SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

スタンダードPAとメッセージ秘匿性との関係
Relationship between Standard Model Plaintext Awareness and Message Hiding[1]

寺西勇*† 尾形わかは†
Isamu Teranishi Wakaha Ogata

あらまし 近年 Bellare と Palacio がスタンダードモデルにおける PA の概念を定式化するのに成功した．彼らは情報論的，統計的，計算量的の 3 種類の PA を定義した．本稿では，スタンダードモデル PA と IND-CPA 安全性の関係を考察する．一見この 2 つの性質は無関係に見える．しかし非自明な公開鍵暗号方式に関してはそうではなく，暗号化関数が一方向性を満たす暗号方式がもし情報論的 PA，統計的 PA，計算量的 PA のいずれかを満たせば，IND-CPA 安全性を満たすことを証明する．この事実を用いることで,「PA + 一方向性 ⇒ IND-CCA2」が成立することをも示す．この事実は PA 安全な方式の平文秘匿性が「最強か無か」であることを意味する．すなわち，PA 安全な方式は最強の平文秘匿性である IND-CCA2 を満たすか，最弱の平文秘匿性である一方向性すら満たさないかのいずれかであることを意味する．本稿ではさらに，計算量的 PA が統計的 PA よりも真に弱い性質であることをも示す．

キーワード Plaintext Awareness，スタンダードモデル，識別不能性

1 はじめに

Plaintext Awareness (PA) [BR94,BDPR98, HLM03,BP04] は公開鍵暗号方式の安全性に関する概念である．直観的には，ある方式が PA 安全であるとは，いかなる攻撃者も平文を「知らずに」暗号文を作成することができないことを指す．

公開鍵暗号方式が IND-CPA 安全である場合には，PA 性から IND-CCA2 安全性を導くことができることが知られているので，PA の概念は公開鍵暗号の研究にとても重要である．

PA 安全性はもともと，ランダムオラクルモデルのもとで定式化され，しかもその定義はランダムオラクルに強く依存していた [BR94, BDPR98]．しかし PA の直感的定義は，前述のようにランダムオラクルとは無関係なものであるので，ランダムオラクルに頼らず PA を定義するにはどうすればよいかというのが，PA の初期の研究において重要な課題の一つであった．

しかし Asiacrypt 2004 で Bellare と Palacio [BP04] はスタンダードモデルにおける PA 安全性を定義することに成功した．これにより暗号方式が PA であるかかどうかという視点から方式を解析できるようになり，その後 Cramer-Shoup 方式 [CS98] が PA 安全性を満たすことが Dent[D06] により示された．

Bellare 等 [BP04] による PA の定義の概略をふりかえってみよう．PA の概念は「Dec」および「Ext」という 2 つの世界の識別不能性をもって定義される.「Dec」における攻撃者は復号オラクルなどにアクセスできるが，一方で「Ext」における攻撃者は復号オラクルの代わりに抽出者というエンティティにアクセスできる．抽出者は平文を抽出することによって復号オラクルをシミュレートするエンティティであり，抽出者は攻撃者が「知っている」データのみを用いてシミュレートを行う.「Dec」と「Ext」が攻撃者にとって情報論的，統計的，計算量的に識別不能であるかに応じて，Bellare 等 [BP04] は情報論的/統計的/計算量的の三種類の PA 安全性を定義した．

彼らはさらに，暗号方式が IND-CPA 安全であれば，情報論的 PA，統計的 PA，計算量的 PA のいずれからも IND-CCA2 安全性が従うことを示した．

本論文ではスタンダードモデル PA と IND-CPA 安全性との関係を示す．一見これら 2 つの概念は独立なものにみえるが，非自明な公開鍵暗号方式に関してはそうではないことを我々は示す．すなわち，暗号化関数が一方向性を満たす暗号方式がもし情報論的 PA，統計的 PA，計算量的 PA のいずれかを満たせば，IND-CPA 安全性をも満たすことを証明する．

* NEC 〒 211-8666 神奈川県川崎市中原区下沼部 1753 1753, Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa, 211-8666, Japan. teranisi@ah.jp.nec.com
† 東京工業大学 〒 152-8552 東京都目黒区大岡山 2-12-1 Tokyo Institute of Technology. 2-12-1 Ookayama, Meguro-ku Tokyo, 152-8550, Japan. wakaha@mot.titech.ac.jp
[1] 本研究は Asiacrypt 2006 で発表した内容 [TO06] と同一である。

