Computer Security Symposium 2019
21 - 24 October 2019

IDベース暗号における強秘匿匿名性と識別不可能匿名性の等価性

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：多くの暗号要素技術では，識別不可能性（IND：Indistinguishability）に基づきデータの秘匿性の定義がなされている．本来，これはINDが強秘匿性を直接捉えた定義（SS：Semantic Security）と等価関係である場合に可能な手段であり，必ずしも全ての暗号要素技術において成り立つとは限らない．特に，IDベース暗号の匿名性の定義では，INDに基づく定義であるAno-LORが一般的に利用されてきたが，SSに基づく定義との等価性について検証がなされていなかった．これを踏まえ，CSS 2018において著者らは，SSに基づく匿名性としてAno-SSを定義し，Ano-SSがAno-LORを包含することを示した．本研究では，Ano-LORがAno-SSを包含することを明らかにし，Ano-LORとAno-SSが等価であることを示す．本成果は，これまで15年間以上利用されてきたAno-LORの概念が，厳密な強秘匿匿名性を示唆することを初めて明らかにするものである．

キーワード：IDベース暗号，匿名性，強秘匿性

On the Equivalence of Semantic Security and Indistinguishability of Anonymous Identity-Based Encryption

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

Abstract: In many cryptographic primitives, their security is usually defined based on the notion of indistinguishability. Originally, this is appropriate only for cases in which indistinguishability implies semantic security, but it is not always the case. Especially, regarding anonymity of identity-based encryption, indistinguishability-based definition has been widely used in the literature, but its relationship with semantic-security-based definition is still not clear. In this work, we show that indistinguishability-based and semantic-security-based definitions of anonymity in identity-based encryption are equivalent.

Keywords: Identity-based encryption, anonymity, semantic security

1. はじめに

1.1 背景

安全性の厳密な定義は，暗号技術の安全性を正確に評価するうえで非常に重要な基盤となる．IDベース暗号（IBE：Identity-Based Encryption）[5], [11], [22], [23]は，最も基本的な高機能暗号のひとつであり，検索可能暗号[1], [4]をはじめとする幅広い応用が知られている（他に[6], [9], [12], [19]等）．また，IBEから検索可能暗号を構成するうえで，基礎となるIBEにおける受信者IDの秘匿性（即ち，**匿名性**）が安全性の根幹をなしている．しかしながら，検索可能暗号が提案された2004年から現在に至るまで，IBEの匿名性に関し，厳密な安全性定義に基づく評価がなされてきたとは必ずしも言えない状況にある．具体的には，[1], [4]を起点とする匿名IBEについての一連の文献（たとえば，[3], [8], [10], [13], [15], [20], [26]）において，いずれも識別

[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

不可能性（IND：Indistinguishability）に基づき匿名性の定義がなされているが，これは暗号文から受信者 ID が漏えいしていないことを直ちに保証するものではない．つまり，**既存の匿名 IBE や検索可能暗号が実際には安全でない可能性があることを示唆している．**そのため，匿名性の厳密な定義のもと，これら既存技術の安全性を評価することは急務と言える．

IND に基づく匿名性の定義が不十分であることを補足する．Goldwasser と Micali [14] は，公開鍵暗号における平文秘匿性について，暗号文を与えられた任意の攻撃者に対して，暗号文を与えられずに同攻撃者の振る舞いを模倣可能なシミュレータを構成できるとき，この公開鍵暗号方式が強秘匿性（SS：Semantic Security）を持つものと定義した．これは，攻撃者の振る舞いが暗号文の有無によって変化しないことが意味しており，すなわち，攻撃者が暗号解読を行う上で暗号文自体から有益な情報を一切得ることが出来ていないことを示唆している．このように，SS は平文秘匿性を直接的に捉えた安全性定義であり，SS のもとで安全性証明可能な公開鍵暗号方式を用いることで平文に関する情報が一切漏えいされないことを保証できる．しかしながら，SS は複雑な安全性定義であり，そのような安全性定義のもとでの安全性証明は必ずしも容易ではない．それに対し，Goldwasser と Micali は，IND に基づく平文秘匿性の定義も併せて提案し，同時にこれら両定義が等価であることを明らかにした．そのため，実際には SS のもとで直接安全性証明を行わなくとも，IND に基づく証明を行えば十分となり，平文秘匿性については，現在まで IND に基づき議論がなされている．しかしながら，匿名 IBE においては，上記のような議論を経ずに始めから IND に基づく安全性定義が利用され，SS との関係が議論されてこなかったばかりか，SS に基づく定義が明示的に与えられたのはごく最近となっている [18]．そのため，既存の匿名 IBE において，**暗号文から受信者 ID が洩れていないことが必ずしも保証されない．**

1.2 貢献

上記の状況を鑑み，IND に基づく従来の匿名性定義（Ano-LOR）[1], [4] に対し，[18] において，著者らは SS に基づく匿名性定義（Ano-SS）を新たに提案し，Ano-SS が Ano-LOR を包含することを示すことなどにより定義の妥当性を明らかにした．本稿では，Ano-LOR が Ano-SS を包含することを明らかにする．これにより，**従来の匿名性定義である Ano-LOR を満足していれば，暗号文から受信者 ID が一切漏れていないことを直接的に捉えた Ano-SS も満足していることが自動的に証明される．**したがって，従来の安全性定義により安全性が証明された既存方式の匿名性がそのまま保証されるだけでなく，今後提案がなされる匿名 IBE についても，従来同様に Ano-LOR に基づく簡便な安全性証明を行うことが可能となる．

