Constructions of CCA Secure Public Key Encryption and Attribute Based Encryption（CCA 安全な公開鍵暗号と属性ベース暗号の設計）

数理第一研究室 2 年　山田翔太
指導教員：國廣昇准教授

1　背景

属性ベース暗号は，公開鍵暗号の一般化であり，受信者の集合を細かく指定することができる．本研究では，検証可能性または委譲可能性という性質をもち，IND-CPA 安全性という弱い安全性をもつような属性ベース暗号を IND-CCA 安全性という強い安全性をもつ属性ベース暗号に変換する一般的な変換方法を提案した．

2　準備

本節ではまず関数型暗号定義を行う．次にその特殊ケースである Ciphertext-policy ABE (CP-ABE) と Key-policy ABE (KP-ABE) の定義を行う．

2.1　関数型暗号

定義 Σ_k と Σ_e をそれぞれ “鍵属性”と “暗号文属性” の空間とし，$R:\ \Sigma_k \times \Sigma_e \to \{0,1\}$ を論理関数とする．R を用いた関数型暗号は **Setup**, **KeyGen**，**Encrypt**，**Decrypt**，の 4 つのアルゴリズムからなる．

Setup$(\lambda, \mathrm{des}) \to (PK, MSK)$: セキュリティパラメータ λ を入力とし，方式の記述 des，公開鍵 PK，マスター秘密鍵 MSK を出力する．

KeyGen$(MSK, PK, X) \to SK_X$: マスター秘密鍵 MSK，公開鍵 PK，鍵属性 $X \in \Sigma_k$ を入力とし，X のための秘密鍵 SK_X を出力する．

Encrypt$(PK, M, Y) \to CT$: 公開鍵 PK，メッセージ M，暗号文属性 $Y \in \Sigma_e$ を入力とし，暗号文 CT を出力する．Y は CT の中に含まれているものと仮定する．

Decrypt$(PK, CT, SK_X) \to M$or $\perp$: 公開鍵 PK，暗号文 CT，秘密鍵 SK_X を入力とし，メッセージ M，または暗号文が不正であることを示す $\perp$ を出力する．

2.2　属性ベース暗号の定義

定義 1 (KP-ABE)**.** U を属性の空間とする．U の上のアクセス構造の集合 $\mathcal{A}$ に関する *KP-ABE* は，論理関数として $R^{\mathsf{KP}} : \mathcal{A} \times 2^U \to \{0,1\}$ を用いる関数型暗号である．ここで，R^{KP} は，$\omega \in \mathbb{A}$ であるときに限り $R^{\mathsf{KP}}(\mathbb{A}, \omega) \mapsto 1$ となる関数であると定義する．

定義 2 (CP-ABE)**.** U を属性の空間とし，U の上のアクセス構造の集合 $\mathcal{A}$ に関する *CP-ABE* は，論理関数として $R^{\mathsf{CP}} : 2^U \times \mathcal{A} \to \{0,1\}$ を用いる関数型暗号である．ここで，R^{CP} は，$\omega \in \mathbb{A}$ であるときに限り $R^{\mathsf{CP}}(\omega, \mathbb{A}) \mapsto 1$ となる関数であると定義する．

Table 1: X', Y' と **Subroutine** の設定の仕方

変換 CP-ABE1	変換 KP-ABE1
検証可能性を持つ CPA CP-ABE ⇒ CCA CP-ABE	検証可能性を持つ CPA KP-ABE⇒ CCA KP-ABE
鍵属性 $X' = X$ **暗号文属性** $Y' = Y \vee (\wedge_{P \in S_{vk}} P)$ **Subroutine** If **Verify**$(PK, CT, X, S_{vk}) = 0$ or $\perp$ Return $\perp$. Else Return **Decrypt**$(PK, CT, SK_{X'})$.	**鍵属性** $X' = X$ **暗号文属性** $Y' = Y \cup S_{vk}$ **Subroutine** If **Verify**$(PK, CT, X, \wedge_{P \in S_{vk}} P) = 0$ or $\perp$ Return $\perp$. Else Return **Decrypt**$(PK, CT, SK_{X'})$.
変換 CP-ABE2	**変換 KP-ABE2**
委譲可能性をもつ CPA CP-ABE ⇒ CCA CP-ABE	委譲可能性をもつ CPA KP-ABE ⇒ CCA KP-ABE
鍵属性 $X' = X \cup W$ **暗号文属性** $Y' = Y \wedge (\wedge_{P \in S_{vk}} P)$ **Subroutine** Run **Delegate**$(PK, SK'_X, X \cup W, X \cup S_{vk})$ $\rightarrow SK_{X \cup S_{vk}}$. Return **Decrypt**$(PK, CT, SK_{X \cup S_{vk}})$.	**鍵属性** $X' = X$ **暗号文属性** $Y' = Y \cup S_{vk}$ **Subroutine** Run **Delegate**$(PK, SK'_X, X, X \wedge (\wedge_{P \in S_{vk}} P))$ $\rightarrow SK_{X \wedge (\wedge_{P \in S_{vk}} P)}$. Return **Decrypt**$(PK, CT, SK_{X \wedge (\wedge_{P \in S_{vk}} P)})$.

3 変換方式

属性空間の設定

- Π が小さい属性の空間をもつならば，W は $W = \{P_{1,0}, P_{1,1}, P_{2,0}, P_{2,1}, \ldots, P_{\ell,0}, P_{\ell,1}\}$ と定義される．ダミー属性の集合 $S_{vk} \subset W$ は $S_{vk} = \{P_{1,vk_1}, P_{2,vk_2}, \ldots, P_{\ell,vk_\ell}\}$ と定義される．ここで vk_j は vk の j 番目のビットである．
- Π が大きい属性の空間を持つならば，W は $W = \{0,1\}^\ell$ と定義される．ダミー属性の集合 $S_{vk} \subset W$ は $S_{vk} = \{vk\}$ と定義される．

テンプレート 検証可能性または委譲可能性を持つCPA安全な関数型暗号 $\Pi = (\mathbf{Setup}, \mathbf{KeyGen}, \mathbf{Encrypt}, \mathbf{Decrypt})$ を用いて，CCA 安全な関数型暗号 $\Pi' = (\mathbf{Setup}', \mathbf{KeyGen}', \mathbf{Encrypt}', \mathbf{Decrypt}')$ を以下のように構成する．$\Sigma = (\mathcal{G}, \mathcal{S}, \mathcal{V})$ をワンタイム署名とする．

Setup$'(\lambda, U)$. **Setup**$(\lambda, U \cup W) \rightarrow (PK, MSK)$ を実行し，(PK, MSK) を出力する．

KeyGen$'(MSK, PK, X)$. **KeyGen**$(MSK, PK, X') \rightarrow SK_{X'}$ を実行し，$SK'_X = SK_{X'}$ を出力する．

Encrypt$'(PK, M, Y)$ $\mathcal{G}(\lambda) \rightarrow (vk, sk)$ を最初に実行する．次に **Encrypt**$(PK, M, Y') \rightarrow CT$ と $\mathcal{S}(sk, CT) \rightarrow \sigma$ を実行し，$CT' = (vk, CT, \sigma)$ を出力する．

Decrypt$'(PK, CT', SK'_X)$ 最初に，暗号文 CT' を (vk, CT, σ) と分離する．もし $\mathcal{V}(vk, CT, \sigma) = 0$ ならば $\perp$ を出力し，そうでないならば **Subroutine** を実行し，得られた値を出力する．