IDベース暗号の強秘匿匿名性について

小松 みさき[1,2,a)]　山田 翔太[2]　坂井 祐介[2]　花岡 悟一郎[2]

概要：匿名性を持つ ID ベース暗号の具体的構成や安全性について，これまで多くの研究がなされているが，これらのほとんどにおいては識別不可能性に基づいた安全性定義が与えられており，強秘匿性（semantic security）を必ずしも直接的に捉えたものとはなっていない．本研究においては，ID ベース暗号の匿名性に関する強秘匿性の定義を行い，これが識別不可能性に基づく安全性を示唆することを明らかにする．

キーワード：ID ベース暗号，匿名性，強秘匿性

Semantic Security of Anonymous Identity-Based Encryption

Misaki Komatsu[1,2,a)]　Shota Yamada[2]　Yusuke Sakai[2]　Goichiro Hanaoka[2]

Abstract: The security notions of anonymity for identity-based encryption (IBE) as well as constructions satisfying it have long been studied. However, these definitions are indistinguishability-based and does not necessarily capture more natural notion of the semantic security. In this paper, we give a semantic security style definition of the anonymity for IBE and prove that this security notion implies indistinguishability-based definition.

Keywords: identity-based encryption, anonymity, semantic security

1. はじめに

ID ベース暗号（IBE：identity-based encryption）は公開鍵暗号を拡張した概念であり，任意に選ばれた ID 情報に向けて暗号化することが可能である．IBE の安全性としては，平文情報が暗号文から漏れないことを要求する平文秘匿性と，ID 情報が暗号文から漏れないことを要求する匿名性を考えることができる．多くの IBE の具体的構成がこれまでに考えられてきており，また，様々な安全性定義間の関係性についても明らかになっている [3]．しかしながら，先行研究においては ID に関する匿名性の定義のほとんどは識別不可能性に基づいており（例えば [4], [1]），強秘匿性を直接的な意味で捉えた安全性定義は存在しない．

本稿では，この問題に取り組み，IBE の匿名性に関する強秘匿性を定義する．より具体的には，IBE の拡張である属性ベース暗号の属性情報に関する強秘匿性の安全性定義 [7] をもとにして，ID ベース鍵カプセル化メカニズム（IB-KEM：identity-based key encapsulation mechanism）に関する匿名性を，強秘匿性をとらえた形で定義する（Ano-SS-CPA 安全：Anonymous Semantic Security under chosen plaintext attack）．また，定義した Ano-SS-CPA 安全性が従来の識別不可能性に基づく安全性 Ano-LOR-CPA 安全：Anonymous Left-or-Right under chosen plaintext attack）を示唆することを証明により明らかにする．なお，以降，登場する安全性は匿名性について考えるので Ano の記述は省略する．今後の課題としては，本研究で定義した SS-CPA 安全と LOR-CPA 安全が等価であるかどうか明らかにすることが挙げられる．

2. 準備

本節ではまず，この論文で使用する語句や必要な知識に

[1] 東京電機大学
Tokyo Denki University
[2] 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
[a)] 18rmd09@ms.dendai.ac.jp

ついて述べた後，ID ベース鍵カプセル化メカニズムを定義し，ID に関する匿名性を捉えた既存の安全性概念である LOR-CPA 安全について説明する．

2.1 基礎的な記述法

本稿において $x \leftarrow Y$ と書く時，Y が集合である場合，一様ランダムに Y の要素を取り出し，x に代入したことを示す．Y がアルゴリズムまたは関数である場合，x を出力する操作を意味する．A を確率的多項式時間アルゴリズムとした時，A^O は A がオラクル O へアクセスできることを表す．k は常にセキュリティパラメータを示す．$\mathbb{N}$ を自然数の集合，$\mathbb{R}$ を実数の集合とするとき，関数 $\varepsilon : \mathbb{N} \to \mathbb{R}$ に関して，全ての定数 $c > 0$ に対して，$n \in \mathbb{N}$ が存在し，全ての $k > n$ に対して $\varepsilon(k) < k^{-c}$ が成立するとき $\varepsilon(k)$ は k に関して無視できる（negligible）という．

2.2 ID ベース鍵カプセル化メカニズム

ここでは ID ベース鍵カプセル化メカニズム（IB-KEM）のシンタックス，正当性について述べる．

2.2.1 シンタックス

IB-KEM Σ は 4 つの確率的アルゴリズム (S, K, E, D) から構成される．$\mathcal{ID}$ は ID 空間，$\mathcal{K}$ は鍵空間である．