なお，本成果は，Goldwasser と Micali の手法 [14] を匿名 IBE の文脈に単純に適用しただけでは得ることが困難であり，非自明な解析的議論のもとで初めて明示されたものとなっている．具体的には，本結果を証明する過程において，「攻撃者が暗号文を与えられたとしても，そこから受信者 ID を特定することが不可能である」ことを示す必要が生じる．これは，一見，「IBE の匿名性を証明するためには，IBE の匿名性を証明する必要がある」ことを意味しており，そのような証明は極めて困難に思われる．本研究においては，この部分についても適切にゲームホップを分解し，それらのステップ間における攻撃成功確率の差を慎重に評価することで初めて証明の完成に成功している（この部分は本稿の 4.2 節に対応する）．本結果は，Ano-SS と Ano-LOR が等価であることを単に示すだけでなく，各々の文脈において，IND および SS に基づく定義が仮に等価であったとしてもその証明が容易とは限らないこと示唆しており，場合によっては，証明できないことも十分にありうることを暗示するものと考えられる．

1.3 関連研究

IBE は，Shamir [22] によって提唱がなされ，境ら [23]，Boneh ら [5]，Cocks [11] により独立に，具体的な方式の提案がなされている．特に，Boneh らは，IBE における平文秘匿性についての定義を与えており，これが今日まで標準的に利用されている．Boneh らの定義は，IND に基づくものであり，したがって SS に基づく安全性について，当初は厳密に議論がなされていなかったが，後に Attrapadung ら [2] により，両定義の等価性が示されている．また，後に Izabachene ら [16] により，多様な平文秘匿性の定義やそれらの関係について議論がなされている．IBE の匿名性については，Abdalla ら [1] により IND に基づく定義（Ano-LOR）がなされている．しかしながら，それ以降，安全性定義に関する深い検討はあまり行われておらず，特に SS に基づく定義の具体的な定式化や，IND に基づく定義との関連についてはよくわかっていなかった．また，Boneh ら [7] は，IBE の上位概念である関数暗号 [17], [24] においては，IND および SS に基づく安全性定義が等価でない可能性を示唆している．大友ら [21] は，IBE の匿名性について新たないくつかの定義を行い，それらと既存の定義の関係について議論を行っている．なお，大友らの定義はいずれも IND に基づくものであり，SS に基づくものではない．Wee [25] は，関数暗号の匿名性について SS に基づく定義を行い，この安全性を満足する方式を提案している．小松ら [18] は，Wee の定義をもとに SS に基づく IBE の匿名性（Ano-SS）を定義し，Ano-SS が Ano-LOR を包含することを示している．

2. ID ベース鍵カプセル化メカニズム

本章では，本論文における基本的な記法について述べた後，ID ベース鍵カプセル化メカニズム（IB-KEM）のシンタックスと正当性，そして IB-KEM の強秘匿平文秘匿性の IND-ID-CPA 安全性を定義する．本論文では議論の簡潔化のため IB-KEM を用いるが，IB-KEM は適切な共通鍵暗号を組み合わせることで IBE に変換可能である．

2.1 基本的な記法

本稿において $x \leftarrow Y$ と書くとき，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．$\mathbb{N}$ を自然数の集合，$\mathbb{R}$ を実数の集合とするとき，関数 $\epsilon : \mathbb{N} \to \mathbb{R}$ 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 $\epsilon(k) < k^{-c}$ が成立するとき $\epsilon(k)$ は k に関して無視できるという．

2.2 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．

2.3 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とき，$\Pr[kem = D(usk_{id}, ct)] = 1$ が成立することをいう．

2.4 IND-ID-CPA 安全

本節では，IB-KEM の平文についての安全性定義である IND-ID-CPA について述べる．IBE において，暗号文から平文についての情報を一切得られないという安全性である強秘匿平文秘匿性を直接的に捉えた安全性定義として SS-ID-CPA が存在する．また，識別不可能性に基づいて定式化された安全性定義を IND-ID-CPA と呼び，この 2 つの定義は等価関係であることが [2] において既に明らかにされている．本節の定義は [2] における IND-ID-CPA を IB-KEM における IND-ID-CPA に書き換えたものである．

当該定義は確率的多項式時間攻撃者（PPT 攻撃者）$C = (C_1, C_2)$ と挑戦者の下記のようなゲームにより定式化される．$b \in \{0, 1\}$ とするとき，IND-ID-CPA-b という試行を考える．

$$
\begin{aligned}
&\underline{Exp^{\text{IND-ID-CPA-}b}_{\Sigma,C}(k)} \\
&(prm, msk) \leftarrow S(1^k); \\
&(id^*, s) \leftarrow C_1^{K(msk,\cdot)}(prm); \\
&(ct, kem) \leftarrow E(id^*, prm); \\
&kem_0 = kem;\ kem_1 \leftarrow \mathcal{K}; \\
&b' \leftarrow C_2^{K(msk,\cdot)}(ct, kem_b, s);
\end{aligned}
$$

鍵生成オラクル $K(msk, \cdot)$ は msk と任意の ID id を入力とし，id と紐づいたユーザー秘密鍵 usk_{id} を出力する．C_1 は $K(msk, \cdot)$ にクエリした id を id^* として出力することはできない．また，C_2 が id^* をクエリしたとき，$\perp$ が返される．IND-ID-CPA 攻撃者 C の優位性 $Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k)$ は次のように定義される．

$$
Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k) := \left| \begin{array}{c} \Pr[\ Exp^{\text{IND-ID-CPA-0}}_{\Sigma,C}(k) \to 1\ ] \\ -\Pr[\ Exp^{\text{IND-ID-CPA-1}}_{\Sigma,C}(k) \to 1\ ] \end{array} \right|
$$

