y = \mathsf{ABE.sk}_{y,1}$ とすると，$(x,x') \in \mathcal{X}^2$ の 2 つの暗号文 $(\mathsf{ct}_x, \mathsf{ct}_{x'})$ と $\mathsf{P}(x,y) = \mathsf{P}(x',y') = 1$ となる 2 つのトラップドア $(\mathsf{td}_y, \mathsf{td}_{y'})$ が与えられたとき，トラップドア $\mathsf{ABE.sk}_{y,1}$ と $\mathsf{ABE.sk}_{y',1}$ を用いてそれぞれ $\mathsf{ABE.ct}_{x,1}$ と $\mathsf{ABE.ct}_{x',1}$ を復号することで，同じ平文の暗号化かどうか確認できる．

次に，上記の ABEET 方式が CPA 安全性を満たすことを確認する．詳細は省略するが，ABEET はタイプ I 攻撃者とタイプ II 攻撃者と呼ばれる 2 つのタイプの攻撃者に対して安全でなければならない．x^* をチャレンジ暗号文属性とするとき，タイプ I 攻撃者は $\mathsf{P}(x^*,y) = 1$ となるトラップドア td_y を得ることができるが，タイプ II 攻撃者は得ることができない．タイプ I 攻撃者は定義より識別不可能性を破ることができるため，一方向性を証明する．した

がって，チャレンジ暗号文 $\mathsf{ct}^*_{x^*} = (\mathsf{ABE.ct}^*_{x^*,0}, \mathsf{ABE.ct}^*_{x^*,1})$ はチャレンジャーによって選ばれた M^* の暗号文である．ここで，ABE 方式の IND-CPA 安全性より，チャレンジ暗号文の $\mathsf{ABE.ct}^*_{x^*,0}$ は M^* の情報を漏らさない．また，タイプ I 攻撃者は $\mathsf{P}(x^*, y) = 1$ となるトラップドアを持つため $\mathsf{H}(\mathsf{M}^*)$ を得られるが，ハッシュ関数 H の一方向性より M^* を求められない．よって，タイプ I 攻撃者に対して一方向性が成立する．これに対し，タイプ II 攻撃者については識別不可能性を証明する．したがって，チャレンジ暗号文 $\mathsf{ct}^*_{x^*}$ は攻撃者が $(\mathsf{M}^*_0, \mathsf{M}^*_1)$ をチャレンジャーに送り，チャレンジャーが $\mathsf{coin}^* \leftarrow_\$ \{0,1\}$ を選んだ $\mathsf{M}^*_{\mathsf{coin}^*}$ の暗号文である．このとき，ABE 方式の IND-CPA 安全性より，$\mathsf{ABE.ct}^*_{x^*,0}$ と $\mathsf{ABE.ct}^*_{x^*,1}$ から coin^* の識別ができない．ただし上記の構成では，ABE 方式が IND-CCA 安全であっても CCA 安全な ABEET 方式は得られない．実際，タイプ II 攻撃者がチャレンジ暗号文 $\mathsf{ct}^*_{x^*} = (\mathsf{ABE.ct}^*_{x^*,0}, \mathsf{ABE.ct}^*_{x^*,1})$ を受け取ったとき，攻撃者自身で $\mathsf{H}(\mathsf{M}^*_0)$ または $\mathsf{H}(\mathsf{M}^*_1)$ の暗号文 $\mathsf{ABE.ct}_{x^*,1}$ を計算し，復号クエリ $(\mathsf{ABE.ct}^*_{x^*,0}, \mathsf{ABE.ct}_{x^*,1})$ を行うことで coin^* を推測できる．

上記構成の問題点を解決し，CCA 安全な ABEET を構成するために，我々は Lee らが提案した 3 階層の階層型 ID ベース暗号を用いた CCA 安全な IBEET の一般的構成 [19] を属性ベースの場合に拡張する．Lee らは CHK 変換 [11] を用いて，上記構成に類似の IBEET 方式の CCA 安全性を証明した．同様に，我々は CHK 変換を ABE の場合に拡張した Yamada らの変換 [25] を用いて CCA 安全性を達成する．そのために，我々は 3 階層の委譲可能 ABE 方式を用いる．具体的には，述語 $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ に対する ABEET を構成するために，$(x, b, v) \in \mathcal{X} \times \{0,1\} \times \mathcal{V}$ に紐づく暗号文 $\mathsf{ABE.ct}_{x,b,v}$ と $(y, b', v') \in \mathcal{Y} \times \{0,1\} \times \mathcal{V}$ に紐づく秘密鍵 $\mathsf{ABE.sk}_{y,b',v'}$ を持ち，$\mathsf{P}(x, y) = 1$ かつ $b = b'$ かつ $v = v'$ のときに復号可能な委譲可能 ABE 方式を用いる．ここで，2 階層目 $b, b' \in \{0,1\}$ は上記の CPA 安全な構成においてどちらの ABE 方式であるかを，3 階層目 $v, v' \in \mathcal{V}$ はワンタイム署名方式の検証鍵を指定するために用いている．最終的に，ABEET のマスター公開鍵を $\mathsf{mpk} = \mathsf{ABE.mpk}$, $x \in \mathcal{X}$ に対する暗号文を $\mathsf{ct}_x = (\mathsf{ABE.ct}_{x,0,\mathsf{verk}}, \mathsf{ABE.ct}_{x,1,\mathsf{verk}}, \sigma)$, $y \in \mathcal{Y}$ に対する秘密鍵とトラップドアをそれぞれ $\mathsf{sk}_y = \mathsf{ABE.sk}_y$, $\mathsf{td}_y = \mathsf{ABE.sk}_{y,1}$ とする．ただし，verk はワンタイム署名方式の検証鍵，σ は $[\mathsf{ABE.ct}_{x,0,\mathsf{verk}} \| \mathsf{ABE.ct}_{x,1,\mathsf{verk}}]$ の署名である．直感的には，上記の CPA 安全な ABEET の構成と Yamada らによる ABE の CCA 安全性証明 [25] を組み合わせることで，この ABEET 方式の CCA 安全性を証明できる．

