SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

任意の頑強な ID ベース暗号に基づく CCA 安全な公開鍵暗号の効率的構成方法
Simple CCA-Secure Public Key Encryption from Any Non-Malleable ID-based Encryption

松田 隆宏 * 花岡 悟一郎 † 松浦 幹太 * 今井 秀樹 †
Takahiro Matsuda Goichiro Hanaoka Kanta Matsuura Hideki Imai

あらまし 本稿では、頑強性を持つ ID ベース暗号から CCA 安全性を持つ公開鍵暗号の構成法を示す。2005 年に提案された Boneh と Katz による方法 (BK 変換) では、構成要素として MAC と特殊なコミットメント方式が必要であり、暗号文サイズの変換によるオーバーヘッドが 704 ビット程度生じてしまう。これに対し本稿で提案する方法では、ID ベース暗号に従来の変換で用いられる識別不可能性よりも強い頑強性を仮定することで、構成要素は、一方向性及びターゲット衝突困難性を同時に満たす一つのハッシュ関数のみとでき、暗号文サイズのオーバーヘッドは 256 ビット程度である。これまで、安全性の帰着をある種の暗号方式の頑強性に帰着させるような方式はあまり提案されていないが、本稿での証明は、新しい証明技法として、他の暗号技術の安全性をある種の暗号方式の頑強性へと帰着する必要がある場合に有用な可能性がある。

キーワード 公開鍵暗号、ID ベース暗号、IND-CCA 安全性、頑強性、NM-sID-CPA 安全性

1 はじめに

効率的な選択暗号文攻撃 (CCA) に対する安全性を持つ公開鍵暗号方式 (Public Key Encryption, PKE) の構成法についての研究は、暗号研究の分野の一つの主流となっている。その中で一つのパラダイムとして、選択平文攻撃 (CPA) に対する安全性しか持たない様な ID ベース暗号 (Identity-based Encryption, IBE) から CCA 安全性を持つ PKE を構成しようとする IBE-PKE 変換の研究が近年盛んである。

IBE-PKE 変換 2004 年に Canetti ら [6] により、CPA 安全な任意の IBE を用いた PKE への一般的構成方法が提案された (CHK 変換)。この構成法は One-Time 署名を用いるものであり、暗号文サイズ及び暗号文作成の際の計算コストのオーバーヘッドが大きい。その後、One-Time 署名のオーバーヘッドを改善するため、2005 年に Boneh ら [4] は MAC と特殊なコミットメント方式 (実体はターゲット衝突困難ハッシュ関数及び汎用ハッシュ関数 (Universal Hash Function)) を用いた構成法を提案した (BK 変換)。しかし、Leftover Hash Lemma [8] を用いるため、大きなサイズの乱数を用いる必要があり、暗号文作成の計算コストのオーバーヘッドは改善されるものの、依然として暗号文サイズのオーバーヘッドは大きい (128 ビット安全性を得るためにおよそ 704 ビット)。IBE の構成に対し一般性を犠牲にすることで、さらなる効率性を目指した研究もある [5, 1, 9]。以上の研究において共通していることは、IBE に選択平文攻撃に対する識別不可能性 (IND-(s)ID-CPA) を仮定している点である。

IBE の頑強性 暗号方式での頑強性 (Non-Malleability, NM) とは、概略を言えば、暗号文 χ を与えられた攻撃者が、その平文 m とある関係 R を満たすことが分かる平文 m' に復号できてしまう様な暗号文 χ' を作りだすことができないという安全性の概念である。IBE において、選択平文攻撃に対する頑強性 (NM-(s)ID-CPA) と識別不可能性 (IND-(s)ID-CPA) の間には差があると考えられているが、選択暗号文攻撃に対する頑強性 (NM-(s)-ID-CCA) は、同攻撃に対する識別不可能性 (IND-(s)ID-CCA) と等価であることが示されている [2]。

本研究の成果 本稿では、識別不可能性よりも強い安全性である頑強性を持つ任意の IBE から一般的に CCA 安全な PKE を構成する方法を提案する。より具体的には、IBE において、頑強性を持つものの中で最も弱い安全性である選択的 ID 及び選択平文攻撃に対する頑強性 (NM-sID-CPA) を持つ IBE と、一方向性及びターゲット衝突困難性を同時に満たすハッシュ関数一つを用いて、CCA 安全な PKE の効率的な構成法を示し、その安全性証明を示す。残念なことに、これまで、IND-sID-CCA 以上の安全性を持っていると証明されている方式を除けば、NM-sID-CPA 安全性を持つ実用的な IBE の構成法は知られていない。しかしながら今後、NM-sID-CPA 安全性を持つと示される (あるいは仮定できる) ような効率

* 東京大学 生産技術研究所, 〒 153-8505 東京都目黒区駒場 4-6-1, Institute of Industrial Science, The University of Tokyo, 4-6-1 Komaba, Meguro-ku, Tokyo 153-8505, Japan. Email: tmatsuda@iis.u-tokyo.ac.jp
† 産業技術総合研究所 情報セキュリティ研究センター, 〒 101-0021 東京都千代田区外神田 1-18-13, Research Center for Information Security, National Institute of Advanced Industrial Science and Technology, 1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan.

的な IBE あれば、我々の構成法によりただちに効率的な CCA 安全性を持つ PKE を得ることができる。

また、現在まで、ある方式の安全性をある種の暗号の頑強性に帰着する証明は、PKE 間及び IBE 間などの安全性の定義間の関係性の議論などの研究 ([3]、[2] など) を除いては行われていない。実際の証明の構成についても、攻撃者の振舞いやシミュレータ自身のランダムコインによって、シミュレータの対応が多様に変化しており、CHK 変換や、BK 変換の安全性証明とは非常に異なった新しいものとなっている。そのため、安全性を IBE の頑強性に帰着できるような方式を証明と共に示したことも本研究の理論的な成果である。今後、暗号技術の安全性を、ある種の暗号方式の頑強性に帰着する場合は、本稿での安全性の証明技法が有用である可能性がある。

2 準備

本節では、本稿で使用する言葉や安全性の定義を行う。本稿では、$x \leftarrow y$ と書くとき、y が集合ならばそこから一様ランダムに要素を取り出し x に代入する操作を、y がアルゴリズムまたは関数ならば x を出力する操作を表す。"$x||y$" は x と y の連結を表す。

2.1 公開鍵暗号

公開鍵暗号 Π は以下の 3 つのアルゴリズムからなる。

鍵生成 PKE.KG**:** 確率的アルゴリズム。セキュリティパラメータ 1^κ を入力とし、秘密鍵 sk と公開鍵 pk の対を出力する。

暗号化 PKE.Enc**:** 確率的アルゴリズム。公開鍵 pk、平文 $m \in \mathcal{M}$ を入力とし、暗号文 $\chi \in \mathcal{X}$ を出力する。