PA に関する基本定理として「(情報論的，統計的，もしくは計算量的) PA + IND-CPA ⇒ IND-CCA2」が成り立つことを思い出されたい．我々の成果をこの基本定理と組み合わせることで，より強いバージョンの基本定理「PA + 一方向性 ⇒ IND-CCA2」を証明できる．

この事実は PA 安全な方式の平文秘匿性が「最強か無か」であることを意味する．すなわち，(情報論的，統計的，もしくは計算量的に) PA 安全な方式は最強の平文秘匿性である IND-CCA2 を満たすか，最弱の平文秘匿性である一方向性すら満たさないかのいずれかであることを意味する．

我々の成果は理論的な側面のみならず，暗号方式の IND-CCA2 安全性を示す際に役立つというより現実的な応用をも持つ．OAEP 方式 [BR94] の変種達の IND-CCA2 安全性を示す際に，PA 安全性のみならず IND-CPA 安全性をも証明しなければならなかった．我々の成果は，こうした IND-CPA 安全性の証明がスタンダードモデルの場合には必要がないことを意味しているのである．

我々はさらに，計算量的 PA が統計的 PA より真に弱い概念であることを証明する．この成果は藤崎 [F06] の成果と関係が深い．藤崎は [F06] で，ランダムオラクル PA の計算量バージョンにあたる *Plaintext Simulatability(PS)* という概念を提唱し，この概念が通常のランダムオラクル PA よりも真に弱いことを示している．我々の成果は藤崎の成果のスタンダードモデル版であると解釈することができる．よって我々の成果を藤崎 [F06] の成果を比較することにより，スタンダードモデルにおける統計的 PA と計算量的 PA がそれぞれランダムオラクルにおける PA と PS に対応した概念であることが分かる．

2 スタンダードモデル PA の定義

定義 2.1 (スタンダードモデル **PA** [**BP04**])**.** $\kappa \in \mathbb{N}$ をセキュリティ・パラメータとし、$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とする．$\mathcal{A}$，$\mathcal{P}$，$\mathcal{K}$ を多項式時間機械とし，それぞれ**攻撃者**，**平文生成器**，**抽出器**と呼ぶ．

これらの機械を使って、2 つの実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A},\mathcal{P}}(\kappa)$ と $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A},\mathcal{K},\mathcal{P}}(\kappa)$ を定義する．実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A},\mathcal{P}}(\kappa)$ では $\mathcal{A}$ は**暗号化オラクル**と**復号オラクル**にアクセスする事ができ，実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A},\mathcal{K},\mathcal{P}}(\kappa)$ では暗号化オラクルと抽出器 $\mathcal{K}$ とにアクセスする事ができる．$\mathcal{A}$ が暗号化オラクルに送信したクエリを**暗号化クエリ**といい，復号オラクルもしくは $\mathcal{K}$ 送信したクエリを**復号クエリ**という．

実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A},\mathcal{P}}(\kappa)$，$\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A},\mathcal{K},\mathcal{P}}(\kappa)$ は図 1 のように定義される．図 1 で記号 $\mathcal{A}(\mathsf{pk}; R_{\mathcal{A}})$ は $\mathcal{A}$ に入力 pk と乱数テープ $R_{\mathcal{A}}$ をいれて動作させることを表す．またこれらの実験において，$\mathcal{A}$ は $C \in \mathsf{CList}$ を満たす (dec, C) をクエリすることはできない．

公開鍵暗号方式 Π が (スタンダードモデルにおいて)

—$\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A},\mathcal{P}}(\kappa)$—