2. 準備

記法． λ は安全性パラメータを表す．i ビット文字列 $s_1 \in \{0,1\}^i$ と j ビット文字列 $s_2 \in \{0,1\}^j$ に対し，$[s_1 \| s_2] \in \{0,1\}^{i+j}$ は s_1 と s_2 を連結した $i + j$ ビットの文字列を表す．有限集合 S に対して，S から一様ランダムに要素 s を取り出すことを $s \leftarrow_\$ S$ と表記し，$|S|$ を S の要素数とする．確率的多項式時間を PPT と書く．

2.1 平文一致確認可能属性ベース暗号

モデル． $\mathcal{X}$ と $\mathcal{Y}$ をそれぞれ暗号文と秘密鍵の属性空間とし，$\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ を述語とする．述語 $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ に対する ABEET 方式 II は以下の 6 つのアルゴリズム (Setup, Enc, KeyGen, Dec, Trapdoor, Test) からなる：

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$：安全性パラメータ λ を入力に取り，マスター公開鍵 mpk とマスター秘密鍵 msk を出力する．mpk には安全性パラメータのみから定まる平文空間 $\mathcal{M}$ が含まれる．
- $\mathsf{Enc}(\mathsf{mpk}, x, \mathsf{M}) \to \mathsf{ct}_x$：mpk と $x \in \mathcal{X}$, 平文 $\mathsf{M} \in \mathcal{M}$ を入力に取り，暗号文 ct_x を出力する．
- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y) \to \mathsf{sk}_y$：mpk と msk, $y \in \mathcal{Y}$ を入力に取り，秘密鍵 sk_y を出力する．
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x) \to \mathsf{M}$ or $\perp$：mpk と sk_y, ct_x を入力に取り，$\mathsf{P}(x, y) = 1$ であるとき復号結果 M を，そうでないとき $\perp$ を出力する．
- $\mathsf{Trapdoor}(\mathsf{mpk}, \mathsf{sk}_y) \to \mathsf{td}_y$：mpk と sk_y を入力に取り，トラップドア td_y を出力する．
- $\mathsf{Test}(\mathsf{mpk}, \mathsf{td}_{y_0}, \mathsf{ct}_{x_0}, \mathsf{td}_{y_1}, \mathsf{ct}_{x_1}) \to 1$ or 0：mpk, td_{y_0} と td_{y_1}, ct_{x_0} と ct_{x_1} を入力に取り，1 または 0 を出力する．

正当性． 全ての $\lambda \in \mathbb{N}$, $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ に対し，以下に定義される 3 つの条件を満たす必要がある．

(1) 全ての $\mathsf{M} \in \mathcal{M}$, $\mathsf{P}(x, y) = 1$ となる $(x, y) \in \mathcal{X} \times \mathcal{Y}$ に対して，$\mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, \mathsf{M})$, $\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$, $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x) = \mathsf{M}$ が圧倒的な確率で成立する．

(2) 全ての $\mathsf{M} \in \mathcal{M}$, $\mathsf{P}(x_0, y_0) = \mathsf{P}(x_1, y_1) = 1$ を満たす $(x_0, x_1, y_0, y_1) \in \mathcal{X}^2 \times \mathcal{Y}^2$ に対して，$1 \leftarrow \mathsf{Test}(\mathsf{mpk}, \mathsf{td}_{y_0}, \mathsf{ct}_{x_0}, \mathsf{td}_{y_1}, \mathsf{ct}_{x_1})$ が圧倒的な確率で成立する．ここで，$i = 0, 1$ について，$\mathsf{sk}_{y_i} \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y_i)$, $\mathsf{ct}_{x_i} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x_i, \mathsf{M})$, $\mathsf{td}_{y_i} \leftarrow \mathsf{Trapdoor}(\mathsf{mpk}, \mathsf{sk}_{y_i})$ とする．

(3) 全ての $\mathsf{P}(x_0, y_0) = \mathsf{P}(x_1, y_1) = 1$ を満たす $(x_0, x_1, y_0, y_1) \in \mathcal{X}^2 \times \mathcal{Y}^2$, mpk と msk を入力に取り $(\mathsf{M}_0, \mathsf{M}_1)$ を出力する任意の PPT 攻撃者 $\mathcal{A}$ に対して，$\mathsf{M}_0 \neq \mathsf{M}_1$ かつ $1 \leftarrow \mathsf{Test}(\mathsf{mpk}, \mathsf{td}_{y_0}, \mathsf{ct}_{x_0}, \mathsf{td}_{y_1}, \mathsf{ct}_{x_1})$ が成立する確率が無視可能である．ここで，$i = 0, 1$ について，$\mathsf{sk}_{y_i} \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y_i)$, $\mathsf{ct}_{x_i} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x_i, \mathsf{M})$, $\mathsf{td}_{y_i} \leftarrow \mathsf{Trapdoor}(\mathsf{mpk}, \mathsf{sk}_{y_i})$ とする．

安全性． ABEET の安全性に関して，ターゲット属性 x^* に対して $\mathsf{P}(x^*, y) = 1$ となる属性 y のトラップドア td_y を

持っているタイプ I 攻撃者と，持っていないタイプ II 攻撃者を考える．チャレンジ暗号文を $\mathsf{ct}^*_{x^*}$ とする．タイプ I 攻撃者は td_y を持っており，ct_{x^*} に対して平文一致確認を行うことができるため一方向性を考える．タイプ II 攻撃者は td_y を持っておらず，ct_{x^*} に対して平文一致確認を行うことができないため識別不可能性を考える．

定義 2.1 (タイプ I 攻撃者に対する適応的 OW-CCA2 安全性)．タイプ I 攻撃者に対する ABEET の適応的 OW-CCA2 安全性は，攻撃者 $\mathcal{A}$ とチャレンジャー $\mathcal{C}$ による以下のゲームによって定義される．

Init：$\mathcal{C}$ は $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ を実行し，mpk を $\mathcal{A}$ に送る．

Phase 1：$\mathcal{A}$ は適応的に以下の 3 つのクエリを $\mathcal{C}$ に行う：

秘密鍵生成クエリ：$\mathcal{A}$ のクエリ $y \in \mathcal{Y}$ に対して，$\mathcal{C}$ は $\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$ を実行し，sk_y を $\mathcal{A}$ に送る．