定義 1. いかなる PPT 攻撃者 $C = (C_0, C_1)$ に対しても，無視できる $\epsilon(k)$ が存在し，$Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k) \leq \epsilon(k)$ が成立するならば，IB-KEM Σ は IND-ID-CPA 安全である．

3. 匿名性定義

本章では IB-KEM における匿名性の定義として，Ano-LOR と Ano-SS の 2 つの安全性定義について述べる．Ano-LOR は識別不可能性に基づいた定義であり，定義が強秘匿匿名性を意味しているかを直接判断することはできない．Ano-SS は強秘匿匿名性を直接的に捉えた定義として [18] で提案されている．以下，各定義についての詳細を述べる．

3.1 Ano-LOR 安全

Ano-LOR は攻撃者が任意に ID を 2 つ選びそのどちらかを使用して暗号化した (ct, kem) を受け取ったとき，どちらの ID を用いた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．当該安全性は，PPT 攻撃者 $B = (B_1, B_2)$ と挑戦者のゲームによって定義される．以下，$Exp^{\text{LOR-}b}_{\Sigma,B}(k)$ という試行を考える．

$\underline{Exp^{\text{LOR-}b}_{\Sigma,B}(k)}$
$(prm, msk) \leftarrow S(1^k);$
$(id_0, id_1, s) \leftarrow B_1^{K(msk,\cdot)}(prm);$
$(ct, kem) \leftarrow E(id_b, prm);$
$b' \leftarrow B_2^{K(msk,\cdot)}(ct, kem, s);$

鍵生成オラクル $K(msk,\cdot)$ は msk と任意の ID id を入力とし，id と紐づいたユーザー秘密鍵 usk_{id} を出力する．B_1 は $K(msk,\cdot)$ にクエリした id を id_0 または id_1 として出力することはできない．また，B_2 が id_0 または id_1 を $K(msk,\cdot)$ にクエリしたとき，$\perp$ が返される．Ano-LOR 攻撃者 B の優位性 $Adv^{\text{LOR}}_{\Sigma,B}(k)$ を次のように定義する．

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

定義 2. いかなる多項式確率時間攻撃者 $B = (B_0, B_1)$ に対しても，無視できる $\epsilon(k)$ が存在し，$Adv^{\text{LOR}}_{\Sigma,B}(k) \leq \epsilon(k)$ が成立するならば，IB-KEM Σ は Ano-LOR 安全である．

3.2 Ano-SS 安全

[18] において定義された Ano-SS は IB-KEM の強秘匿匿名性を直接的に捉えた安全性定義である．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．IB-KEM $\Sigma = (S, K, E, D)$ を用いて暗号化が行われる REAL 環境での試行 $Exp^{\text{SS-REAL}}_{\Sigma,A}(k)$ と，シミュレータ $\Sigma^* = (S^*, K^*, E^*)$ を使用する IDEAL 環境での試行 $Exp^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,A}(k)$ を考える．

$\underline{Exp^{\text{SS-REAL}}_{\Sigma,A}(k)}$	$\underline{Exp^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,A}(k)}$
$(prm, msk) \leftarrow S(1^k);$	$(prm, msk) \leftarrow S^*(1^k);$
$(id^*, s) \leftarrow A_1^{K(msk,\cdot)}(prm);$	$(id^*, s) \leftarrow A_1^{K^*(msk,\cdot)}(prm);$
$(ct, kem) \leftarrow E(prm, id^*);$	$ct \leftarrow E^*(msk);\ kem' \leftarrow \mathcal{K};$
$v \leftarrow A_2^{K(msk,\cdot)}(ct, kem, s);$	$v \leftarrow A_2^{K^*(msk,\cdot)}(ct, kem', s);$

鍵生成オラクル $K(msk,\cdot)$ とシミュレータ $K^*(msk,\cdot)$ は msk と任意の ID id を入力とし，id と紐づいたユーザー秘密鍵 usk_{id} を出力する．A_1 は，鍵生成オラクルへクエリした ID をターゲット ID id^* にすることはできない．また，A_2 が id^* を $K(msk,\cdot)$ にクエリすると，$\perp$ が返される．Ano-SS 攻撃者 A の優位性 $Adv^{\text{SS}}_{\Sigma,\Sigma^*,A}(k)$ を次のように定義する．

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

定義 3. いかなる PPT 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，$Adv^{\text{SS}}_{\Sigma,\Sigma^*,A}(k) \leq \epsilon(k)$ が成立するならば，IB-KEM Σ は Ano-SS 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．REAL 環境では，攻撃者が選択した ID である id^* を用いて作成した (ct, kem) を攻撃者に与える．IDEAL 環境では，シミュレータが id^* を知らずに (ct, kem') を作成しているため，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，id^* の情報は A に漏れていないといえる．

4. 定義の関係性

本章では，Ano-LOR が Ano-SS を包含することの証明を行う．本証明においては，図 1 に示されるようなシミュレータを構成することで，Ano-LOR を満足する IBE が，常に Ano-SS を満足することを示す．証明は図 2 に示されるゲーム変換列に沿って行う．この際，Game 0 から 3 までの変換における攻撃成功確率の差は標準的な手法で素朴に導出可能である．一方，Game 3 から 4 への変換における攻撃成功確率の差は，暗号文 ct からその受信者 ID である id_1 を導出することに成功する確率で評価がなされるため，いわば，IBE の匿名性を証明するために IBE の匿名性を必要とするような状況となり非自明となる．そこで，本証明は，Game 0 から 3 までの変換部分と，Game 3 から 4 への変換部分に分け，前者を 4.1 節，後者を 4.2 節に述べる．