復号 PKE.Dec**:** 決定的アルゴリズム。秘密鍵 sk、暗号文 χ を入力とし、平文 m (あるいは $\perp$) を出力する。

ただし、$\mathcal{M}$、$\mathcal{X}$ はそれぞれ、Π の平文空間、暗号文空間である。

IND-CCA 安全性　公開鍵暗号の適応的選択暗号文攻撃に対する識別不可能性 (Indistinguishability against Adaptive Chosen-Ciphertext Attacks, IND-CCA) は、以下の攻撃者 $\mathcal{A}$ と IND-CCA Challenger $\mathcal{C}$ 間の IND-CCA game を用いて定義される。

Setup. $\mathcal{C}$ は $\mathsf{PKE.KG}(1^\kappa)$ を実行する。出力された pk を $\mathcal{A}$ に渡し、sk を保持しておく。

Phase 1. $\mathcal{A}$ は Challenger に対し、q_1 回の復号クエリ $(\chi_1, \chi_2, \ldots, \chi_{q_1})$ を発行することができる。$\mathcal{C}$ はそれぞれのクエリ χ_i に対し、正しい復号結果 $m_i \leftarrow \mathsf{PKE.Dec}(sk, \chi_i)$ $(m_i \in \mathcal{M} \cup \{\perp\})$ を返す。

Challenge. $\mathcal{A}$ は 2 つの任意の平文 m_0, m_1 を選び、$\mathcal{C}$ に送る。$\mathcal{C}$ はランダムにコイン $b \in \{0, 1\}$ を振り、m_b の暗号文 $\chi^* \leftarrow \mathsf{PKE.Enc}(pk, m_b)$ を計算し、χ^* を $\mathcal{A}$ に渡す。

Phase 2. $\mathcal{A}$ は Phase 1 と同様 q_2 回の復号クエリを発行することができる。ただし、Challenge の際受け取った暗号文 χ^* を復号クエリとすることはできない。

Guess. $\mathcal{A}$ は $\mathcal{C}$ の選んだ b の予測として b' を出力する。

$q_D = q_1 + q_2$ を $\mathcal{A}$ が発行することができる復号クエリの回数とする。ここで、ある公開鍵暗号 Π における $\mathcal{A}$ の IND-CCA アドバンテージを以下の様に定義する。

$$\mathsf{Adv}^{\text{IND-CCA}}_{\Pi,\mathcal{A}} = |\Pr[b' = b] - 1/2|$$

定義 1. 復号クエリを最大 q_D 回発行する全ての動作時間 t のアルゴリズム $\mathcal{A}$ に対し、$\mathsf{Adv}^{\text{IND-CCA}}_{\Pi,\mathcal{A}} \leq \epsilon$ を満たすとき、Π は *(t,q_D,ϵ)-IND-CCA* 安全であるという。また、ϵ が無視できる値のとき、単に Π は *IND-CCA* 安全であるという。

2.2 ID ベース暗号

ID ベース暗号 Π は以下の 4 つのアルゴリズムからなる。

セットアップ IBE.Setup**:** 確率的アルゴリズム。セキュリティパラメータ 1^κ を入力とし、マスター秘密鍵 msk と公開パラメータ prm の対を出力する。

鍵導出 IBE.Ext**:** 確率的あるいは決定的アルゴリズム。公開パラメータ prm、マスター秘密鍵 msk、$\mathsf{ID} \in \mathcal{I}$ を入力とし、ID に対する復号鍵 d_{ID} を出力する。

暗号化 IBE.Enc**:** 確率的アルゴリズム。公開パラメータ prm、$\mathsf{ID} \in \mathcal{I}$、平文 $m \in \mathcal{M}$ を入力とし、暗号文 $\chi \in \mathcal{X}$ を出力する。

復号 IBE.Dec**:** 決定的アルゴリズム。復号鍵 d_{ID}、暗号文 χ を入力とし、平文 m (あるいは $\perp$) を出力する。

ただし、$\mathcal{I}$、$\mathcal{M}$、$\mathcal{X}$ はそれぞれ、Π の ID 空間、平文空間、暗号文空間である。

NM-sID-CPA 安全性　本稿で用いる IBE の NM-sID-CPA 安全性の定義は、Attrapadung ら [2] による。ID ベース暗号の選択的 ID 及び選択平文攻撃に対する頑強性 (Non-Malleability against selective-ID Chosen-Plaintext Attacks, NM-sID-CPA) は、以下の攻撃者 $\mathcal{A}$ と NM-sID-CPA Challenger $\mathcal{C}$ 間の NM-sID-CPA game を用いて定義される。

Init. $\mathcal{A}$ は初めに攻撃対象とする ID^* を宣言する。

Setup. $\mathcal{C}$ は $\mathsf{IBE.Setup}(1^\kappa)$ を実行する。出力された prm を $\mathcal{A}$ に渡し、msk を保持しておく。

Phase 1. $\mathcal{A}$ は $\mathcal{C}$ に対し、q_1 回の鍵導出クエリ $(\mathsf{ID}_1, \mathsf{ID}_2, \ldots, \mathsf{ID}_{q_1})$ を発行することができる。$\mathcal{C}$ はそれぞれのクエリ ID_i に対し、正しい復号鍵 $d_{\mathsf{ID}_i} \leftarrow \mathsf{IBE.Ext}(\mathsf{prm}, \mathsf{msk}, \mathsf{ID}_i)$ を返す。ただし、$\mathcal{A}$ は ID^* を鍵導出クエリとすることはできない。

Challenge. $\mathcal{A}$ は $\mathcal{M}^* \subset \mathcal{M}$ となるような $\mathcal{M}^*$ を選び、$\mathcal{C}$ に送る。$\mathcal{C}$ は $\mathcal{M}^*$ から一様ランダムに、m^* 及び $m^{\bar{*}}$ を選ぶ。$\chi^* \leftarrow \mathsf{IBE.Enc}(\mathsf{prm}, \mathsf{ID}^*, m^*)$ を計算し、$\mathcal{A}$ に渡す。

Phase 2. $\mathcal{A}$ は Phase 1 と同様 q_2 回の復号クエリを発行することができる。

Output. $\mathcal{A}$ は $\mathcal{C}$ の選んだ m^* とある関係 R を満たすような平文ベクトル $\overrightarrow{m}' = (m'_1, m'_2, \ldots, m'_t)$ の暗号文ベクトル $\overrightarrow{\chi}' = (\chi'_1, \chi'_2, \ldots, \chi'_t)$ $(\chi'_i \leftarrow \mathsf{IBE.Enc}(\mathsf{prm}, \mathsf{ID}^*, m'_i)_{i\in\{1,\ldots,t\}})$ とその関係 R の具体的記述を $\mathcal{C}$ に出力する[1]。$\mathcal{C}$ は $\overrightarrow{\chi}'$ を全て $\mathsf{IBE.Dec}(d_{\mathsf{ID}^*}, \cdot)$ $(d_{\mathsf{ID}^*} \leftarrow \mathsf{IBE.Ext}(\mathsf{prm}, \mathsf{msk}, \mathsf{ID}^*))$ を用いて復号し、$\overrightarrow{m}'$ を得る。