復号クエリ：$\mathcal{A}$ のクエリ (y, ct_x) に対して，$\mathcal{C}$ は $\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$ を実行し，$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x)$ を $\mathcal{A}$ に送る．

トラップドア生成クエリ：$\mathcal{A}$ のクエリ y に対して，$\mathcal{C}$ は $\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$ と $\mathsf{td}_y \leftarrow \mathsf{Trapdoor}(\mathsf{mpk}, \mathsf{sk}_y)$ を実行し，td_y を $\mathcal{C}$ に送る．

チャレンジクエリ：$\mathcal{A}$ は 1 回だけこのクエリを行う．$\mathcal{A}$ からクエリ x^* を受け取り，$\mathcal{C}$ は $\mathsf{M}^* \leftarrow_\$ \mathcal{M}$ を選び，$\mathsf{ct}^*_{x^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*, \mathsf{M}^*)$ を実行し，$\mathsf{ct}^*_{x^*}$ を $\mathcal{A}$ に送る．ただし，秘密鍵生成クエリが行われた全ての $y \in \mathcal{Y}$ に対して，$\mathsf{P}(x^*, y) = 0$ が成り立つとする．

Phase 2：$\mathcal{A}$ は Phase 1 と同じ 3 つのクエリを適応的に行うことができるが，秘密鍵生成クエリと復号クエリの際にそれぞれ $\mathsf{P}(x^*, y) \neq 1$ と $\mathsf{ct}_x \neq \mathsf{ct}^*_{x^*}$ が成り立つことを確認し，そうでなければ $\perp$ を出力する．

Guess：$\mathcal{A}$ は M^* の推測値として $\widehat{\mathsf{M}}$ を出力する．

攻撃者 $\mathcal{A}$ は $\widehat{\mathsf{M}} = \mathsf{M}^*$ のときゲームに勝利するとし，そのときの優位性は以下のように定義される．

$$\mathsf{Adv}^{\mathsf{OW\text{-}CCA2}}_{\Sigma,\mathcal{A}}(\lambda) \coloneqq \left| \Pr\left[\widehat{\mathsf{M}} = \mathsf{M}^*\right] - \frac{1}{|\mathcal{M}|} \right|.$$

ABEET 方式 Σ において，任意の PPT 攻撃者 $\mathcal{A}$ に対し，$\mathsf{Adv}^{\mathsf{OW\text{-}CCA2}}_{\Sigma,\mathcal{A}}(\lambda)$ が λ に関して無視可能であるとき，タイプ I 攻撃者に対する適応的 OW-CCA2 安全性を満たすという．

定義 2.2 (タイプ II 攻撃者に対する適応的 IND-CCA2 安全性)．タイプ II 攻撃者に対する ABEET の適応的 IND-CCA2 安全性は，攻撃者 $\mathcal{A}$ とチャレンジャー $\mathcal{C}$ による以下のゲームによって定義される．定義 2.1 の OW-CCA2 ゲームからの変更点のみを以下に示す．

チャレンジクエリ：$\mathcal{A}$ は 1 回だけクエリを行う．$\mathcal{A}$ からクエリ $(x^*, \mathsf{M}^*_0, \mathsf{M}^*_1) \in \mathcal{Y} \times \mathcal{M}^2$ (ただし，$|\mathsf{M}^*_0| = |\mathsf{M}^*_1|$) を受け取り，$\mathcal{C}$ は $\mathsf{coin}^* \leftarrow_\$ \{0,1\}$ を選び，$\mathsf{ct}^*_{x^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*, \mathsf{M}^*_{\mathsf{coin}^*})$ を実行し，$\mathsf{ct}^*_{x^*}$ を $\mathcal{A}$ に送る．ただし，秘密鍵生成クエリとトラップドア生成クエリが行われた全ての $y \in \mathcal{Y}$ に対して，$\mathsf{P}(x^*, y) = 0$ が成り立つとする．

Phase 2：$\mathcal{A}$ は Phase 1 と同じクエリを適応的に行えるが，トラップドア生成クエリの際に $\mathsf{P}(x^*, y) \neq 1$ が成り立つことを確認し，そうでなければ $\perp$ を出力する．

Guess：$\mathcal{A}$ は coin^* の推測値として $\widehat{\mathsf{coin}}$ を出力する．

攻撃者 $\mathcal{A}$ は $\widehat{\mathsf{coin}} = \mathsf{coin}^*$ のときゲームに勝利するとし，そのときの優位性は以下のように定義される．

$$\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Sigma,\mathcal{A}}(\lambda) \coloneqq \left| \Pr\left[\widehat{\mathsf{coin}} = \mathsf{coin}^*\right] - \frac{1}{2} \right|.$$

ABEET 方式 Σ において，任意の PPT 攻撃者 $\mathcal{A}$ に対し，$\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Sigma,\mathcal{A}}(\lambda)$ が λ に関して無視可能であるとき，タイプ II 攻撃者に対する適応的 IND-CCA2 安全性を満たすという．

2.2 委譲可能性を持つ属性ベース暗号

議論を簡潔にするため，本論文では ABEET の提案構成を説明するのに十分な 3 階層構造を持つ特殊な委譲可能 ABE を定義する．本稿で用いる述語 $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ に対する委譲可能 ABE は，1 階層目のみがこの述語 P に対応し，2 階層目と 3 階層目は IBE と同様の等号述語のみを扱う．さらに，2 階層目と 3 階層目はそれぞれ $\{0,1\}$ と識別子空間 $\mathcal{V}$ の要素を取る．そのため，暗号文 $\mathsf{ABE.ct}_{x,b,v}$ と秘密鍵 $\mathsf{ABE.sk}_{y,b',v'}$ はそれぞれ $(x,b,v) \in \mathcal{X} \times \{0,1\} \times \mathcal{V}$ と $(y,b',v') \in \mathcal{Y} \times \{0,1\} \times \mathcal{V}$ に紐づいており，$\mathsf{P}(x,y) = 1$ かつ $b = b'$ かつ $v = v'$ を満たすとき秘密鍵 $\mathsf{ABE.sk}_{y,b',v'}$ で暗号文 $\mathsf{ABE.ct}_{x,b,v}$ を復号できる．ただし，委譲可能性により，秘密鍵 $\mathsf{ABE.sk}_y$ や $\mathsf{ABE.sk}_{y,b'}$ を用いて秘密鍵 $\mathsf{ABE.sk}_{y,b',v'}$ を計算可能である．