定理 1. IB-KEM Σ が Ano-LOR 安全性かつ IND-ID-CPA 安全性を満たすとき，Σ は Ano-SS 安全性を満たす．

証明． ある IB-KEM $\Sigma = (S, K, E, D)$ に対し，いかなる Ano-LOR 攻撃者 $B = (B_1, B_2)$ に対しても無視できる $\epsilon_B(k)$ が存在し，$Adv^{\text{LOR}}_{\Sigma,B}(k) \leq \epsilon_B(k)$ で，かつ，いかなる IND-ID-CPA 攻撃者 $C = (C_1, C_2)$ に対しても，無視できる $\epsilon_C(k)$ が存在し，$Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k) \leq \epsilon_C(k)$ ならば，Σ に対し，いかなる Ano-SS 攻撃者 $A = (A_1, A_2)$ に対しても無視できる $\epsilon_A(k)$ が存在し，シミュレータ $\Sigma^* = (S^*, K^*, E^*)$ が存在し，$Adv^{\text{SS}}_{\Sigma,\Sigma^*,A}(k) \leq \epsilon_A(k)$ であることをゲーム列を用いて示す．

まず，SS ゲームにおけるシミュレータ Σ^* を図 1 のように構成する．

次に，Ano-SS ゲームを図 2 のように変形させていく．

Game 0 通常の SS-REAL ゲームで，攻撃者 A_1 によって選ばれた id_0 をターゲット ID とする．ただし，A_1 が鍵生成オラクル $K(msk,\cdot)$ にクエリした ID をターゲット ID id_0 とすることはできない．また，A_2 が $K(msk,\cdot)$ に id_0 がクエリした場合，$\perp$ が返される．

Game 1 Game 0 において，A_1 の直後に ID 空間 $\mathcal{ID}$ からランダムに ID を 1 つ選ぶ操作 $id_1 \leftarrow \mathcal{ID}$ を追加す

$\underline{S^*(1^k)}$ $(prm, msk) \leftarrow S(1^k)$ $output\ (prm, msk)$	$\underline{E^*(msk)}$ $id_1 \leftarrow \mathcal{ID}$ $(ct, kem) \leftarrow E(id_1, prm)$ $output\ ct$
$\underline{K^*(msk, \cdot)}$ $usk_{id'} \leftarrow K(msk, \cdot)$ $output\ usk_{id'}$	

図 1 シミュレータの構成

Game 0 $(prm, msk) \leftarrow S(1^k)$; $(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$; $(ct, kem) \leftarrow E(prm, id_0)$; $v \leftarrow A_2^{K(msk,\cdot)}(ct, kem, s)$;	Game 1 $(prm, msk) \leftarrow S(1^k)$; $(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}}(prm)$; $id_1 \leftarrow \mathcal{ID}$; $(ct, kem) \leftarrow E(prm, id_0)$; $v \leftarrow A_2^{\overline{K(msk,\cdot)}}(ct, kem, s)$;
Game 2 $(prm, msk) \leftarrow S(1^k)$; $(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}}(prm)$; $id_1 \leftarrow \mathcal{ID}$; $(ct, kem) \leftarrow E(prm, id_1)$; $v \leftarrow A_2^{\overline{K(msk,\cdot)}}(ct, kem, s)$;	Game 3 $(prm, msk) \leftarrow S(1^k)$; $(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}}(prm)$; $id_1 \leftarrow \mathcal{ID}$; $(ct, kem) \leftarrow E(prm, id_1)$; $kem' \leftarrow \mathcal{K}$; $v \leftarrow A_2^{\overline{K(msk,\cdot)}}(ct, kem', s)$;
Game 4 $(prm, msk) \leftarrow S^*(1^k)$; $(id_0, s) \leftarrow A_1^{K^*(msk,\cdot)}(prm)$; $ct \leftarrow E^*(msk)$; $kem' \leftarrow \mathcal{K}$; $v \leftarrow A_2^{K^*(msk,\cdot)}(ct, kem', s)$;	

図 2 ゲームの変換

る．A_1 の鍵生成オラクル $\overline{K(msk,\cdot)}$ へのクエリ条件は Game 0 と同様である．A_2 が $\overline{K(msk,\cdot)}$ に id_0 または id_1 をクエリした場合，$\perp$ が返される．

Game 2 Game 1 において，ターゲット ID を id_0 から id_1 に変更する．鍵生成オラクル $\overline{K(msk,\cdot)}$ が $\perp$ を返す条件は Game 1 と同様である．

Game 3 Game 2 において，$(ct, kem) \leftarrow E(prm, id_1)$ の直後に鍵空間 $\mathcal{K}$ からランダムに kem を 1 つ選ぶ操作 $kem' \leftarrow \mathcal{K}$ を追加し，A_2 へ入力される kem を kem' に変更する．鍵生成オラクル $\overline{K(msk,\cdot)}$ が $\perp$ を返す条件は Game 1 と同様である．

Game 4 通常の SS-IDEAL ゲームで，シミュレータ Σ^* は図 1 で示したものが実行される．鍵生成オラクル $K^*(msk,\cdot)$ は Game 0 と同じく，id_0 をクエリしたときのみ $\perp$ が返される．