$\mathcal{A}$，$\mathcal{P}$ の乱数テープ $R_{\mathcal{A}}$，$R_{\mathcal{P}}$ をランダムに選ぶ．
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^{\kappa})$，$\mathsf{CList} \leftarrow \varepsilon$，$\mathsf{St}_{\mathcal{P}} \leftarrow \varepsilon$．
　(ここで $\mathsf{St}_{\mathcal{P}}$ は $\mathcal{P}$ の内部状態)．
$\mathcal{A}(\mathsf{pk}; R_{\mathcal{A}})$ を実行．
　ただし $\mathcal{A}$ のオラクル・クエリに対しては以下のように返答：
　If($\mathcal{A}$ が暗号化オラクルに Q をクエリした)
　　$(M_Q, \mathsf{St}_{\mathcal{P}}) \leftarrow \mathcal{P}(Q, \mathsf{St}_{\mathcal{P}}; R_{\mathcal{P}})$，$C_Q \leftarrow \mathsf{Enc}_{\mathsf{pk}}(M_Q)$，
　　$\mathsf{CList} \leftarrow \mathsf{CList} || C_Q$．$C_Q$ を $\mathcal{A}$ に返答．
　If($\mathcal{A}$ が復号オラクルに C をクエリした)
　　$M \leftarrow \mathsf{Dec}_{\mathsf{sk}}(C)$．$M$ を $\mathcal{A}$ に返答．
$\mathcal{A}$ の出力 S を出力．

—$\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A},\mathcal{K},\mathcal{P}}(\kappa)$—

$\mathcal{A}$，$\mathcal{P}$，$\mathcal{K}$ の乱数テープ $R_{\mathcal{A}}$，$R_{\mathcal{P}}$，$R_{\mathcal{K}}$ をランダムに選ぶ．
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^{\kappa})$, $\mathsf{CList} \leftarrow \varepsilon$, $\mathsf{St}_{\mathcal{P}} \leftarrow \varepsilon$, $\mathsf{St}_{\mathcal{K}} \leftarrow (\mathsf{pk}, R_{\mathcal{A}})$.
　(ここで $\mathsf{St}_{\mathcal{P}}$，$\mathsf{St}_{\mathcal{K}}$ は $\mathcal{P}$，$\mathcal{K}$ の内部状態)．
$\mathcal{A}(\mathsf{pk}; R_{\mathcal{A}})$ を実行．
　ただし $\mathcal{A}$ のオラクル・クエリに対しては以下のように返答：
　If($\mathcal{A}$ が暗号化オラクルに Q をクエリした)
　　$(M_Q, \mathsf{St}_{\mathcal{P}}) \leftarrow \mathcal{P}(Q, \mathsf{St}_{\mathcal{P}}; R_{\mathcal{P}})$，$C_Q \leftarrow \mathsf{Enc}_{\mathsf{pk}}(M_Q)$，
　　$\mathsf{CList} \leftarrow \mathsf{CList} || C$．$C$ を $\mathcal{A}$ に返答．
　If($\mathcal{A}$ が $\mathcal{K}$ に C をクエリした)
　　$(M, \mathsf{St}_{\mathcal{K}}) \leftarrow \mathcal{K}(C, \mathsf{CList}, \mathsf{St}_{\mathcal{K}}; R_{\mathcal{K}})$．$M$ を $\mathcal{A}$ に返答．
$\mathcal{A}$ の出力 S を出力．

図 1: PA の概念 [BP04] を定義するのに使う実験

情報論的/統計的/計算量的に PA 安全であるとは以下が成立することを指す：

$$^{\forall}\mathcal{A}^{\exists}\mathcal{K}^{\forall}\mathcal{P} : \mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A},\mathcal{P}}(\kappa) \text{ と } \mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A},\mathcal{K},\mathcal{P}}(\kappa) \text{ が}$$
情報論的/統計的/計算量的に識別不能．

定理 2.2 (スタンダードモデル **PA** の基本定理 [**BP04**])**.** 公開鍵暗号方式 Π が IND-CPA 安全かつ (情報論的，統計的，もしくは計算量的に)PA 安全なら Π は IND-CCA2 安全である．

3 統計的 PA $\gneqq$ 計算量的 PA

この章では統計的 PA が計算量的 PA より真に強い概念であることを示す．すなわち，統計的 PA 安全だが計算量的 PA 安全ではない公開鍵暗号方式 $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ を例示する．