シンタックス． 一般的な ABE の定義と同様，述語 P に対する委譲可能 ABE 方式 Π は以下の 5 つのアルゴリズム ($\mathsf{ABE.Setup}$, $\mathsf{ABE.Enc}$, $\mathsf{ABE.KeyGen}$, $\mathsf{ABE.Delegate}$) からなるが，ABEET の提案構成を説明するのに十分であるため，$\mathsf{ABE.Enc}$ アルゴリズムは常に $(x,b,v) \in \mathcal{X} \times \{0,1\} \times \mathcal{V}$ を入力に取り，暗号文 $\mathsf{ABE.ct}_{x,b,v}$ を出力し，$\mathsf{ABE.ct}_x$ や $\mathsf{ABE.ct}_{x,b}$ という暗号文は考えないことに注意されたい．

$\mathsf{ABE.Setup}(1^\lambda) \to (\mathsf{ABE.mpk}, \mathsf{ABE.msk})$：安全性パラメータ λ を入力に取り，マスター公開鍵 $\mathsf{ABE.mpk}$ とマスター秘密鍵 $\mathsf{ABE.msk}$ を出力する．$\mathsf{ABE.mpk}$ には安全性パラメータのみから定まる平文空間 $\mathcal{M}$ が含まれる．

$\mathsf{ABE.Enc}(\mathsf{ABE.mpk}, (x,b,v), \mathsf{M}) \to \mathsf{ABE.ct}_{x,b,v}$：$\mathsf{ABE.mpk}$ と $(x,b,v) \in \mathcal{X} \times \{0,1\} \times \mathcal{V}$, $\mathsf{M} \in \mathcal{M}$ を入力に取り，暗号文 $\mathsf{ABE.ct}_{x,b,v}$ を出力する．

$\mathsf{ABE.KeyGen}(\mathsf{ABE.mpk}, \mathsf{ABE.msk}, Y) \to \mathsf{ABE.sk}_Y$：$\mathsf{ABE.mpk}$ と Y を入力に取り，秘密鍵 $\mathsf{ABE.sk}_Y$ を出力

する．ただし，Y は $\mathcal{Y}$ または $\mathcal{Y}\times\{0,1\}$, $\mathcal{Y}\times\{0,1\}\times\mathcal{V}$ の要素とする．

$\mathsf{ABE.Dec}(\mathsf{ABE.mpk}, \mathsf{ABE.ct}_{x,b,v}, \mathsf{ABE.sk}_{y,b',v'}) \to \mathsf{M}$ or $\perp$：$\mathsf{ABE.mpk}$ と $\mathsf{ABE.ct}_{x,b,v}$, $\mathsf{ABE.sk}_{y,b',v'}$ を入力に取り，$\mathsf{P}(x,y)=1$ かつ $(b,v)=(b',v')$ であるとき復号結果 M を，そうでないとき $\perp$ を出力する．

$\mathsf{ABE.Delegate}(\mathsf{ABE.mpk}, \mathsf{ABE.sk}_Y, Y') \to \mathsf{ABE.sk}_{Y'}$：$\mathsf{ABE.mpk}$ と $\mathsf{ABE.sk}_Y$, Y' を入力に取り，$\mathsf{ABE.sk}_{Y'}$ を出力する．ただし，Y は $\mathcal{Y}$ または $\mathcal{Y}\times\{0,1\}$ の要素で，Y' は $Y\in\mathcal{Y}$ のとき $\{Y\}\times\{0,1\}$ または $\{Y\}\times\{0,1\}\times\mathcal{V}$ の要素で，$Y\in\mathcal{Y}\times\{0,1\}$ のとき $\{Y\}\times\{0,1\}\times\mathcal{V}$ の要素とする．

正当性．全ての $\lambda\in\mathbb{N}$, $(\mathsf{ABE.mpk}, \mathsf{ABE.msk}) \leftarrow \mathsf{ABE.Setup}(1^\lambda)$, $\mathsf{M}\in\mathcal{M}$, $\mathsf{P}(x,y)=1$ となる $(x,y)\in\mathcal{X}\times\mathcal{Y}$, $(b,v)\in\{0,1\}\times\mathcal{V}$ に対して，$\mathsf{ABE.sk}_{y,b,v} \leftarrow \mathsf{ABE.KeyGen}(\mathsf{ABE.mpk}, \mathsf{ABE.msk}, (y,b,v))$, $\mathsf{ABE.ct}_{x,b,v} \leftarrow \mathsf{ABE.Enc}(\mathsf{ABE.mpk}, (x,b,v), \mathsf{M})$, $\mathsf{ABE.Dec}(\mathsf{ABE.mpk}, \mathsf{ABE.ct}_{x,b,v}, \mathsf{ABE.sk}_{y,b,v}) = \mathsf{M}$ が圧倒的な確率で成立する．また，$\mathsf{ABE.KeyGen}(\mathsf{ABE.mpk}, \mathsf{ABE.msk}, Y')$ と $\mathsf{ABE.Delegate}(\mathsf{ABE.mpk}, \mathsf{ABE.KeyGen}(\mathsf{ABE.mpk}, \mathsf{ABE.msk}, Y), Y')$ の出力が同一の分布となる．

安全性．本論文で扱う委譲可能 ABE の IND-CPA 安全性は，一般的な ABE の IND-CPA 安全性と同様のため詳細は省略する．直感的には，PPT 攻撃者 $\mathcal{A}$ は自分の選んだ $((x^*,b^*,v^*), \mathsf{M}_0^*, \mathsf{M}_1^*)\in\mathcal{X}\times\{0,1\}\times\mathcal{V}\times\mathcal{M}^2$ に対して，$\mathsf{coin}^* \leftarrow_\$ \{0,1\}$ となるチャレンジ暗号文 $\mathsf{ABE.ct}^*_{x^*,b^*,v^*} \leftarrow \mathsf{ABE.Enc}(\mathsf{ABE.mpk}, (x^*,b^*,v^*), \mathsf{M}^*_{\mathsf{coin}^*})$ とチャレンジ暗号文を自明には復号できない秘密鍵 $\mathsf{ABE.sk}_{y,b,v}$ を受け取っても coin^* を識別できない．