以降，Game i において 1 が出力される確率を $\Pr[G_i]$ と表記する．Game 0 は通常の SS-REAL ゲームであるので，$\Pr[G_0] = \Pr[Exp^{\text{SS-REAL}}_{\Sigma,A}(k) \to 1]$ である．このとき，4.1 節および 4.2 節に記載の命題 1〜4 より，

$$\begin{aligned} Adv^{\text{SS}}_{\Sigma,\Sigma^*,A}(k) &= \left| \begin{array}{c} \Pr[\ Exp^{\text{SS-REAL}}_{\Sigma,A}(k) \to 1\ ] \\ -\Pr[\ Exp^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,A}(k) \to 1\ ] \end{array} \right| \\ &= \big|\Pr[G_0] - \Pr[G_4]\big| \\ &\le \big|\Pr[G_0] - \Pr[G_1]\big| + \big|\Pr[G_1] - \Pr[G_2]\big| \\ &\quad + \big|\Pr[G_2] - \Pr[G_3]\big| + \big|\Pr[G_3] - \Pr[G_4]\big| \\ &\le \frac{q}{|\mathcal{ID}|} + Adv^{\text{LOR}}_{\Sigma,B}(k) \\ &\quad + Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k) + \frac{2q}{|\mathcal{ID}|} + Adv^{\text{LOR}}_{\Sigma,D}(k) \end{aligned}$$

が得られる．なお，q はセキュリティパラメータに関する多項式程度で，ID は指数的なので $\frac{q}{|\mathcal{ID}|}$ は無視できる値である．よって，IB-KEM Σ が Ano-LOR 安全性かつ IND-ID-CPA 安全性を満たすとき，Σ は Ano-SS 安全性を満たす． □

4.1 命題 1 から 3 の証明

命題 1. $\big|\ \Pr[G_0] - \Pr[G_1]\ \big| \le \frac{q}{|\mathcal{ID}|}$

証明． Game 1 は Game 0 において $id_1 \leftarrow \mathcal{ID}$ を追加しているが，id_1 は A には一切入力されていない．つまり，id_1 は A から情報理論的に隠されている．Game 0 では $K(msk,\cdot)$ で id_1 がクエリされたとき usk_{id_1} を返す．一方，Game 1 では $\overline{K(msk,\cdot)}$ で id_1 がクエリされたとき $\perp$ を返すよう変更されている．id_1 は A から情報理論的に隠されていることから，A が鍵生成オラクルへ最大 q 回クエリするとき id_1 をクエリする確率は $\frac{q}{|\mathcal{ID}|}$ であるので，

$$\big|\ \Pr[G_0] - \Pr[G_1]\ \big| \le \frac{q}{|\mathcal{ID}|}$$

が得られる． □

命題 2. $\big|\ \Pr[G_1] - \Pr[G_2]\ \big| = Adv^{\text{LOR}}_{\Sigma,B}(k)$

証明． Game 1 において 1 が出力される確率 $\Pr[G_1]$ と Game 2 において 1 が出力される確率 $\Pr[G_2]$ の差が，$Adv^{\text{Ano-LOR}}_{\Sigma,B}(k)$ で抑えられることを示す．IB-KEM Σ において，Ano-LOR-b ゲームを考えたとき，Ano-LOR 攻撃者 $B = (B_1, B_2)$ が A を内部で以下のように利用した場合を考える．

$\underline{B_1^{K(msk,\cdot)}(prm)}$	$\underline{B_2^{K(msk,\cdot)}(ct, kem, s)}$
$(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}}(prm)$	$v \leftarrow A_2^{\overline{K(msk,\cdot)}}(ct, kem, s)$
$id_1 \leftarrow \mathcal{ID}$	$v = 0 \to b' = 0$
	$v = 1 \to b' = 1$
$output\ (id_0, id_1, s)$	$output\ b'$

B_1, B_2 はそれぞれ，A_1，A_2 の鍵生成クエリを $K(msk,\cdot)$

を用いてシミュレートする．このとき，内部で動く A に対しては id_0 または id_1 がクエリされたとき，$\perp$ が返される．つまり，B_2 よりも A_2 のほうが鍵生成オラクルへのクエリ条件が厳しいことから，B_1，B_2 は A_1，A_2 の鍵生成クエリをシミュレート可能である．

Ano-LOR-0 ゲームにおいて，B が 1 を出力するのは，内部で利用している A_2 が id_0 についての (ct, kem) を受け取っている状態で $v = 1$ を出力する場合である．これは Game 1 で 1 が出力される場合と等価なので，

$$\Pr[Exp^{\text{LOR-0}}_{\Sigma,B}(k) \to 1] = \Pr[G_1]$$

である．

Ano-LOR-1 において，B が 1 を出力するのは，内部で利用している A_2 が id_1 についての (ct, kem) を受け取っている状態で $v = 1$ を出力する場合である．つまり，Game 2 で 1 が出力される場合と等価である．よって，

$$\Pr[Exp^{\text{LOR-1}}_{\Sigma,B}(k) \to 1] = \Pr[G_2]$$

以上より，

$$\begin{aligned}\big|\Pr[G_1] - \Pr[G_2]\ \big| &\le \left| \begin{array}{c} \Pr\left[\ Exp^{\text{LOR-0}}_{\Sigma,B}(k) \to 1\ \right] \\ -\Pr\left[\ Exp^{\text{LOR-1}}_{\Sigma,B}(k) \to 1\ \right] \end{array} \right| \\ &= Adv^{\text{LOR}}_{\Sigma,B}(k)\end{aligned}$$

が得られる． □

命題 3. $\big|\ \Pr[G_2] - \Pr[G_3]\ \big| = Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k)$

証明． Game 2 において 1 が出力される確率 $\Pr[G_2]$ と，Game 3 において 1 が出力される確率 $\Pr[G_3]$ との差が，$Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k)$ で抑えられることを示す．

IB-KEM Σ において，IND-ID-CPA-b ゲームを考えたとき，IND-ID-CPA 攻撃者 $C = (C_1, C_2)$ が A を内部で以下のように利用した場合を考える．