κ をセキュリティ・パラメータとする．$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を計算量的 PA 安全かつ IND-CPA 安全 (従って IND-CCA2 安全) な公開鍵暗号方式とする．我々は Π を改造して求める暗号方式 $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ を作る．鍵生成アルゴリズム $\mathsf{Gen}'(1^{\kappa})$ は $\mathsf{Gen}(1^{\kappa})$ を実行して公開鍵・秘密鍵ペア $(\mathsf{pk}, \mathsf{sk})$ を得た後，平文 M_0 をランダムに選び，暗号文 $C_0 = \mathsf{Enc}_{\mathsf{pk}}(M_0)$ を計算する．そして Gen' は $\mathsf{pk}' = (\mathsf{pk}, C_0)$，$\mathsf{sk}' = \mathsf{sk}$ とし，公開鍵・秘密鍵ペア $(\mathsf{pk}', \mathsf{sk}')$ を出力する．また $\mathsf{Enc}'_{\mathsf{pk}'}(M) = \mathsf{Enc}_{\mathsf{pk}}(M)$，$\mathsf{Dec}'_{\mathsf{sk}'}(C) = \mathsf{Dec}_{\mathsf{sk}}(C)$ と定義する．(図 2)．

我々はまず Π' が統計的 PA 安全ではないことを示す．$\mathcal{A}'_0$ を Π' に対する以下のような攻撃者とする：入力 $\mathsf{pk}' =$

$\mathsf{Gen}'(1^\kappa)$:
　$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$
　平文 M_0 をランダムに選ぶ.
　$C_0 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(M_0)$.
　$\mathsf{pk}' \leftarrow (\mathsf{pk}, C_0)$, $\mathsf{sk}' \leftarrow \mathsf{sk}$.
　$(\mathsf{pk}', \mathsf{sk}')$ を出力.

$\mathsf{Enc}'_{\mathsf{pk}'}(M) = \mathsf{Enc}_{\mathsf{pk}}(M)$, $\mathsf{Dec}'_{\mathsf{sk}'}(C) = \mathsf{Dec}_{\mathsf{sk}}(C)$.

$\mathcal{A}'_0(\mathsf{pk}')$:
　pk' を (pk, C_0) とパースし，復号クエリ C_0 を送信する..

図 2: $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ および $\mathcal{A}'_0$ の記述

(pk, C_0) から C_0 を得，C_0 を出力する．Π' の定義より，平文 M_0 や暗号文 C_0 を作ったのは $\mathcal{A}'_0$ ではなく Gen' であった．よって $\mathcal{A}'_0$ は C_0 に対応する平文 M_0 を「知らない」．$\mathcal{A}'_0$ に対する抽出器 $\mathcal{K}'$ は，$\mathcal{A}'_0$ が見ることができるデータのみを見ることができるので，$\mathcal{K}'$ も $M_0 = \mathsf{Dec}'_{\mathsf{sk}'}(C_0) = \mathsf{Dec}_{\mathsf{sk}}(C_0)$ を「知らない」．よって $\mathcal{K}'$ は M_0 を抽出することはできない．すなわち Π' は統計的 PA 安全ではない．

しかし一方で我々は Π' が計算量的 PA 安全であることを示すことができる．一見，Π' は計算量的 PA 安全ではないように見える．なぜなら計算量的 PA 安全性を示す場合も，抽出器 $\mathcal{K}'$ に M_0 を抽出させねばならないように見えるからである．しかし実際には，M_0 が抽出可能でなくても Π' の計算量的 PA 安全性を示すことができる．計算量的 PA 安全性の定義が $\mathcal{K}'$ に要求しているのは，$\mathcal{A}_0$ にとって M_0 と**計算量的に識別不能な**平文を出力することだけである．よって $\mathcal{K}'$ は M_0 自身を出力しなくてもすむのである．

$\mathcal{A}'_0$ は M_0 はもちろん，$C_0 = \mathsf{Enc}_{\mathsf{pk}}(M_0; r)$ を計算するのに使った乱数 r すらも「知らない」ことを思い出されたい．しかも Π は IND-CCA2 安全であった．よって $\mathcal{A}'_0$ は M_0 をランダムなメッセージ M_1 と区別することはできない．従って $\mathcal{K}'$ は，$\mathcal{A}'_0$ の復号クエリ C_0 に対する返答としてランダムに選んだメッセージ M_1 を返すことができる．

以上の議論を精緻化することで，以下の定理を得ることができる：

定理 3.1 (統計的 PA $\gneqq$ 計算量的 PA). 計算量的 PA 安全な公開鍵暗号方式が少なくとも一つ存在すると仮定する．このとき，計算量的 PA 安全だが統計的 PA 安全ではない公開鍵暗号方式が存在する．