2.3 ワンタイム署名

シンタックス．ワンタイム署名（OTS）方式 Γ は 3 つのアルゴリズム (Sig.Setup, Sig.Sign, Sig.Vrfy) からなる．Sig.Setup アルゴリズムは安全性パラメータを入力に取り，検証鍵と署名鍵のペアを出力する．Sig.Sign アルゴリズムは署名鍵を用いて，任意長の平文に対する署名を生成する．Sig.Vrfy アルゴリズムは平文と対応する署名に対し，検証鍵を用いて受理を表す 1 または却下を表す 0 を出力する．

安全性．本論文で扱う OTS の強偽造不可能性は，一般的な OTS の強偽造不可能性と同様のため詳細は省略する．直感的には，PPT 攻撃者 $\mathcal{A}$ は自分の選んだ $\mathsf{M}^*\in\{0,1\}^*$ に対して，$\sigma^* \leftarrow \mathsf{Sig.Sign}(\mathsf{sigk}, \mathsf{M}^*)$ と検証鍵 verk を受け取っても，verk で受理可能な平文と署名のペア $(\widehat{\mathsf{M}}, \widehat{\sigma})$ $(\neq(\mathsf{M}^*, \sigma^*))$ を偽造できない．

2.4 ハッシュ関数

$\mathsf{H}: \mathcal{M}\to\mathcal{M}$ をハッシュ関数とする．本論文で扱うハッシュ関数の一方向性と衝突困難性は，一般的なハッシュ関数のものと同様のため詳細は省略する．直感的に一方向性は，PPT 攻撃者 $\mathcal{A}$ は $\mathsf{M}^* \leftarrow_\$ \mathcal{M}$ のハッシュ値 $\mathsf{H}(\mathsf{M}^*)$ を受け取っても，$\mathsf{H}(\mathsf{M}^*)=\mathsf{H}(\widehat{\mathsf{M}})$ となる $\widehat{\mathsf{M}}\in\mathcal{M}$ を計算できない．また，衝突困難性は，PPT 攻撃者 $\mathcal{A}$ は $\mathsf{H}(\mathsf{M}_0)=\mathsf{H}(\mathsf{M}_1)$ を満たす異なる $(\mathsf{M}_0,\mathsf{M}_1)\in\mathcal{M}^2$ を見つけられない．

3. 提案手法

本節では，ABEET の一般的構成法を提案する．まず，3.1 節で構成を示し，3.2 節で正当性を証明する．

3.1 構成

委譲可能 ABE 方式 Π，OTS 方式 Γ，ハッシュ関数 H を用いて，述語 P に対する ABEET を以下のように構成する．

$\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$：$(\mathsf{ABE.mpk}, \mathsf{ABE.msk}) \leftarrow \mathsf{ABE.Setup}(1^\lambda)$ を実行し，OTS 方式 Γ とハッシュ関数 H を選び，$\mathsf{mpk} \coloneqq (\mathsf{ABE.mpk}, \Gamma, \mathsf{H})$ と $\mathsf{msk} \coloneqq \mathsf{ABE.msk}$ を出力する．

$\mathsf{Enc}(\mathsf{mpk}, x, \mathsf{M}) \to \mathsf{ct}_x$：以下を実行する．

- $(\mathsf{verk}, \mathsf{sigk}) \leftarrow \mathsf{Sig.Setup}(1^\lambda)$,
- $\mathsf{ABE.ct}_{x,0,\mathsf{verk}} \leftarrow \mathsf{ABE.Enc}(\mathsf{ABE.mpk}, (x,0,\mathsf{verk}), \mathsf{M})$,
- $\mathsf{ABE.ct}_{x,1,\mathsf{verk}} \leftarrow \mathsf{ABE.Enc}(\mathsf{ABE.mpk}, (x,1,\mathsf{verk}), \mathsf{H}(\mathsf{M}))$,
- $\sigma \leftarrow \mathsf{Sig.Sign}(\mathsf{sigk}, [\mathsf{ABE.ct}_{x,0,\mathsf{verk}} \| \mathsf{ABE.ct}_{x,1,\mathsf{verk}}])$.

最後に，$\mathsf{ct}_x \coloneqq (\mathsf{verk}, \mathsf{ABE.ct}_{x,0,\mathsf{verk}}, \mathsf{ABE.ct}_{x,1,\mathsf{verk}}, \sigma)$ を出力する．

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y) \to \mathsf{sk}_y$：$\mathsf{ABE.sk}_y \leftarrow \mathsf{ABE.KeyGen}(\mathsf{ABE.mpk}, \mathsf{ABE.msk}, y)$ を実行し，$\mathsf{sk}_y \coloneqq \mathsf{ABE.sk}_y$ を出力する．

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x) \to \mathsf{M}$ or $\perp$：$\mathsf{ct}_x \coloneqq (\mathsf{verk}, \mathsf{ABE.ct}_{x,0,\mathsf{verk}}, \mathsf{ABE.ct}_{x,1,\mathsf{verk}}, \sigma)$ とし，

- $\mathsf{Sig.Vrfy}(\mathsf{verk}, [\mathsf{ABE.ct}_{x,0,\mathsf{verk}} \| \mathsf{ABE.ct}_{x,1,\mathsf{verk}}], \sigma) \to 0$,
- $\mathsf{P}(x,y)=0$,

のいずれかを満たすとき $\perp$ を出力する．そうでないとき，以下を実行する．

- $\mathsf{ABE.sk}_{y,0,\mathsf{verk}} \leftarrow \mathsf{ABE.Delegate}(\mathsf{ABE.mpk}, \mathsf{ABE.sk}_y, (y,0,\mathsf{verk}))$,
- $\mathsf{ABE.sk}_{y,1,\mathsf{verk}} \leftarrow \mathsf{ABE.Delegate}(\mathsf{ABE.mpk}, \mathsf{ABE.sk}_y, (y,1,\mathsf{verk}))$,
- $\mathsf{M} \leftarrow \mathsf{ABE.Dec}(\mathsf{ABE.mpk}, \mathsf{ABE.sk}_{y,0,\mathsf{verk}}, \mathsf{ABE.ct}_{x,0,\mathsf{verk}})$,
- $h \leftarrow \mathsf{ABE.Dec}(\mathsf{ABE.mpk}, \mathsf{ABE.sk}_{y,1,\mathsf{verk}}, \mathsf{ABE.ct}_{x,1,\mathsf{verk}})$.