セットアップ：$S(1^k) \to (prm, msk)$
k をセキュリティパラメータとしたとき 1^k を入力とし，公開パラメータ prm とマスター秘密鍵 msk を出力する．

鍵生成：$K(msk, id) \to usk_{id}$
マスター秘密鍵 msk と $id \in \mathcal{ID}$ を入力とし，入力 ID に対応した復号鍵（ユーザー秘密鍵）usk_{id} を出力する．

暗号化：$E(prm, id) \to (ct, kem)$
公開パラメータ prm と $id \in \mathcal{ID}$ から，暗号文 ct と対称鍵 $kem \in \mathcal{K}$ を出力する．

復号：$D(ct, usk_{id}) \to kem / \perp$
暗号文 ct とユーザ秘密鍵 usk_{id} を入力とし，対称鍵 kem または $\perp$ を出力する．

2.2.2 正当性

IB-KEM Σ が正当性をもつとは，$(prm, msk) \leftarrow S(1^k)$ および $(ct, kem) \leftarrow E(prm, id)$ に関して確率を取った時，$\Pr[\, kem = D(usk_{id}, ct)\,] = 1$ が成立することを言う．

2.3 LOR-CPA 安全

LOR は，攻撃者が適当な ID を 2 つ選びそのどちらかを使用して暗号化した (ct, kem) を受け取った時どちらの ID の暗号化なのか識別できない，という形で定義される安全性である．該当安全性は，確率的多項式時間攻撃者 $A = (A_1, A_2)$ と挑戦者のゲームによって定義される．以下，$LOR\text{-}CPA\text{-}0$ および $LOR\text{-}CPA\text{-}1$ という 2 つの実験を考える．

$\underline{\mathrm{Exp}_{\Sigma,A}^{LOR\text{-}CPA\text{-}0}(k)}$

$(prm, msk) \leftarrow S(1^k);$
$(id_0, id_1, s) \leftarrow A_1(prm);$
$(ct, kem) \leftarrow E(id_0, prm);$
$b' \leftarrow A_2^{K(\,msk,\,\cdot\,)}(ct, kem, s);$

$\underline{\mathrm{Exp}_{\Sigma,A}^{LOR\text{-}CPA\text{-}1}(k)}$

$(prm, msk) \leftarrow S(1^k);$
$(id_0, id_1, s) \leftarrow A_1(prm);$
$(ct, kem) \leftarrow E(d_1, prm);$
$b' \leftarrow A_2^{K(\,msk,\,\cdot\,)}(ct, kem, s);$

鍵生成オラクル $K(\,msk, \cdot\,)$ は id が入力されると，id と紐づいた usk_{id} を送り返す．この時，id_0, id_1 をクエリすることは禁止される．

この時，Σ における A の優位性は

$$\mathrm{Adv}_{\Sigma,A}^{LOR\text{-}CPA}(k) := \left| \begin{array}{l} \Pr\left[\mathrm{Exp}_{\Sigma,A}^{LOR\text{-}CPA\text{-}0}(k) \to 1\right] \\ -\Pr\left[\mathrm{Exp}_{\Sigma,A}^{LOR\text{-}CPA\text{-}1}(k) \to 1\right] \end{array} \right|$$

定義 1　いかなる確率的多項式時間攻撃者 A に対しても無視できる $\epsilon(k)$ に対し $\mathrm{Adv}_{\Sigma,A}^{LOR\text{-}CPA}(k) < \epsilon(k)$ が成立するならば，IB-KEM Σ は LOR-CPA 安全である．上記の定義では，A_1 は $K(msk, \cdot)$ に関するオラクルアクセスが与えられていないことに注意されたい．これは semi-adaptive security と呼ばれる種類の安全性 [2] である．本稿の結果が A_1 に $K(msk, \cdot)$ へのオラクルアクセスが与えられた設定においても（すなわち，Adaptive security の設定においても）成り立つかどうかは今後の課題としたい．

定理 1　いかなる確率的多項式時間攻撃者 A に対して IB-KEM Σ が LOR-CPA 安全である時，次の式が成り立つ．b はコイントスにより選ばれる 0 または 1 の値である．

$$\left| \Pr\left[\, b = b' \,|\, \mathrm{Exp}_{\Sigma,A}^{LOR\text{-}CPA\text{-}b}(k) \to b' \,\right] - \frac{1}{2} \right| < \epsilon(k)$$