$q_E = q_1 + q_2$ を $\mathcal{A}$ が発行することができる鍵導出クエリの回数とする。$\mathsf{R}(m, \overrightarrow{\chi}')$ を $\chi^* \notin \overrightarrow{\chi}' \wedge \perp \notin \overrightarrow{m}' \wedge R(m, \overrightarrow{m}') = \mathtt{true}$ が起こるイベントと定義する。$\mathsf{R}^* := \mathsf{R}(m^*, \overrightarrow{\chi}')$、$\mathsf{R}^{\bar{*}} := \mathsf{R}(m^{\bar{*}}, \overrightarrow{\chi}')$ と定義する。ここで、ある ID ベース暗号 Π における $\mathcal{A}$ の NM-sID-CPA アドバンテージを以下の様に定義する。

$$\mathsf{Adv}^{\text{NM-sID-CPA}}_{\Pi,\mathcal{A}} = \Pr[\mathsf{R}^*] - \Pr[\mathsf{R}^{\bar{*}}]$$

定義 2. 鍵導出クエリを最大 q_E 回発行する全ての動作時間 t のアルゴリズム $\mathcal{A}$ に対し、$\mathsf{Adv}^{\text{NM-sID-CPA}}_{\Pi,\mathcal{A}} \leq \epsilon$ を満たすとき、Π は *(t,q_E,ϵ)-NM-sID-CPA* 安全であるという。また、ϵ が無視できる値のとき、単に Π は *NM-sID-CPA* 安全であるという。

2.3 ハッシュ関数

$H : \mathcal{K} \times \mathcal{M}_{in} \rightarrow \mathcal{M}_{out}$ を鍵付きハッシュ関数とする。ただし、$\mathcal{M}_{in}$、$\mathcal{M}_{out}$、$\mathcal{K}$ をそれぞれ、H の入力空間、出力空間、ハッシュ鍵空間とする。

2.3.1 一方向ハッシュ関数

攻撃者 $\mathcal{A}$ の一方向ハッシュ関数 (One-Way Hash Function, OWHF) H に対するアドバンテージを以下の様に定義する。

$$\mathsf{Adv}^{\text{OW}}_{H,\mathcal{A}} = \Pr[k \leftarrow \mathcal{K}; m \leftarrow \mathcal{M}_{in}; h \leftarrow H_k(m); m' \leftarrow \mathcal{A}(k,h) : H_k(m') = h]$$

定義 3. 全ての動作時間 t のアルゴリズム $\mathcal{A}$ に対し、$\mathsf{Adv}^{\text{OW}}_{H,\mathcal{A}} \leq \epsilon$ を満たすとき、H は *(t,ϵ)-OWHF* であるという。また、ϵ が無視できる値のとき、H を単に *OWHF* であるという。

2.3.2 ターゲット衝突困難ハッシュ関数

本稿で用いる TCRHF の定義は Cramer ら [7] による。攻撃者 $\mathcal{A}$ のターゲット衝突困難ハッシュ関数 (Target Collision Resistant Hash Function, TCRHF) H に対するアドバンテージを以下の様に定義する。

$$\mathsf{Adv}^{\text{TCR}}_{H,\mathcal{A}} = \Pr[k \leftarrow \mathcal{K}; m_1 \leftarrow \mathcal{M}_{in}; m_2 \leftarrow \mathcal{A}(k, m_1) : H_k(m_1) = H_k(m_2) \wedge m_1 \neq m_2]$$

[1] t は κ に関し多項式倍程度の大きさの自然数であり、$\mathcal{A}$ によって決められる。$t = 1$ の場合も考えることができる。その場合、R は二項関係となる。本稿では 3 節以降、R が二項関係の場合のみを取り扱っているが、ここでは一般的に記述するためにこのように記す。

定義 4. 全ての動作時間 t のアルゴリズム $\mathcal{A}$ に対し、$\mathsf{Adv}^{\text{TCR}}_{H,\mathcal{A}} \leq \epsilon$ を満たすとき、H は *(t,ϵ)-TCRHF* であるという。また、ϵ が無視できる値のとき、H を単に *TCRHF* であるという。

3 提案方式

本節では、我々の提案方式及びその安全性について議論する。

$\Pi = (\mathsf{IBE.Setup}, \mathsf{IBE.Ext}, \mathsf{IBE.Enc}, \mathsf{IBE.Dec})$ を NM-sID-CPA 安全な ID ベース暗号とする。また、$H : \mathcal{K} \times \{0,1\}^\gamma \rightarrow \mathcal{I}$ (定義域のうち $\mathcal{K}$ がハッシュ鍵空間、$\{0,1\}^\gamma$ が H の入力空間) をターゲット衝突困難性かつ一方向性を持つハッシュ関数とする。このとき公開鍵暗号方式 Π' を図 1 の様に構成する。Π' の平文空間を $\mathcal{M}_{\Pi'}$ とすると、内部の ID ベース暗号 Π の平文空間は $\mathcal{M}_\Pi$ は $\mathcal{M}_{\Pi'} \times \{0,1\}^\gamma$ となっている必要がある。

3.1 安全性

定理 1. 構成要素である Π が *(t, q_D, $\frac{1}{2q_D}(1-\epsilon_{tcr})\epsilon_{cca} - \frac{1}{4}(\epsilon_{ow} + \frac{1}{2^\gamma})$) -NM-sID-CPA* 安全な *ID* ベース暗号方式、H が (t, ϵ_{ow})-*OWHF* かつ (t, ϵ_{tcr})-*TCRHF* のとき、提案方式 Π' は *(t, q_D, ϵ_{cca})-IND-CCA* 安全な公開鍵暗号方式である。

証明 $\mathcal{A}$ を、公開鍵暗号方式 Π' の (t, q_D, ϵ_{cca}) -IND-CCA 安全性を破る攻撃者とする。すなわち、$\mathcal{A}$ は確率 $1/2 + \epsilon_{cca}$ で Π' を破るとする。このとき $\mathcal{A}$ と、(t, ϵ_{tcr})-TCRHF かつ (t, ϵ_{ow})-OWHF である H を用いて ID ベース暗号方式 Π の $(t, q_D, \frac{1}{2q_D}(1-\epsilon_{tcr})\epsilon_{cca} - \frac{1}{4}(\epsilon_{ow} + \frac{1}{2^\gamma}))$ -NM-sID-CPA 安全性を破ることができるシミュレータ $\mathcal{S}$ を構成する。一般性を失わずに、$q_D > 0$ とする。$\mathcal{S}$ は $\mathcal{A}$ に対して以下の様に IND-CCA game のシミュレートを行いつつ利用して自身の NM-sID-CPA Challenger $\mathcal{C}$ との間で NM-sID-CPA game を行う。