最後に，$\mathsf{H}(\mathsf{M})=h$ ならば M を，そうでないとき $\perp$ を出力する．

$\mathsf{Trapdoor}(\mathsf{mpk}, \mathsf{sk}_y) \to \mathsf{td}_y$：$\mathsf{ABE.sk}_{y,1} \leftarrow \mathsf{ABE.Delegate}(\mathsf{ABE.mpk}, \mathsf{ABE.sk}_y, (y,1))$ を実行し，$\mathsf{td}_y \coloneqq \mathsf{ABE.sk}_{y,1}$ を出力する．

$\mathsf{Test}(\mathsf{mpk}, \mathsf{td}_y, \mathsf{ct}_x, \mathsf{td}_{y'}, \mathsf{ct}_{x'}) \to 1$ or $0 : \mathsf{td}_y = \mathsf{ABE.sk}_{y,1}$, $\mathsf{ct}_x = (\mathsf{verk}, \mathsf{ABE.ct}_{x,0,\mathsf{verk}}, \mathsf{ABE.ct}_{x,1,\mathsf{verk}}, \sigma)$, $\mathsf{td}_{y'} = \mathsf{ABE.sk}_{y,1}$, $\mathsf{ct}_{x'} = (\mathsf{verk}', \mathsf{ABE.ct}_{x',0,\mathsf{verk}'}, \mathsf{ABE.ct}_{x',1,\mathsf{verk}'}, \sigma')$ とし，

- $\mathsf{Sig.Vrfy}(\mathsf{verk}, [\mathsf{ABE.ct}_{x,0,\mathsf{verk}} \| \mathsf{ABE.ct}_{x,1,\mathsf{verk}}], \sigma) \to 0$,
- $\mathsf{Sig.Vrfy}(\mathsf{verk}', [\mathsf{ABE.ct}_{x',0,\mathsf{verk}'} \| \mathsf{ABE.ct}_{x',1,\mathsf{verk}'}], \sigma') \to 0$,

のいずれかを満たすとき 0 を出力する．そうでないとき，以下を実行する．

- $\mathsf{ABE.sk}_{y,1,\mathsf{verk}} \leftarrow \mathsf{ABE.Delegate}(\mathsf{ABE.mpk}, \mathsf{ABE.sk}_{y,1}, (y, 1, \mathsf{verk}))$,
- $\mathsf{ABE.sk}_{y',1,\mathsf{verk}'} \leftarrow \mathsf{ABE.Delegate}(\mathsf{ABE.mpk}, \mathsf{ABE.sk}_{y',1}, (y', 1, \mathsf{verk}'))$,
- $h \leftarrow \mathsf{ABE.Dec}(\mathsf{ABE.mpk}, \mathsf{ABE.ct}_{x,1,\mathsf{verk}}, \mathsf{ABE.sk}_{y,1,\mathsf{verk}})$,
- $h' \leftarrow \mathsf{ABE.Dec}(\mathsf{ABE.mpk}, \mathsf{ABE.ct}_{x',1,\mathsf{verk}'}, \mathsf{ABE.sk}_{y',1,\mathsf{verk}'})$.

最後に，$h = h'$ のとき 1 を，そうでないとき 0 を出力する．

3.2 正当性

定理 3.1. 提案方式の構成に用いる委譲可能 ABE 方式 Π, OTS 方式 Γ が正当性を，ハッシュ関数 H が衝突困難性を満たすのであれば，提案方式は正当性を満たす．

紙面の都合で，定理 3.1 の証明の概要のみを示す．委譲可能 ABE 方式 Π と OTS 方式 Γ が正当ならば，Dec アルゴリズム実行の際に Sig.Vrfy アルゴリズムは 1 を出力し，ABE.Dec アルゴリズムは $\mathsf{H}(\mathsf{M}) = h$ を満たす M と h を出力するので，正当性 (1) が成り立つ．同様に，委譲可能 ABE 方式 Π と OTS 方式 Γ が正当ならば，Test アルゴリズム実行の際に Sig.Vrfy アルゴリズムは 1 を出力し，ABE.Dec アルゴリズムは $h = h'$ を満たす h と h' を出力するので，正当性 (2) が成り立つ．また，委譲可能 ABE 方式 Π が正当ならば，正当性 (3) が成り立つためには PPT 攻撃者 $\mathcal{A}$ は $\mathsf{H}(\mathsf{M}_0) = \mathsf{H}(\mathsf{M}_1)$ を満たす異なる $\mathsf{M}_0, \mathsf{M}_1$ を見つけなければならないので，ハッシュ関数 H が衝突困難ならば正当性 (3) が成り立つ．よって，提案 ABEET 方式は正当である．

4. 安全性

本節では，3.1 節の提案構成の安全性を証明する．提案構成が，タイプ I 攻撃者に対する適応的 OW-CCA2 安全性を満たすことを 4.1 節で，タイプ II 攻撃者に対する適応的 IND-CCA2 安全性を満たすことを 4.2 節で証明する．

4.1 タイプ I 攻撃者に対する適応的 OW-CCA2 安全性

定理 4.1 (タイプ I 攻撃者に対する適応的 OW-CCA2 安全性)**.** 提案方式の構成に用いる委譲可能 ABE 方式 Π が適応的 (準適応的，選択的) CPA 安全性を，OTS 方式 Γ が強偽造不可能性を，ハッシュ関数 H が一方向性を満たすとき，提案 ABEET 方式 Σ はタイプ I 攻撃者に対する適応的 (準適応的，選択的) OW-CCA2 安全性を満たす．