証明は簡単な式変形によって可能である．類似の証明は [8] 等に詳しく書かれているため，ここでは省く．

3. 提案する強秘匿匿名性定義

本節では，新たに定義した強秘匿性を直接的に捉える SS-CPA 安全とその定義についてまとめる．

Goldwsser らは [5] において，暗号文からどのような部分情報も攻撃者に漏れないということを Semantic Security（SS 定義）として定義した．いかなる攻撃者に対しても，それに対してシミュレータが存在し、攻撃者が暗号文を受け取った環境（REAL 環境）における出力と，シミュレータが何も受け取らない環境（IDEAL 環境）における出力

とが，計算量的に区別がつかない時，強秘匿安全であるという．

通常，多くの SS 定義は [5] を利用して再定義される．しかし，[5] は平文秘匿性に関する SS 定義であるため，本研究の目標である匿名性を考える SS 定義の再定義には適さなかった．

従って，本研究では Wee が [7] で定義した属性ベース暗号（ABE：Attribute-based encryption）の属性情報に関する SS 定義を用いた．この定義では，安全性を証明したい暗号方式に対して，その理想機能を記述するシミュレータが存在し，攻撃者が，実際の環境 (REAL 環境) と，シミュレータによりシミュレートされた環境 (IDEAL 環境) を識別できない時，どのような部分情報も攻撃者に漏れていない，と定義される．

また，[7] の SS 定義は ABE についての定義だが，本研究の目標は IBE（IB-KEM）における SS の定義である．IBE は ABE の一種であるので，本節では一般の ABE ではなく IBE に限定した定義を与え，IB-KEM の SS 定義として再定義した．

3.1 SS-CPA 安全

SS は暗号文からどのような部分情報も得られないことを意味する安全性定義である．Σ を用いて暗号化が行われる REAL 環境 ($SS\text{-}CPA\text{-}REAL$) と，$\Sigma^* = (S^*, E^*, K^*)$ を使用する IDEAL 環境 ($SS\text{-}CPA\text{-}IDEAL$) を考える．

$\underline{\mathrm{Exp}^{SS\text{-}CPA\text{-}REAL}_{\Sigma,A}(k)}$

$(prm, msk) \leftarrow S(1^k);$

$(id', s) \leftarrow A_1(prm);$

$(ct, kem) \leftarrow E(prm, id');$

$b \leftarrow A_2^{K(msk,\cdot)}(ct, kem, s);$

$\underline{\mathrm{Exp}^{SS\text{-}CPA\text{-}IDEAL}_{\Sigma^*,A}(k)}$

$(prm, msk) \leftarrow S^*(1^k);$

$(id', s) \leftarrow A_1(prm);$

$ct \leftarrow E^*(msk); \quad kem \leftarrow \mathcal{K};$

$b \leftarrow A_2^{K^*(msk,\cdot)}(ct, kem, s);$

s は状態情報，$\mathcal{K}$ は対称鍵空間である．鍵生成オラクル $K(msk, \cdot)$ とシミュレータ $K^*(msk, \cdot)$ は入力に id をとり，その ID と紐づいた usk_{id} を返す．この時，id' のクエリは禁止される．A_2 は 0 または 1 を出力する．

SS-CPA 攻撃者 A の優位性 $\mathrm{Adv}^{SS\text{-}CPA}_{\Sigma,A}(k)$ を次のように定義できる．

$$\mathrm{Adv}^{SS\text{-}CPA}_{\Sigma,A}(k) := \left| \begin{array}{l} \Pr\left[\mathrm{Exp}^{SS\text{-}CPA\text{-}REAL}_{\Sigma,A}(k) \to 1\right] \\ -\Pr\left[\mathrm{Exp}^{SS\text{-}CPA\text{-}IDEAL}_{\Sigma^*,A}(k) \to 1\right] \end{array} \right|$$

定義 2　いかなる確率的多項式時間攻撃者 A に対しても確率的多項式時間シミュレータ Σ^* が存在し無視できる $\epsilon(k)$ に対し，$\mathrm{Adv}^{SS\text{-}CPA}_{\Sigma,A}(k) < \epsilon(k)$ が成立するならば，IB-KEM Σ は SS-CPA 安全である．