$\underline{C_1^{K(msk,\cdot)}(prm)}$	$\underline{C_2^{K(msk,\cdot)}(ct, kem_b, s)}$
$(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}}(prm)$	$v \leftarrow A_2^{\overline{K(msk,\cdot)}}(ct, kem_b, s)$
$id_1 \leftarrow \mathcal{ID}$	$v = 0 \to b' = 0$
$output\ (id_1, s)$	$v = 1 \to b' = 1$
	$output\ b'$

C_1，C_2 はそれぞれ，A_1，A_2 の鍵生成クエリを $K(msk, \cdot)$ を用いてシミュレートする．このとき，内部で動く A_2 に対しては id_0 または id_1 がクエリされたとき，$\perp$ が返される．つまり，C_2 よりも A_2 のほうが鍵生成オラクルへのクエリ条件が厳しいことから，C_1，C_2 は A_1，A_2 の鍵生成クエリをシミュレート可能である．IND-ID-CPA-0 において，C が 1 を出力するのは，id_1 によって生成された (ct, kem) を受け取った A_2 が $v = 1$ を出力したときである．これは Game 2 と一致する．つまり，

$$\Pr[Exp^{\text{IND-ID-CPA-0}}_{\Sigma,C}(k) \to 1] = \Pr[G_2]$$

IND-ID-CPA-1 において，C が 1 を出力するのは，id_1 によって生成された ct とランダムに選択された kem' の組を受け取った A_2 が $v = 1$ を出力したときである．これは Game 3 と一致する．つまり，

$$\Pr[Exp^{\text{IND-ID-CPA-1}}_{\Sigma,C}(k) \to 1] = \Pr[G_3]$$

したがって，

$$\begin{aligned}\big|\Pr[G_2] - \Pr[G_3]\big| &\le \left| \begin{array}{c} \Pr\left[\ Exp^{\text{IND-ID-CPA-0}}_{\Sigma,C}(k) \to 1\ \right] \\ -\Pr\left[\ Exp^{\text{IND-ID-CPA-1}}_{\Sigma,C}(k) \to 1\ \right] \end{array} \right| \\ &= Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k)\end{aligned}$$

よって，$\big|\Pr[G_2] - \Pr[G_3]\big| = Adv^{\text{IND-ID-CPA}}_{\Sigma,C}(k)$ が得られる． □

4.2 命題 4 の証明

上述の通り、Game 3 から 4 への変換における攻撃成功確率の差は、暗号文 ct からその受信者 ID である id_1 を導出することに成功する確率で評価される。この確率は、IBE の匿名性を破る攻撃成功確率そのものと考えられるため、一見、導出が困難と思われる。しかし、本証明においては、IBE の（Ano-SS 安全性ではなく）Ano-LOR 安全性を仮定しているため、こちらの匿名性への帰着を目指すことで証明を完成させる。そこで、Game 3 から 4 への変換を、さらに、図 3 に示すゲーム変換列に分解し、これに沿って Game 3 から 4 への変換における攻撃成功確率の差を導出する。

命題 4. 攻撃者 A に対して，ある Ano-LOR 攻撃者 D が存在して，$\big|\ \Pr[G_3] - \Pr[G_4]\ \big| \le \frac{2q}{|\mathcal{ID}|} + Adv^{\text{LOR}}_{\Sigma,D}(k)$

証明． Game 4 は SS-IDEAL ゲームである．内部で動くシミュレータ Σ^* は**図 1** のように動作している．Game 4 に図 1 のシミュレータを代入したゲームを Game 4′ とすると，Game 4′ は Game 4 にシミュレータを代入しただけなので，$\Pr[G_{4'}] = \Pr[G_4]$ である．以降，$\Pr[G_3]$ と $\Pr[G_{4'}]$ の差について考える．この二つのゲームの違いは，鍵生成オラクルにおける条件である．Game 3 では id_1 がクエリされたとき $\perp$ を出力するのに対し，Game 4′ では id_1 がクエリされたとき usk_{id_1} を出力する．つまり，A_2 によって鍵生成オラクルへ id_1 がクエリされたときにゲームの差が生じる．どちらのゲームにおいても攻撃者 A は id_1 についての ct を受け取っているので，A_2 が鍵生成オラクルへ id_1 をクエリする確率が無視できるほど小さい値で抑えられるならば，$\Pr[G_3]$ と $\Pr[G_{4'}]$，すなわち，$\Pr[G_3]$ と $\Pr[G_4]$ の差は無視できるほど小さいことが示せる．ここで，Game i において id_1 がクエリされる確率を $\Pr[F_i]$ とする．攻撃者 A に対して，ある Ano-LOR 攻撃者 D が存在するとき，$\big|\ \Pr[G_3] - \Pr[G_{4'}]\ \big| \le \Pr[F_3] \le \frac{2q}{|\mathcal{ID}|} + Adv^{\text{LOR}}_{\Sigma,D}(k)$ を示せ

ばよい．

まず，Game 3 を図 3 のように変形する．

Game 3	Game 3-1
$(prm, msk) \leftarrow S(1^k)$;	$(prm, msk) \leftarrow S(1^k)$;
$(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}}(prm)$;	$(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}}(prm)$;
$id_1 \leftarrow \mathcal{ID}$;	$id_1 \leftarrow \mathcal{ID}$;
	$id_2 \leftarrow \mathcal{ID}$;
$(ct, kem) \leftarrow E(prm, id_1)$;	$(ct, kem) \leftarrow E(prm, id_1)$;
$kem' \leftarrow \mathcal{K}$;	$kem' \leftarrow \mathcal{K}$;
$v \leftarrow A_2^{\overline{K(msk,\cdot)}}(ct, kem', s)$;	$v \leftarrow A_2^{\overline{K(msk,\cdot)}'}(ct, kem', s)$;
Game 3-2	
$(prm, msk) \leftarrow S(1^k)$;	
$(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}'}(prm)$;	
$id_1 \leftarrow \mathcal{ID}$;	
$id_2 \leftarrow \mathcal{ID}$;	
$(ct, kem) \leftarrow E(prm, id_2)$;	
$kem' \leftarrow \mathcal{K}$;	
$v \leftarrow A_2^{\overline{K(msk,\cdot)}'}(ct, kem', s)$;	