Setup. $\mathcal{S}$ は $k \in \mathcal{K}$ 及び $r^* \in \{0,1\}^\gamma$ をそれぞれ一様ランダムに選び、$\mathsf{ID}^* \leftarrow H_k(r^*)$ を計算する。ID^* を自身の NM-sID-CPA game での攻撃対象 ID として宣言し、$\mathcal{C}$ から prm を受け取る。$\mathcal{S}$ は $PK = (\mathsf{prm}, k)$ を $\mathcal{A}$ に渡す。

Phase 1. $\mathcal{S}$ は $\mathcal{A}$ の発行する復号クエリ $\chi_i = \langle \mathsf{ID}_i, y_i \rangle_{i\in\{1,\ldots,q_1\}}$ に対し、ID_i の値により以下の様に m_i を作成し応答する。

- $\mathsf{ID}_i = \mathsf{ID}^*$ **のとき:** $m_i = \perp$ を返す。
- **それ以外のとき:** ID_i を鍵導出クエリとして $\mathcal{C}$ に問い合わせ、d_{ID_i} を受け取る。$\mathsf{IBE.Dec}(d_{\mathsf{ID}_i}, y_i)$ を計算しこの結果が $\perp$ ならば $m_i = \perp$ を返し、そうでなければ復号結果 $m_i||r_i$ の m_i を返す。

Challenge. $\mathcal{A}$ が (m_0, m_1) を出力したとき、$\mathcal{S}$ は以下の様にしてチャレンジ暗号文 χ^* を作成して応答する。コイン $b_S \in \{0,1\}$ を振る。$m' \in \mathcal{M}_{\Pi'}(m_{b_S}$ と長さの等しい乱数) と $r' \in \{0,1\}^\gamma$ をそれぞれ一様ランダムに選ぶ。$M_{b_S} = m_{b_S}||r^*$, $M_{1-b_S} = m'||r' \in \mathcal{M}_\Pi$ とする。$\mathcal{M}^*_\Pi = (M_0, M_1)$ を自身の

$\mathsf{PKE.KG}(1^\kappa)$:	$\mathsf{PKE.Enc}(PK, m)$:	$\mathsf{PKE.Dec}(SK, \chi)$:
$(\mathsf{prm}, \mathsf{msk}) \leftarrow \mathsf{IBE.Setup}(1^\kappa)$	$r \leftarrow \{0,1\}^\gamma$; $\mathsf{ID} \leftarrow H_k(r)$	Parse χ as $\langle \mathsf{ID}, y \rangle$; $d_{\mathsf{ID}} \leftarrow \mathsf{IBE.Ext}(\mathsf{prm}, \mathsf{msk}, \mathsf{ID})$
$k \leftarrow \mathcal{K}$	$y \leftarrow \mathsf{IBE.Enc}(\mathsf{prm}, \mathsf{ID}, m\|\|r)$	$m\|\|r \leftarrow \mathsf{IBE.Dec}(d_{\mathsf{ID}}, y)$
$SK = \mathsf{msk}$, $PK = (\mathsf{prm}, k)$	$\chi = \langle \mathsf{ID}, y \rangle$	(If this decrypts to $\perp$ then output $\perp$ and stop.)
Output (SK, PK).	Output χ.	Output m if $H_k(r) = \mathsf{ID}$. Otherwise output $\perp$.

図 1: 提案する公開鍵暗号方式 Π'

Challenge として $\mathcal{C}$ に対し出力し、y^* を受け取る。$\chi^* = \langle \mathsf{ID}^*, y^* \rangle$ を $\mathcal{A}$ に渡す。

Phase 2. Phase 1 と同様の処理を行う。

Guess. $\mathcal{A}$ が b_A を出力する。$R :=$“下位 γ ビットが等しい” という 2 項関係とする。b_A の値により $\mathcal{S}$ は y' を以下の様に作成する。

- $b_A = b_S$ **のとき:** $m'' \in \mathcal{M}_{\Pi'}(m_{b_S}$ と長さの等しい乱数) と $r'' \in \{0,1\}^\gamma$ をそれぞれ一様ランダムに選ぶ。バイアスがかかったコインを振り、確率 α で $y' \leftarrow \mathsf{IBE.Enc}(\mathsf{prm}, \mathsf{ID}^*, m''||r^*)$、確率 $(1-\alpha)$ で $y' \leftarrow \mathsf{IBE.Enc}(\mathsf{prm}, \mathsf{ID}^*, m''||r'')$ とする。
- **それ以外のとき:** $\mathcal{A}$ の復号クエリ $\chi_j = \langle \mathsf{ID}_j, y_j \rangle_{j \in \{1,\ldots,q_D\}}$ の中からランダムに一つの y_j を選び、y' とする。

$\mathcal{S}$ は $\mathcal{C}$ に対し (R, y') を出力する。

以上が $\mathcal{S}$ の構成である。確率 α については今は未知数としておき、後で議論する。次に、$\mathcal{S}$ の NM-sID-CPA アドバンテージ $\mathsf{Adv}^{\text{NM-sID-CPA}}_{\Pi,\mathcal{S}}$ を計算する。

我々の $\mathcal{S}$ の構成法では、NM-sID-CPA の Challenge として $\mathcal{C}$ に送る $\mathcal{M}^*_\Pi$ は必ず 2 つの平文からなる。NM-sID-CPA game の定義により、$\mathcal{M}^*_\Pi$ からチャレンジとして選ばれる M^* は、$\mathcal{S}$ の作る M_0 か M_1 のどちらかでありその確率は等しく 1/2 の確率であるため、便宜上 NM-sID-CPA Challenger も自身のコイン $b_C \in \{0,1\}$ を振って、M_{b_C} をチャレンジのための平文 M^* として決定していると考えることにする。b_C は $\mathcal{S}$ のコイン b_S とは完全に独立に選ばれるため、$\Pr[b_S = b_C] = \Pr[b_S \neq b_C] = 1/2$ である。$b_S \neq b_C$ が起こる場合、$\mathcal{S}$ の $\mathcal{A}$ に対する Challenge のシミュレーションが完全ではなくなる。