上記の定義における A は，ゲーム内で得られる情報から自身のいる環境が REAL 環境か IDEAL 環境かを推測する．A が REAL 環境下で得られる情報と，IDEAL 環境下で得られる情報とが識別できないならば，どのような部分情報も A に漏れていないので，安全である．という形で定式化される．つまり，安全性を証明したい暗号方式 Σ はその理想機能として記述された Σ^* を事実上実現している時，安全であると考える．

上記の定義において，REAL 環境では，攻撃者が推測したい ID（id'）を用いて作成した (ct, kem) が攻撃者に与えられる．IDEAL 環境では，id' を用いずにシミュレータが作成した (ct, kem) が与えられる．つまり，IDEAL 環境下において，攻撃者の視点からは id' は情報理論的に隠されている．よって，この 2 つの環境が区別つかない時，ID に関する情報は攻撃者に一切漏れていないと考えられる．

4. 定義の関係性

本節では，3 節で定義した SS-CPA 安全が LOR-CPA 安全を示唆することを背理法を用いて証明する．

定理 2　ある IB-KEM Σ が SS-CPA 安全であるならば，Σ は LOR-CPA 安全である．

証明　定理の対偶である「Σ が LOR-CPA 安全でないならば，Σ は SS-CPA 安全ではない」ことが正しいことを示す．つまり，Σ に対して LOR-CPA を破る確率的多項式時間攻撃者 $A := (A_1, A_2)$ を内部で利用することで，SS-CPA を破る確率的多項式時間攻撃者 $B := (B_1, B_2)$ を構成すればよい．

A を利用して B を以下のように構成する．

$\underline{B_1(prm)}$	$\underline{B_2^{\mathcal{O}}(ct, kem, s)}$
$(id_0, id_1, s) \leftarrow A_1(prm);$	$b' \leftarrow A_2(ct, kem, s);$
$b \xleftarrow{R} \{0, 1\};$	$b' = b$ ならば, 1 を出力
id_bを出力	$b' \neq b$ ならば, 0 を出力

$\mathcal{O}$ は鍵生成オラクルである．msk, id^* を入力とし，usk_{id^*} を出力する．B_2 は，A_2 から id^* が送られてきた時に id^* を $\mathcal{O}$ へクエリする．そして，得られた usk_{id*} を A_2 に送り返す．

ここで，Σ における SS-CPA 攻撃者 B の優位性について考える．

$\underline{\mathrm{Exp}^{SS\text{-}CPA\text{-}REAL}_{\Sigma,B}(k)}$

$(prm, msk) \leftarrow S(1^k);$
$(id_b, s) \leftarrow B_1(prm);$
$(ct, kem) \leftarrow E(id_b, prm);$
$v \leftarrow B_2^{K(\,msk,\,\cdot\,)}(ct, kem, s);$

$\underline{\mathrm{Exp}^{SS\text{-}CPA\text{-}IDEAL}_{\Sigma^*,B}(k)}$

$(prm, msk) \leftarrow S^*(1^k);$
$(id_b, s) \leftarrow B_1(prm);$
$ct \leftarrow E^*(msk); \quad kem \leftarrow \mathcal{K};$
$v \leftarrow B_2^{K^*(\,msk,\,\cdot\,)}(ct, kem, s);$

上記２つの実験について，A の視点から状況を考える．

まず $\mathrm{Exp}^{SS\text{-}CPA\text{-}REAL}_{\Sigma,B}(k)$ における LOR-CPA 攻撃者 A の視点を考える．A が受け取る (ct, kem) は Σ を用いて正しく生成されている．鍵生成オラクルに対するクエリでは，オラクルへアクセスする際，A は B を経由する．この時，A は自身が選んだ id_0, id_1 のクエリが禁止されている．B は id_b のみクエリが禁止されているため，A がクエリしようとする全ての ID についての結果を得ることができる．よって，問題なく鍵生成オラクルへのクエリが行われる．

これらの事実から A の視点では LOR-CPA ゲームが行われているように見える．このことから，B が SS-CPA を破るのに成功する確率は A が b の識別に成功する確率と同じであると考えられる．