図 3 ゲームの変換

Game 3 $\overline{K(msk,\cdot)}$ は id_0 または id_1 がクエリされた場合，$\perp$ を返す．

Game 3-1 Game 3 において，id_1 を選んだ直後，さらに ID 空間 $\mathcal{ID}$ からランダムに ID を 1 つ選ぶ操作 $id_2 \leftarrow \mathcal{ID}$ を追加する．$\overline{K(msk,\cdot)}'$ は id_0，id_1，id_2 のいずれかがクエリされた場合，$\perp$ を返す．

Game 3-2 Game 3-1 において，ターゲット ID を id_1 から id_2 に変更する．$\overline{K(msk,\cdot)}'$ は Game 3-1 同様とする．

このとき，Game 3, Game 3-1, Game 3-2 のゲーム間における関係を明らかにし，$|\Pr[F_3] - \Pr[F_{3\text{-}2}]| \leq \frac{q}{|\mathcal{ID}|}$，すなわち A が id_1 をクエリする確率が無視できるほど小さい値であることを示す．

補題 1. $\left|\Pr[F_3] - \Pr[F_{3\text{-}1}]\right| \leq \frac{q}{|\mathcal{ID}|}$

証明． Game 3-1 において，id_2 は A に対して情報理論的に隠されている．よって，A_2 が鍵生成オラクルへ最大 q 回クエリするとき id_2 が $K(msk,\cdot)$ へクエリされる確率は $\frac{q}{|\mathcal{ID}|}$，つまり

$$|\Pr[F_3] - \Pr[F_{3\text{-}1}]| \leq \frac{q}{|\mathcal{ID}|}$$

である． □

補題 2. $|\Pr[F_{3\text{-}1}] - \Pr[F_{3\text{-}2}]| = Adv^{\mathrm{LOR}}_{\Sigma,D}(k)$

証明． Game 3-1 において id_1 がクエリされる確率 $\Pr[F_{3\text{-}1}]$ と，Game 3-2 において id_1 がクエリされる確率 $\Pr[F_{3\text{-}2}]$ との差が，ある Ano-LOR 攻撃者 D の優位性 $Adv^{\mathrm{LOR}}_{\Sigma,D}(k)$ で抑えられることを示す．Ano-LOR 攻撃者 $D = (D_1, D_2)$ が A を内部で以下のように利用する場合を考える．

$\underline{D_1^{K(msk,\cdot)}(prm)}$	$\underline{D_2^{K(msk,\cdot)}(ct, kem, s)}$
$(id_0, s) \leftarrow A_1^{\overline{K(msk,\cdot)}'}(prm)$	$kem' \leftarrow \mathcal{K}$
$id_1 \leftarrow \mathcal{ID}$	$v \leftarrow A_2^{\overline{K(msk,\cdot)}'}(ct, kem', s)$
$id_2 \leftarrow \mathcal{ID}$	$id_1 \in \mathcal{ID}' \rightarrow b' = 1$
$output\ (id_1, id_2, s)$	$id_1 \notin \mathcal{ID}' \rightarrow b' = 0$
	$output\ b'$

上記における $\mathcal{ID}'$ は，A_2 が $\overline{K(msk,\cdot)}'$ にクエリした ID の集合とする．D_2 は id_1 または id_2 を $K(msk,\cdot)$ にクエリすることを禁止されている．しかし，A_2 が id_1 または id_2 をクエリした場合は $\perp$ を返せばよいので，A_2 に対する $\overline{K(msk,\cdot)}'$ のシミュレーションは可能である．

Ano-LOR-0 において，D が 1 を出力するのは，id_1 によって生成された ct とランダムに選択された kem' の組を受け取った A_2 が id_1 を $K(msk,\cdot)'$ に対してクエリしたときである．これは $F_{3\text{-}1}$ と一致する．つまり，

$$\Pr[Exp^{\text{LOR-0}}_{\Sigma,D}(k) \rightarrow 1] = \Pr[G_{3\text{-}1}]$$

Ano-LOR-1 において，D が 1 を出力するのは，id_2 によって生成された ct とランダムに選択された kem' の組を受け取った A_2 が id_1 を $K(msk,\cdot)'$ に対してクエリしたときである．これは $F_{3\text{-}2}$ と一致する．つまり，

$$\Pr[Exp^{\text{LOR-1}}_{\Sigma,D}(k) \rightarrow 1] = \Pr[G_{3\text{-}2}]$$

したがって，

$$\left|\Pr[F_{3\text{-}1}] - \Pr[F_{3\text{-}2}]\right| \leq \left| \begin{array}{c} \Pr\left[Exp^{\text{LOR-0}}_{\Sigma,D}(k) \rightarrow 1\right] \\ -\Pr\left[Exp^{\text{LOR-1}}_{\Sigma,D}(k) \rightarrow 1\right] \end{array} \right| = Adv^{\mathrm{LOR}}_{\Sigma,D}(k)$$