暗号文 χ が提案方式 Π' の復号手順を実行すると $\perp$ を返さず正しく復号される場合、χ を “正当” であると呼ぶ。Valid を $\mathcal{A}$ が $\chi = \langle \mathsf{ID}^*, y \rangle$ という形でかつ正当な暗号文を復号クエリとして一回以上発行するイベントと定義する。Valid が起こる場合、$\mathcal{A}$ の復号クエリに対する $\mathcal{S}$ の応答のシミュレーションが完全ではなくなる。

b_S と b_C が一致するかどうか及び Valid が起こっているかどうかを $\mathcal{S}$ は知ることができない。

以下、b_A、b_S、b_C、及び Valid について、6 通りの場合を考える。

Case 1: $b_A = b_S \wedge b_S = b_C \wedge \overline{\mathsf{Valid}}$
Case 2: $b_A = b_S \wedge b_S = b_C \wedge \mathsf{Valid}$
Case 3: $b_A = b_S \wedge b_S \neq b_C$
Case 4: $b_A \neq b_S \wedge b_S = b_C \wedge \overline{\mathsf{Valid}}$
Case 5: $b_A \neq b_S \wedge b_S = b_C \wedge \mathsf{Valid}$
Case 6: $b_A \neq b_S \wedge b_S \neq b_C$

これら Case は、全ての場合を網羅している。① を Case i が起こるイベントと定義する。Case i における $\mathcal{S}$ のアドバンテージ Adv_i を以下の様に定義する。

$$\begin{aligned}\mathsf{Adv}_i &:= \Pr[\mathsf{R}^* \wedge ①] - \Pr[\mathsf{R}^* \wedge ①] \\ &= \Pr[①] \cdot (\Pr[\mathsf{R}^*|①] - \Pr[\mathsf{R}^*|①])\end{aligned}$$

NM-sID-CPA アドバンテージの定義により、

$$\mathsf{Adv}^{\text{NM-sID-CPA}}_{\Pi,\mathcal{S}} = \textstyle\sum_{i=1}^{6} \mathsf{Adv}_i$$

は明らかである。以下、各場合のアドバンテージを見積もっていく。

***Case 1*:** $b_A = b_S \wedge b_S = b_C \wedge \overline{\mathsf{Valid}}$
この場合、$M^* = m_{b_S}||r^*$、$M^{\bar{*}} = m'||r'$ となっている。$b_A = b_S$ ということは、$\mathcal{A}$ が guess に成功し、$\mathcal{S}$ にとってのチャレンジ暗号文 y^* の平文 $m_{b_S}||r^*$ を当てるということである。この状況下で $\mathcal{A}$ の出力 b_A を信用する場合は、$\mathcal{S}$ は自身のチャレンジ暗号文の平文を知ることになる。従って確率 α で $\mathcal{S}$ は $M^* = m_{b_S}||r^*$ と下位 γ ビットが等しい平文の暗号文 y' を出力できる。また、$\mathcal{A}$ の出力を信用しない場合はランダムな平文 $m''||r''$ の暗号文を出力するが、この平文の下位 γ ビット r'' と r^* が等しくなる確率は $(1-\alpha) \cdot 1/2^\gamma$ (以下簡単のため、$1/2^\gamma = \mathrm{P}_\gamma$ とおく)。従って、

$$\Pr[\mathsf{R}^*|①] = \alpha + (1-\alpha) \cdot \mathrm{P}_\gamma$$

また、r' と r^* 及び r' と r'' は独立に選ばれているため、y^* の平文として選ばれなかった平文 $m'||r'$ の下位 γ ビットと $\mathcal{S}$ の出力する暗号文 y' の平文の同部分が等しくなる確率は下記の様に評価できる。

$$\Pr[\mathsf{R}^{\bar{*}}|①] = \mathrm{P}_\gamma$$

次に、$\Pr[①]$ を評価する。

$$\begin{aligned}\Pr[①] &= \Pr[b_A = b_S \wedge b_S = b_C \wedge \overline{\mathsf{Valid}}] \\ &= \Pr[b_A = b_S | b_S = b_C \wedge \overline{\mathsf{Valid}}] \cdot \Pr[\overline{\mathsf{Valid}} | b_S = b_C] \\ &\qquad \cdot \Pr[b_S = b_C]\end{aligned}$$

ここで、以下が成り立つ。

$$\Pr[b_A = b_S | b_S = b_C \wedge \overline{\mathsf{Valid}}] = 1/2 + \epsilon_{cca}$$

なぜならば、$\mathcal{S}$ にとってのチャレンジ暗号文 y^* は ID^* を用いた $m_{b_S}||r^*$ の暗号であり、$\mathcal{A}$ に対する Challenge のシミュレーションは完全であり、Valid も起こらず復号クエリに対するシミュレーションも完全なため、$\mathcal{A}$ の View は実際に Π' を攻撃しているときと同一になるからである。従って $\mathcal{A}$ は通常の成功確率で動作する。$\Pr[\overline{\mathsf{Valid}}|b_S = b_C]$ はこの時点では $(1 - \mathrm{P_v})$ とおく (すなわち、$\Pr[\mathsf{Valid}|b_S = b_C] = \mathrm{P_v}$)。また、$\Pr[b_S = b_C] = 1/2$。以上により、Case 1 の $\mathcal{S}$ のアドバンテージは、

$$\begin{aligned}\mathsf{Adv}_1 &= \Pr[①] \cdot (\Pr[\mathsf{R}^*|①] - \Pr[\mathsf{R}^{\bar{*}}|①]) \\ &= (1/2 + \epsilon_{cca}) \cdot (1 - \mathrm{P_v}) \cdot 1/2 \cdot (\alpha + (1-\alpha) \cdot \mathrm{P}_\gamma - \mathrm{P}_\gamma) \\ &= 1/2 \cdot \alpha \cdot (1/2 + \epsilon_{cca}) \cdot (1 - \mathrm{P_v}) \cdot (1 - \mathrm{P}_\gamma)\end{aligned}$$

***Case 2*:** $b_A = b_S \wedge b_S = b_C \wedge \mathsf{Valid}$
この場合も Case 1 と同様に $M^* = m_{b_S}||r^*$、$M^{\bar{*}} = m'||r'$ となっているため以下の評価ができる。

$\Pr[\mathsf{R}^*|②] = \alpha + (1-\alpha)\cdot \mathrm{P}_\gamma$

$\Pr[\mathsf{R}^{\bar{*}}|②] = \mathrm{P}_\gamma$

次に $\Pr[②]$ を評価する。

$$\begin{aligned}\Pr[②] &= \Pr[b_A = b_S \wedge b_S = b_C \wedge \mathsf{Valid}] \\ &= \Pr[b_A = b_S | b_S = b_C \wedge \mathsf{Valid}]\cdot\Pr[\mathsf{Valid}|b_S = b_C] \\ &\qquad \cdot \Pr[b_S = b_C]\end{aligned}$$