紙面の都合で，適応的安全性の場合の定理 4.1 の証明の概要のみを示す．証明のために，ゲーム列 $\mathbf{Game}_0, \mathbf{Game}_1, \mathbf{Game}_2$ を用いる．$\mathbf{Game}_0$ は定義 2.1 のゲームと同じである．$\mathbf{Game}_1$ では，$\mathcal{A}$ の復号クエリ $(y, \mathsf{ct}_x) = (y, (\mathsf{verk}, \mathsf{ABE.ct}_{x,0,\mathsf{verk}}, \mathsf{ABE.ct}_{x,1,\mathsf{verk}}, \sigma))$ が

- $\mathsf{verk} = \mathsf{verk}^*$,
- $\mathsf{Sig.Vrfy}(\mathsf{verk}, [\mathsf{ABE.ct}_{x,0,\mathsf{verk}} \| \mathsf{ABE.ct}_{x,1,\mathsf{verk}}], \sigma) \to 1$,
- $(\mathsf{ABE.ct}_{x,0,\mathsf{verk}}, \mathsf{ABE.ct}_{x,1,\mathsf{verk}}, \sigma) \neq (\mathsf{ABE.ct}^*_{x^*,0,\mathsf{verk}^*}, \mathsf{ABE.ct}^*_{x^*,1,\mathsf{verk}^*}, \sigma^*)$,

のいずれかを満たす場合には，$\mathcal{C}$ はゲームを中止し，$\mathsf{M} \leftarrow_{\$} \mathcal{M}$ を出力する．ただし，$(\mathsf{ABE.ct}^*_{x^*,0,\mathsf{verk}^*}, \mathsf{ABE.ct}^*_{x^*,1,\mathsf{verk}^*}, \sigma^*)$ はチャレンジ暗号文である．$\mathbf{Game}_2$ では，$\mathsf{ABE.ct}^*_{x^*,0,\mathsf{verk}^*}$ を M^* ではなく $\mathsf{M} \leftarrow_{\$} \mathcal{M}$ の暗号文とする．詳細は省略するが，Yamada らによる CHK 変換 [11] の ABE への拡張 [25] と同様に，OTS 方式 Γ が強偽造不可能性を満たすならば $\mathbf{Game}_0$ と $\mathbf{Game}_1$ は計算量的に識別不能であり，委譲可能 ABE 方式 Π が適応的 IND-CPA 安全ならば $\mathbf{Game}_1$ と $\mathbf{Game}_2$ は計算量的に識別不能であることを示せる．

$\mathbf{Game}_2$ の変更により，$\mathcal{A}$ が得る M^* に関する情報は $\mathsf{H}(\mathsf{M}^*)$ の暗号文である $\mathsf{ABE.ct}^*_{x^*,1,\mathsf{verk}^*}$ のみで，$\mathsf{P}(x^*, y) = 1$ を満たすトラップドア td_y を持つ $\mathcal{A}$ は $\mathsf{H}(\mathsf{M}^*)$ を計算できる．ここで，ハッシュ関数 H が一方向性を満たすならば，$\mathcal{A}$ は $\mathsf{H}(\mathsf{M}^*)$ から M^* を計算できず，提案 ABEET 方式は一方向性を満たす．よって，定理 4.1 が証明できる．

4.2 タイプ II 攻撃者に対する適応的 IND-CCA2 安全性

定理 4.2 (タイプ II 攻撃者に対する適応的 IND-CCA2 安全性)**.** 提案方式の構成に用いる委譲可能 ABE 方式 Π が適応的 (準適応的，選択的) CPA 安全性を，OTS 方式 Γ が強偽造不可能性を満たすとき，提案 ABEET 方式 Σ はタイプ II 攻撃者に対する適応的 (準適応的，選択的) IND-CCA2 安全性を満たす．

紙面の都合で，適応的安全性の場合の定理 4.2 の証明の概要のみを示す．ここで，定理 4.1 の証明と本質的に同じゲーム列 $\mathbf{Game}_0, \mathbf{Game}_1, \mathbf{Game}_2$ を用いる．$\mathbf{Game}_2$ の変更により，$\mathcal{A}$ が得る coin^* に関する情報は $\mathsf{H}(\mathsf{M}^*_{\mathsf{coin}^*})$ の暗号文である $\mathsf{ABE.ct}^*_{x^*,1,\mathsf{verk}^*}$ のみとなる．ただし，定理 4.1 のときと違い，$\mathcal{A}$ は $\mathsf{P}(x^*, y) = 1$ を満たすトラップドア td_y を持たないため $\mathsf{H}(\mathsf{M}^*_{\mathsf{coin}^*})$ を自明に得ることはできない．ここで，委譲可能 ABE 方式 Π が適応的 IND-CPA 安全ならば，$\mathcal{A}$ は $\mathsf{ABE.ct}^*_{x^*,1,\mathsf{verk}^*}$ から coin^* を識別できず，提案 ABEET 方式は識別不可能性を満たす．よって，定理 4.2 が証明できる．

5. まとめ

本論文では，IND-CPA 安全な 3 階層の委譲可能 ABE 方式を用いた CCA 安全な ABEET の一般的構成法を提案した．提案構成は，Lee らの 3 階層 HIBE を用いた CCA 安全な IBEET の一般的構成法の属性ベースへの拡張である [19]．CCA 安全性を達成するために，CHK 変換 [11] を ABE の場合に拡張した Yamada らの方法 [25] を使用した．Predicate encoding や Pair encoding の枠組みと既存の格子ベース委譲可能 ABE 方式 [9] を基に，既存方式では未達成の特性を持つ様々な ABEET を得られた．なお ABE に委譲可能性を持たせるための一般的な方法は知られておらず，未解決問題がいくつか考えられる．(非) 単調スパンプログラム (方式 1–12) に対して，標準モデルで同じ述語に対する ABEET 方式を得たが，ランダムオラクルモデルでより効率的な方式 [2], [22] が提案されている．決定性有限オートマトンに対する最初の q-ratio 仮定による ABEET 方式 (方式 13 と 14) を得たが，標準 k-linear 仮定 [5], [16], [17] の基で同じ述語に対する ABE 方式と LWE 仮定 [4] による非決定性有限オートマトンの ABE 方式が提案されている．また，回路と内積述語に対して選択的安全な格子ベース ABEET 方式を得たが，回路に対する準適応的安全な格子ベース ABE 方式 [10] と適応的に安全な格子ベース内積暗号 [18] が存在する．これらの性質を持つ CCA 安全な ABEET 方式を構成することは興味深い未解決問題である．

謝辞　本研究は JSPS 科研費 JP18H05289, JP21H03395 の助成，JST CREST 課題番号 JPMJCR2113 の助成，および文部科学省の卓越研究員事業の支援を受けたものです．

参考文献

[1] Agrawal, S. and Chase, M.: A Study of Pair Encodings: Predicate Encryption in Prime Order Groups, *TCC*, pp. 259–288 (2016).