□

補題 3. $\Pr[F_{3\text{-}2}] = \frac{q}{|\mathcal{ID}|}$

証明． Game 3-2 において，id_1 は A_2 に対して情報理論的に隠されている．A_2 のクエリ最大回数を q としたとき，

$$\Pr[F_{3\text{-}2}] = \frac{q}{|\mathcal{ID}|}$$

である． □

補題 1〜3 より，

$$\Pr[F_3] \leq \left|\Pr[F_3] - \Pr[F_{3\text{-}1}]\right| + \left|\Pr[F_{3\text{-}1}] - \Pr[F_{3\text{-}2}]\right| + \Pr[F_{3\text{-}2}]$$

$$\Pr[F_3] \leq \frac{q}{|\mathcal{ID}|} + Adv^{\mathrm{LOR}}_{\Sigma,D}(k) + \frac{q}{|\mathcal{ID}|}$$

よって，Game 3 において，攻撃者 A が id_1 をクエリする

確率は無視できるほど小さい値で抑えることができる．このとき，

$$\begin{aligned}\left|\Pr[G_3] - \Pr[G_{4'}]\right| &\leq \Pr[F_3] \\ &\leq \frac{2q}{|\mathcal{ID}|} + Adv^{\mathrm{LOR}}_{\Sigma,D}(k)\end{aligned}$$

$\Pr[G'_4] = \Pr[G_4]$ より，

$$\left|\Pr[G_3] - \Pr[G_4]\right| \leq \frac{2q}{|\mathcal{ID}|} + Adv^{\mathrm{LOR}}_{\Sigma,D}(k)$$

□

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] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, Haixia Shi: Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. CRYPTO 2005: 205-222.

[2] Nuttapong Attrapadung, Yang Cui, David Galindo, Goichiro Hanaoka, Ichiro Hasuo, Hideki Imai, Kanta Matsuura, Peng Yang, Rui Zhang: Relations Among Notions of Security for Identity Based Encryption Schemes. LATIN 2006: 130-141.

[3] Olivier Blazy, Laura Brouilhet, Duong Hieu Phan: Anonymous Identity Based Encryption with Traceable Identities. ARES 2019: 13:1-13:10.

[4] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano: Public Key Encryption with Keyword Search. EUROCRYPT 2004: 506-522.

[5] Dan Boneh, Matthew K. Franklin: Identity-Based Encryption from the Weil Pairing. CRYPTO 2001: 213-229.

[6] Dan Boneh, Ben Lynn, Hovav Shacham: Short Signatures from the Weil Pairing. ASIACRYPT 2001: 514-532.

[7] Dan Boneh, Amit Sahai, Brent Waters: Functional Encryption: Definitions and Challenges. TCC 2011: 253-273.

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

[9] Ran Canetti, Shai Halevi, Jonathan Katz: Chosen-Ciphertext Security from Identity-Based Encryption. EUROCRYPT 2004: 207-222.

[10] Jan Camenisch, Markulf Kohlweiss, Alfredo Rial, Caroline Sheedy: Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data. Public Key Cryptography 2009: 196-214.

[11] Clifford C. Cocks: An Identity Based Encryption Scheme Based on Quadratic Residues. IMA Int. Conf. 2001: 360-363.

[12] Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, Moti Yung: Key-Insulated Public Key Cryptosystems. EUROCRYPT 2002: 65-82.

[13] Chun-I Fan, Yi-Fan Tseng: Anonymous Multi-Receiver Identity-Based Authenticated Encryption with CCA Security. Symmetry 7(4): 1856-1881 (2015).

[14] Shafi Goldwasser, Silvio Micali: Probabilistic Encryption. J. Comput. Syst. Sci. 28(2): 270-299 (1984).

[15] Kai He, Jian Weng, Jianan Liu, Joseph K. Liu, Wei Liu, Robert H. Deng: Anonymous Identity-Based Broadcast Encryption with Chosen-Ciphertext Security. AsiaCCS 2016: 247-255.

[16] Malika Izabachène, David Pointcheval: New Anonymity Notions for Identity-Based Encryption. SCN 2008: 375-391.

[17] Jonathan Katz, Amit Sahai, Brent Waters: Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. EUROCRYPT 2008: 146-162.

[18] 小松みさき，山田翔太，坂井祐介，花岡悟一郎: ID ベース暗号の強秘匿匿名性について． コンピュータセキュリティシンポジウム 2018.

[19] Takahiro Matsuda, Yasumasa Nakai, Kanta Matsuura: Efficient Generic Constructions of Timed-Release Encryption with Pre-open Capability. Pairing 2010: 225-245.

[20] Xuecheng Ma, Xin Wang, Dongdai Lin: Anonymous Identity-Based Encryption with Identity Recovery. ACISP 2018: 360-375.

[21] 大友萌夢，佐々木太良，藤岡淳: ID ベース暗号の匿名性定義の関係 〜CCA2 の場合〜．暗号と情報セキュリティシンポジウム 2018.

[22] Adi Shamir: Identity-Based Cryptosystems and Signature Schemes. CRYPTO 1984: 47-53.

[23] 境隆一，大岸聖史，笠原正雄: Cryptosystems Based on Pairing. 暗号と情報セキュリティシンポジウム 2000.

[24] Amit Sahai, Brent Waters: Fuzzy Identity-Based Encryption. EUROCRYPT 2005: 457-473.

[25] Hoeteck Wee: Attribute-Hiding Predicate Encryption in Bilinear Groups, Revisited. TCC (1) 2017: 206-233.

[26] Peng Xu, Jingnan Li, Wei Wang, Hai Jin: Anonymous Identity-Based Broadcast Encryption with Constant Decryption Complexity and Strong Security. AsiaCCS 2016: 223-233.