Case 1 で定義した様に、$\Pr[\mathsf{Valid}|b_S = b_C] = \mathrm{P_v}$。$\Pr[b_A = b_S|b_S = b_C \wedge \mathsf{Valid}]$ は、$\mathcal{A}$ にとっての復号クエリに対するシミュレーションが Valid によって完全でなくなったにも関わらず $\mathcal{A}$ が $\mathcal{S}$ のアドバンテージを伸ばすような行動をする確率である。ここではこれを $\mathrm{P_k}$ とおいて未知のままにしておく。また、$\Pr[b_S = b_C] = 1/2$。

以上より、Case 2 の $\mathcal{S}$ のアドバンテージは、

$$\begin{aligned}\mathsf{Adv}_2 &= \Pr[②]\cdot(\Pr[\mathsf{R}^*|②] - \Pr[\mathsf{R}^{\bar{*}}|②]) \\ &= 1/2\cdot \mathrm{P_k}\cdot\mathrm{P_v}\cdot\alpha\cdot(1-\mathrm{P}_\gamma)\end{aligned}$$

***Case 3*:** $b_A = b_S \wedge b_S \neq b_C$
この場合、$M^* = m'||r'$、$M^{\bar{*}} = m_{b_S}||r^*$ となっており、$\Pr[\mathsf{R}^*|③]$ と $\Pr[\mathsf{R}^{\bar{*}}|③]$ の評価は Case 1 の場合と入れ替わる。すなわち、以下の様になる。

$\Pr[\mathsf{R}^*|③] = \mathrm{P}_\gamma$

$\Pr[\mathsf{R}^{\bar{*}}|③] = \alpha + (1-\alpha)\cdot\mathrm{P}_\gamma$

また、$\Pr[③]$ については、以下の様になる。

$$\begin{aligned}\Pr[③] &= \Pr[b_A = b_S \wedge b_S \neq b_C] \\ &= \Pr[b_A = b_S | b_S \neq b_C]\cdot\Pr[b_S \neq b_C]\end{aligned}$$

$b_S \neq b_C$ の場合、$\mathcal{A}$ に与えられるチャレンジ暗号文 χ^* は $\mathcal{A}$ の選んだ平文 m_0、m_1 のどちらの暗号文でもないため、$\mathcal{A}$ にとっての Challenge のシミュレーションは完全ではない。そのため、$\mathcal{A}$ は $\mathcal{S}$ に対してどのようにも振舞えるが、Case 3 の場合 b_S は $\mathcal{A}$ に対して完全に隠されているため、b_A と b_S が等しくなる確率は情報理論的に 1/2 である。従って、$\Pr[b_A = b_S|b_S \neq b_C] = 1/2$。また、$\Pr[b_S \neq b_C] = 1/2$。

以上により、Case 3 の $\mathcal{S}$ のアドバンテージは、

$$\begin{aligned}\mathsf{Adv}_3 &= \Pr[③]\cdot(\Pr[\mathsf{R}^*|③] - \Pr[\mathsf{R}^{\bar{*}}|③]) \\ &= 1/2\cdot 1/2\cdot\{\mathrm{P}_\gamma - \alpha - (1-\alpha)\cdot\mathrm{P}_\gamma\} \\ &= -1/4\cdot\alpha\cdot(1-\mathrm{P}_\gamma)\end{aligned}$$

***Case 4*:** $b_A \neq b_S \wedge b_S = b_C \wedge \overline{\mathsf{Valid}}$
この場合、M^* および $M^{\bar{*}}$ は Case 1 と同様である。$b_A \neq b_S$ のため、$\mathcal{S}$ は y' を、$\mathcal{A}$ の発行した復号クエリから一つ選ぶことになる。Valid が起こっていないため、$\mathcal{A}$ の復号クエリの中には、一つも r^* と等しくなるような下位 γ ビットを持つものが存在しない。従って、

$\Pr[\mathsf{R}^*|④] = 0$

また、この場合の $\mathcal{A}$ は $M^{\bar{*}} = m'||r'$ に関する情報を何も得ることができない。よって $\mathcal{A}$ が $\mathsf{R}(M^{\bar{*}}, y_i)$ の起こる y_i を含む暗号文を復号クエリとして発行している確率は高々P_γ である。

$\Pr[\mathsf{R}^{\bar{*}}|④] \leq \mathrm{P}_\gamma$

$\Pr[④]$ は以下の様に計算できる。

$$\begin{aligned}\Pr[④] &= \Pr[b_A \neq b_S \wedge b_S = b_C \wedge \overline{\mathsf{Valid}}] \\ &= \Pr[b_A \neq b_S | b_S = b_C \wedge \overline{\mathsf{Valid}}] \\ &\qquad \cdot \Pr[\mathsf{Valid}|b_S = B_C]\cdot\Pr[b_S = b_C] \\ &= (1-(1/2+\epsilon_{cca}))\cdot(1-\mathrm{P_v})\cdot 1/2 \\ &= 1/2\cdot(1/2-\epsilon_{cca})\cdot(1-\mathrm{P_v})\end{aligned}$$

ただし $\Pr[b_A = b_S|b_S = b_C \wedge \overline{\mathsf{Valid}}] = 1/2 + \epsilon_{cca}$、$\Pr[\mathsf{Valid}|b_S = b_C] = \mathrm{P_v}$、$\Pr[b_S = b_C] = 1/2$ を用いた。

以上により、Case 4 の $\mathcal{S}$ のアドバンテージは、

$$\begin{aligned}\mathsf{Adv}_4 &= \Pr[④]\cdot(\Pr[\mathsf{R}^*|④] - \Pr[\mathsf{R}^{\bar{*}}|④]) \\ &\geq -1/2\cdot(1/2-\epsilon_{cca})\cdot(1-\mathrm{P_v})\cdot\mathrm{P}_\gamma\end{aligned}$$

***Case 5*:** $b_A \neq b_S \wedge b_S = b_C \wedge \mathsf{Valid}$
この場合、M^* および $M^{\bar{*}}$ は Case 1 と同様である。Valid が起こり復号クエリの応答のシミュレーションが完全でなくなるため、$\mathcal{A}$ は $\mathcal{S}$ に対してどのようにも振舞うことができる。しかし Valid が起こるとき、$\mathcal{A}$ は少なくとも一つ、$H_k(r_A) = \mathsf{ID}^*$ となるような平文 $M_A = m_A||r_A$ の暗号文 y_A が含まれるような復号クエリ $\langle \mathsf{ID}^*, y_A\rangle$ を発行している。$b_A \neq b_S$ のため、$\mathcal{S}$ は $\mathcal{A}$ が発行した一つの復号クエリを q_D 個の中から選んで y' として出力する。$\Pr[\mathsf{R}^*|⑤]$ は、$\mathcal{S}$ が、q_D 個の復号クエリの中から $H_k(r_A) = \mathsf{ID}^*$ となるような平文 $M_A = m_A||r_A$ の暗号文 y_A を選び、なおかつその平文 $m_A||r_A$ が $r_A = r^*$ を満たす確率である。

$$\begin{aligned}\Pr[\mathsf{R}^*|⑤] &\geq 1/q_D\cdot\Pr[r_A = r^*|⑤] \\ &= 1/q_D\cdot(1-\Pr[r_A \neq r^*|⑤])\end{aligned}$$