[2] Agrawal, S. and Chase, M.: FAME: Fast Attribute-based Message Encryption, *ACM CCS*, pp. 665–682 (2017).

[3] Agrawal, S. and Chase, M.: Simplifying Design and Analysis of Complex Predicate Encryption Schemes, *EUROCRYPT*, pp. 627–656 (2017).

[4] Agrawal, S., Maitra, M. and Yamada, S.: Attribute Based Encryption (and more) for Nondeterministic Finite Automata from LWE, *CRYPTO*, pp. 765–797 (2019).

[5] Agrawal, S., Maitra, M. and Yamada, S.: Attribute Based Encryption for Deterministic Finite Automata from DLIN, *TCC*, pp. 91–117 (2019).

[6] Ambrona, M., Barthe, G. and Schmidt, B.: Generic Transformations of Predicate Encodings: Constructions and Applications, *CRYPTO*, pp. 36–66 (2017).

[7] Attrapadung, N.: Dual System Encryption via Doubly Selective Security: Framework, Fully Secure Functional Encryption for Regular Languages, and More, *EUROCRYPT*, pp. 557–577 (2014).

[8] Attrapadung, N.: Unbounded Dynamic Predicate Compositions in Attribute-Based Encryption, *EUROCRYPT*, pp. 34–67 (2019).

[9] Boneh, D., Gentry, C., Gorbunov, S., Halevi, S., Nikolaenko, V., Segev, G., Vaikuntanathan, V. and Vinayagamurthy, D.: Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits, *EUROCRYPT*, pp. 533–556 (2014).

[10] Brakerski, Z. and Vaikuntanathan, V.: Circuit-ABE from LWE: Unbounded Attributes and Semi-adaptive Security, *CRYPTO*, pp. 363–384 (2016).

[11] Canetti, R., Halevi, S. and Katz, J.: Chosen-Ciphertext Security from Identity-Based Encryption, *EUROCRYPT*, pp. 207–222 (2004).

[12] Chen, J., Gay, R. and Wee, H.: Improved Dual System ABE in Prime-Order Groups via Predicate Encodings, *EUROCRYPT*, pp. 595–624 (2015).

[13] Chen, J. and Gong, J.: ABE with Tag Made Easy - Concise Framework and New Instantiations in Prime-Order Groups, *ASIACRYPT*, pp. 35–65 (2017).

[14] Cui, Y., Huang, Q., Huang, J., Li, H. and Yang, G.: Outsourced Ciphertext-Policy Attribute-Based Encryption with Equality Test, *Inscrypt*, pp. 448–467 (2018).

[15] Cui, Y., Huang, Q., Huang, J., Li, H. and Yang, G.: Ciphertext-Policy Attribute-Based Encrypted Data Equality Test and Classification, *Comput. J.*, Vol. 62, No. 8, pp. 1166–1177 (2019).

[16] Gong, J., Waters, B. and Wee, H.: ABE for DFA from k-Lin, *CRYPTO*, pp. 732–764 (2019).

[17] Gong, J. and Wee, H.: Adaptively Secure ABE for DFA from k-Lin and More, *EUROCRYPT*, pp. 278–308 (2020).

[18] Katsumata, S., Nishimaki, R., Yamada, S. and Yamakawa, T.: Adaptively Secure Inner Product Encryption from LWE, *ASIACRYPT*, pp. 375–404 (2020).

[19] Lee, H. T., Ling, S., Seo, J. H., Wang, H. and Youn, T.: Public key encryption with equality test in the standard model, *Inf. Sci.*, Vol. 516, pp. 89–108 (2020).

[20] Li, C., Shen, Q., Xie, Z., Feng, X., Fang, Y. and Wu, Z.: Large Universe CCA2 CP-ABE With Equality and Validity Test in the Standard Model, *Comput. J.*, Vol. 64, No. 4, pp. 509–533 (2021).

[21] Takayasu, A.: Tag-based ABE in prime-order groups via pair encoding, *Des. Codes Cryptogr.*, Vol. 89, No. 8, pp. 1927–1963 (2021).

[22] Tomida, J., Kawahara, Y. and Nishimaki, R.: Fast, Compact, and Expressive Attribute-Based Encryption, *PKC*, pp. 3–33 (2020).

[23] Wang, Y., Cui, Y., Huang, Q., Li, H., Huang, J. and Yang, G.: Attribute-Based Equality Test Over Encrypted Data Without Random Oracles, *IEEE Access*, Vol. 8, pp. 32891–32903 (2020).

[24] Wee, H.: Dual System Encryption via Predicate Encodings, *TCC*, pp. 616–637 (2014).

[25] Yamada, S., Attrapadung, N., Hanaoka, G. and Kunihiro, N.: Generic Constructions for Chosen-Ciphertext Secure Attribute Based Encryption, *PKC*, pp. 71–89 (2011).

[26] Yang, G., Tan, C. H., Huang, Q. and Wong, D. S.: Probabilistic Public Key Encryption with Equality Test, *CT-RSA*, pp. 119–131 (2010).

[27] 淺野京一，江村恵太，　高安敦：LWE 仮定に基づく適応的 CCA 安全な平文一致確認可能 ID ベース暗号の効率的な構成，信学技報, ISEC2022-29，Vol. 122, pp. 131–138 (2022).