よって，

$$\begin{aligned}&\Pr\left[\mathrm{Exp}^{SS\text{-}CPA\text{-}REAL}_{\Sigma,B}(k) \to 1\right]\\ &= \Pr\left[b = b' \,|\, \mathrm{Exp}^{LOR\text{-}CPA\text{-}b}_{\Sigma,A}(k) \to b'\right]\end{aligned}$$

となる．

次に $\mathrm{Exp}^{SS\text{-}CPA\text{-}IDEAL}_{\Sigma^*,B}(k)$ における A の視点を考える．この時 (ct, kem) は id_b を一切用いずに作られている．A の視点から b が使われているところがないので，b は情報理論的に隠されている．鍵生成オラクル $K^*(\,msk, \cdot\,)$ へのクエリは，REAL 環境同様，A の選択した ID が B を経由して送られる．その出力は B を経由して A に返される．
b と b' は独立なので，A_2 は一様ランダムに b' を出力する．よって，

$$\Pr\left[\mathrm{Exp}^{SS\text{-}CPA\text{-}IDEAL}_{\Sigma^*,B}(k) \to 1\right] = \frac{1}{2}$$

と考えられる．

以上より，

$$\begin{aligned}&\mathrm{Adv}^{SS\text{-}CPA}_{\Sigma,B}(k)\\ &= \left|\Pr\left[\mathrm{Exp}^{SS\text{-}CPA\text{-}REAL}_{\Sigma,B}(k) \to 1\right]\right.\\ &\quad \left. - \Pr\left[\mathrm{Exp}^{SS\text{-}CPA\text{-}IDEAL}_{\Sigma^*,B}(k) \to 1\right]\right|\\ &= \left|\Pr\left[b = b' \,|\, \mathrm{Exp}^{LOR\text{-}CPA\text{-}b}_{\Sigma,A}(k) \to b'\right] - \frac{1}{2}\right|\\ &= \mathrm{Adv}^{LOR\text{-}CPA}_{\Sigma,A}(k)\end{aligned}$$

A は LOR-CPA を破る攻撃者であるから $\mathrm{Adv}^{LOR\text{-}CPA}_{\Sigma,A}(k) > \epsilon(k)$ となる．よって $\mathrm{Adv}^{SS\text{-}CPA}_{\Sigma,B}(k) > \epsilon(k)$ が成り立つ．

したがって，LOR-CPA 攻撃者 A が存在する時，SS-CPA 攻撃者 B が存在するので，その対偶である定理は正しい．

5. まとめ

IBE の強秘匿匿名性定義について，強秘匿性の意味を直接的に捉えた安全性（SS-CPA）の定義を行ない，それが従来の識別不可能性を捉えた安全性（LOR-CPA）の定義を示唆することを明らかにした．今後の課題として，LOR-CPA 安全を満たす時，SS-CPA 安全であることを示唆しているのかどうかを明らかにすることが求められる．また，CPA 攻撃者よりも強い CCA1，CCA2 攻撃者時の安全性定義の評価とそれらの比較も求められる．

謝辞　本研究は，新明るい暗号勉強会にて活発な議論をさせて頂くことにより進めることができた．新明るい暗号勉強会の皆様に深く感謝する．

参考文献

[1] Xavier Boyen, Brent Waters: Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). CRYPTO 2006: 290-307

[2] Jie Chen, Hoeteck Wee:Semi-adaptive Attribute-Based Encryption and Improved Delegation for Boolean Formula. SCN 2014: 277-297

[3] D. Galindo, I. Hasuo. “Security Notions for Identity Based Encryption,” IACR Cryptology ePrint Archive, 2005, 253.

[4] M. Izabachene, D. Pointcheval.“New anonymity notions for identity-based encryption,”In Formal to Practical Security (pp. 138-157). Springer, Berlin, Heidelberg,2009.

[5] G Shafi, S Micali, “Probabilistic encryption,” Journal of computer and system sciences, 1984, 28.2: 270-299.

[6] A. Shamir, “Identity-based cryptosystems and sig- nature schemes,” CRYPTO 1984, pp.4753, 1984.

[7] H. Wee. “Attribute-Hiding Predicate Encryption in Bilinear Groups, Revisited,” In: Theory of Cryptography Conference. Springer, Cham, 2017. p. 206-233.

[8] 森山大輔, 西巻陵, 岡本龍明, : ”日本応用数理学会. 公開鍵暗号の数理.” シリーズ応用数理 / 日本応用数理学会監修 , 第２巻 (共立出版, 2011.)