ここで、$[r_A \neq r^*|⑤]$ というイベントを考えると、Case 5 の場合 $\mathcal{S}$ のシミュレーション中に $\mathcal{A}$ に与えられる r^* の情報は $\mathsf{IBE.Enc}(\mathsf{prm}, H_k(r^*), m_{b_S}||r^*)$ という暗号文と $H_k(r^*)(= \mathsf{ID}^*)$ であり、r^* と k はいずれも $\mathcal{S}$ により前もってそれぞれ一様ランダムに選ばれている。この状況で $\mathcal{A}$ が $r_A \neq r^* \wedge H_k(r_A) = H_k(r^*) = \mathsf{ID}^*$ となる r_A を平文に持つような復号クエリを送っている確率は、ランダムに選んだ r^* そのものを与えられ、ランダムに選ばれたハッシュ鍵 k のもと $r_A \neq r^* \wedge H_k(r_A) = H_k(r^*) = \mathsf{ID}^*$ となる r_A を見つける確率か、それよりも小さくなり、その確率は H のターゲット衝突困難性により、高々ϵ_{tcr} となる。従って、

$\Pr[\mathsf{R}^*|⑤] \geq 1/q_D\cdot(1-\epsilon_{tcr})$

また、Case 4 の場合と同様の議論により、

$\Pr[\mathsf{R}^{\bar{*}}|⑤] \leq \mathrm{P}_\gamma$

$\Pr[⑤]$ は以下の様に計算される。

$$\begin{aligned}\Pr[⑤] &= \Pr[b_A \neq b_S \wedge b_S = b_C \wedge \mathsf{Valid}] \\ &= (1-\Pr[b_A = b_S|b_S = b_C \wedge \mathsf{Valid}]) \\ &\qquad \cdot \Pr[\mathsf{Valid}|b_S = b_C]\cdot\Pr[b_S = b_C] \\ &= (1-\mathrm{P_k})\cdot\mathrm{P_v}\cdot 1/2\end{aligned}$$

ただし、$\Pr[b_A = b_S|b_S = b_C \wedge \mathsf{Valid}] = \mathrm{P_k}$、$\Pr[\mathsf{Valid}|b_S = b_C] = \mathrm{P_v}$、$\Pr[b_S = b_C] = 1/2$ を用いた。

以上により、Case 5 の $\mathcal{S}$ のアドバンテージは、

$$\begin{aligned}\mathsf{Adv}_5 &= \Pr[⑤]\cdot(\Pr[\mathsf{R}^*|⑤] - \Pr[\mathsf{R}^{\bar{*}}|⑤]) \\ &\geq (1-\mathrm{P_k})\cdot\mathrm{P_v}\cdot 1/2\cdot\{1/q_D\cdot(1-\epsilon_{tcr}) - \mathrm{P}_\gamma\}\end{aligned}$$

***Case 6*:** $b_A \neq b_S \wedge b_S \neq b_C$
この場合、M^* および $M^{\bar{*}}$ は Case 3 と同様である。$\Pr[\mathsf{R}^*|⑥]$ については

$\Pr[\mathsf{R}^*|⑥] \geq 0$

と評価する。次に $Pr[\mathsf{R}^*|⑥]$ について考える。Case 6 の場合、$b_S \neq b_C$ のため、$\mathcal{A}$ にはチャレンジ暗号文として

ID^* と ID^* の下で暗号化された $m'||r'$ の暗号文 y^* が与えられる。y^* は r^* の情報を含まないため、$\mathcal{A}$ が r^* に関して得る情報は、$\mathsf{ID}^* = H_k(r^*)$ のみである。この状況の下、r^* と等しくなる下位 γ ビットを持つ平文の暗号文を復号クエリとして一つ以上問い合わているということは、$\mathsf{ID}^* = H_k(r^*)$ のみ与えられて r^* を求めたことになる。その確率は、ID^* のみを与えられて r^* も含めた集合 $\{r|\mathsf{ID}^* = H_k(r)\}(\ni r^*)$ の元をいずれか一つを求める確率以下であり、このような確率は H の一方向性により高々 ϵ_{ow} となる。従って、以下の様に評価できる。

$\Pr[\mathsf{R}^{\bar{*}}|⑥] \leq \epsilon_{ow}$

$\Pr[⑥]$ については、$\Pr[③]$ と全く同様の議論により、

$\Pr[⑥] = 1/4$

以上により、Case 6 の $\mathcal{S}$ のアドバンテージは、

$\mathsf{Adv}_6 = \Pr[⑥] \cdot (\Pr[\mathsf{R}^*|⑥] - \Pr[\mathsf{R}^{\bar{*}}|⑥]) \geq -1/4 \cdot \epsilon_{ow}$

アドバンテージの評価　以上の議論で、全ての Case のアドバンテージを評価した。これらを用いて $\mathsf{Adv}^{\text{NM-sID-CPA}}_{\Pi,\mathcal{S}}$ を計算する。

$$
\begin{aligned}
&\mathsf{Adv}^{\text{NM-sID-CPA}}_{\Pi,\mathcal{S}} = \textstyle\sum_{i=1}^{6} \mathsf{Adv}_i \\
&\geq 1/2 \cdot (1/2 + \epsilon_{cca}) \cdot (1 - \mathrm{P_v}) \cdot \alpha \cdot (1 - \mathrm{P}_\gamma) \\
&\quad + 1/2 \cdot \mathrm{P_k} \cdot \mathrm{P_v} \cdot \alpha \cdot (1 - \mathrm{P}_\gamma) \\
&\quad - 1/4 \cdot \alpha \cdot (1 - \mathrm{P}_\gamma) \\
&\quad - 1/2 \cdot (1/2 - \epsilon_{cca}) \cdot (1 - \mathrm{Pv}) \cdot \mathrm{P}_\gamma \\
&\quad + (1 - \mathrm{P_k}) \cdot \mathrm{P_v} \cdot 1/2 \cdot \{1/q_D \cdot (1 - \epsilon_{tcr}) - \mathrm{P}_\gamma\} \\
&\quad - 1/4 \cdot \epsilon_{ow}
\end{aligned}
$$

このうち第 2 項と第 5 項に注目し、

$\alpha = \{1/q_D \cdot (1 - \epsilon_{tcr}) - \mathrm{P}_\gamma\}/(1 - \mathrm{P}_\gamma)$

とおくと、$\mathrm{P_k}$ に関する項が消える。以降この α を用いて計算していく。

$$
\begin{aligned}
&\mathsf{Adv}^{\text{NM-sID-CPA}}_{\Pi,\mathcal{S}} \\
&\geq 1/2 \cdot (1/2 + \epsilon_{cca}) \cdot (1 - \mathrm{P_v}) \cdot \{1/q_D \cdot (1 - \epsilon_{tcr}) - \mathrm{P}_\gamma\} \\
&\quad - 1/4 \cdot \{1/q_D \cdot (1 - \epsilon_{tcr}) - \mathrm{P}_\gamma\} \\
&\quad - 1/2 \cdot (1/2 - \epsilon_{cca}) \cdot (1 - \mathrm{Pv}) \cdot \mathrm{P}_\gamma \\
&\quad + 1/2 \cdot \mathrm{P_v} \cdot \{1/q_D \cdot (1 - \epsilon_{tcr}) - \mathrm{P}_\gamma) \\
&\quad - 1/4 \cdot \epsilon_{ow} \qquad (\alpha\text{に上記値を代入}) \\
&= 1/2 \cdot 1/q_D \cdot \mathrm{P_v} \cdot (1/2 - \epsilon_{cca}) \cdot (1 - \epsilon_{tcr}) \\
&\quad + 1/2 \cdot 1/q_D \cdot (1 - \epsilon_{tcr}) \cdot \epsilon_{cca} - 1/4 \cdot \mathrm{P}_\gamma - 1/4 \cdot \epsilon_{ow} \\
&\quad (\mathrm{P_v} \text{ に関する項とそうでない項に分類し、整理})
\end{aligned}
$$

最後の等式の第 1 項について、IND-CCA 安全性、ターゲット衝突困難性それぞれの定義により $(1/2 - \epsilon_{cca} \geq 0)$、$(1 - \epsilon_{tcr}) \geq 0$、確率の定義により $\mathrm{P_v} \geq 0$ なので、(第 1 項)≥ 0 である。従って、以下が得られる。

$$
\begin{aligned}
&\mathsf{Adv}^{\text{NM-sID-CPA}}_{\Pi,\mathcal{S}} \\
&\geq 1/2 \cdot 1/q_D \cdot (1 - \epsilon_{tcr}) \cdot \epsilon_{cca} - 1/4 \cdot (\epsilon_{ow} + 1/2^{\gamma})
\end{aligned}
$$

以上の議論から、$\mathcal{A}$ が ϵ_{cca} のアドバンテージで Π' を破り、H が (t, ϵ_{tcr})-TCRHF かつ (t, ϵ_{ow})-OWHF である場合、前述の α を $\mathcal{A}$ を信用する確率として用いることで、$\mathcal{S}$ は上記のアドバンテージで Π の NM-sID-CPA 安全性を破ることができる。 □

ハッシュ関数のターゲット衝突困難性　今回の構成法で用いるハッシュ関数では、本質的な意味でのターゲット衝突困難性、すなわち ϵ_{tcr} が無視できる値であることは必要としていない。定理 1 が成り立つためには、$(1 - \epsilon_{tcr})$ が無視できない値を持つと保障できる様なハッシュ関数ならば十分である。

暗号文サイズのオーバーヘッド　提案した公開鍵暗号 Π' の、内部の ID ベース暗号 Π からの暗号文サイズのオーバーヘッドは、平文と共に暗号化されている乱数 r のサイズと、$\mathsf{ID} = H_k(r)$ のサイズの和、すなわちハッシュ関数 H の入力長及び出力長の和である。提案方式の安全性証明には H の一方向性及びターゲット衝突困難性しか使用していない。これらの性質は、誕生日攻撃の脅威にさらされないため、κ ビット安全性の達成のためには入力長、出力長それぞれ κ ビット程度あればよい。従って、暗号文サイズのオーバーヘッドはおよそ 2κ ビット、128 ビット安全性達成のためにはおよそ 256 ビットとなる。

IND と NM の溝　我々の構成法は、BK 変換 [4] から、MAC 及び汎用ハッシュ関数を取り除いた形になっている。この構成法で CCA 安全性を証明できるということは、IND-sID-CPA と NM-sID-CPA の間には大きな差があることを暗に示していると考えることができる。

4　まとめ

本稿では、任意の頑強性を持つ IBE に基づく CCA 安全性を持つ PKE の構成法を示した。構成要素として、IBE 以外には一方向性とターゲット衝突困難性を併せ持つ一つのハッシュ関数しか必要とせず、構成法は効率的である。安全性証明は、これまでの IBE-PKE 変換の方法とは本質的に異なり、IBE の頑強性に帰着するが、暗号技術の安全性をある種の暗号方式の頑強性に帰着する様な方式はこれまでほとんど存在しないため、本稿での証明は新しい証明技法として興味深い。現在まで NM-sID-CPA 安全性を持つと示されている IBE は本質的には存在しないため、我々の結果は理論的な意味合いが強いが、今後、頑強性についての研究、議論が進めば、我々の結果が実用的にも大きな意味を持つ可能性が出てくることが期待できる。

参考文献

[1] M. Abe, Y. Cui, H. Imai, E. Kiltz, "Efficient Hybrid Encryption from ID-Based Encryption," Available at eprint.iacr.org/2007/023/

[2] N. Attrapadung, Y. Cui, D. Galindo, G. Hanaoka, I. Hasuo, H. Imai, K. Matsuura, P. Yang, R. Zhang, "Relations Among Notions of Security for Identity Based Encryption Schemes," *Proc. of LATIN'06*, LNCS 3887, pp. 130-141, 2006.

[3] M. Bellare, A. Desai, D. Poincheval, P. Rogaway, "Relations among *Proc. of CRYPTO'98*, LNCS 1462, pp. 26-45, 1998.

[4] D. Boneh, J. Katz, "Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption," *Proc. of CT-RSA'05*, LNCS 3376, pp.87-103, 2005.

[5] X. Boyen, Q. Mei, B. Waters, "Direct Chosen Ciphertext Security from Identity-Based Techniques," *CR-RSA'05*, LNCS 3376, pp. 87-103, 2005.

[6] R. Canetti, S. Halevi, J. Katz, "Chosen-Ciphertext Security from Identity-Based Encryption," *Proc. of EUROCRYPT'04*, LNCS 3027, pp. 207-222, 2004.

[7] R. Cramer, V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack," *SIAM Journal on Computing*, Vol. 33, pp. 167-226, 2003.

[8] J. Håstad, R. Impagliazzo, L. Levin, M. Luby, "Construction of a Pseudorandom Generator from any One-Way Function," *SIAM J. Comp.* 28(4):1364-1396, 1999.

[9] R. Zhang, "Tweaking TBE/IBE to PKE Transforms with Chameleon Hash Functions," *Proc. of ACNS'07*, LNCS 4521, pp. 323-339, 2007.