定理 3.1 は，藤崎 [F06] の成果と関係が深い．藤崎は [F06] で，ランダムオラクル PA の計算量バージョンにあたる *Plaintext Simulatability(PS)* という概念を提唱し，この概念が通常のランダムオラクル PA よりも真に弱いことを示している．よって定理 3.1 は藤崎 [F06] の成果のスタンダードモデル版であると解釈することができる．よって定理 3.1 と藤崎 [F06] の成果を比較することにより，スタンダードモデルにおける統計的 PA と計算量的 PA がそれぞれランダムオラクルにおける PA と PS に対応した概念であることが分かる．

4 PA + 一方向性 $\Rightarrow$ IND-CPA

この章のメインの成果は以下のものである：

定理 4.1 (PA + 一方向性 $\Rightarrow$ IND-CPA). $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式で暗号化関数 Enc が一方向性を満たすものとする．もし Π が情報論的，統計的，もしくは計算量的に PA 安全であれば，Π は IND-CPA 安全である（ので IND-CCA2 安全でもある).

定理 4.1 は PA 安全な方式の平文秘匿性が「全てか無か」であることを意味する．すなわち，PA 安全な方式は最強の平文秘匿性である IND-CCA2 を満たすか，最弱の平文秘匿性である一方向性すら満たさないかのいずれかであることを意味する．

定理 4.1 を示す前に，定理 4.1 の仮定から一方向性を取り除くことができないことを見る：

定理 4.2. 情報論的 PA 安全だが一方向でも IND-CPA 安全でもない公開鍵暗号方式が存在する．

定理 4.2 の証明の概略. $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を平文 M の暗号化 $\mathsf{Enc}_{\mathsf{pk}}(M)$ が M 自身である暗号方式とすると，明らかに Π は一方向でも IND-CPA 安全でもない．

しかし Π は情報論的 PA 安全である．なぜなら $\mathsf{Enc}_{\mathsf{pk}}(M)$ はそもそも平文を全く隠していないので，抽出器 $\mathcal{K}$ は攻撃者が出力した暗号文自身から平文を抽出可能だからである． □

我々はまず暗号方式 Π が統計的 PA 安全である場合に対し定理 4.1 を示す．すると Π が情報論的 PA 安全である場合に対しても定理 4.1 が成り立つことが明らかに従う．

統計的な場合に対する定理 4.1 の証明の概略. 背理法で示す．すなわち，統計的 PA 安全だが IND-CPA 安全ではない暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が存在すると仮定して，Π が一方向性を満たさないことを示す．

このことを示す為我々は攻撃者 $\mathcal{A}_0$ で，以下のトリッキーな性質を満たす暗号文 C_0 を出力できるものを作る：(1) $\mathcal{A}_0$ は平文 $M_0 = \mathsf{Dec}_{\mathsf{sk}}(C_0)$ を「知らない」，(2) C_0 は暗号化オラクルによって出力された暗号文ではない．そのような $\mathcal{A}_0$ が存在したと仮りに仮定する．C_0 は暗号化オラクルの出力ではないので，$\mathcal{A}_0$ は復号オラクルに C_0 をクエリできる．よって Π の統計的 PA 性より，$\mathcal{A}_0$ に対する抽出器 $\mathcal{K}$ で，$\mathcal{A}_0$ のクエリ C_0 に対する平文 M_0 を抽出できるものが存在する．これはすなわち，$\mathcal{K}$ が「知られていない」はずの平文 M_0 を暗号文 $C_0 = \mathsf{Enc}_{\mathsf{pk}}(M_0)$

から計算できること，つまり暗号化関数 Enc の逆関数を計算可能であることを意味し，Enc が一方向だという仮定に反する．

次に我々は $\mathcal{A}_0$ を実際に構成する．一見，前述した性質を満たす $\mathcal{A}_0$ を構築するのは不可能であるように見える．なぜなら PA の定義により $\mathcal{A}_0$ は，対応する平文 M_0 を「知らない」暗号文 C_0 を生成することができないからである．しかし PA の定義は，$\mathcal{A}_0$ がそのような C_0 を「生成」するのを禁じているだけで，他のエンティティにそのような C_0 を「作ってもらう」のを禁じているわけではないことに注意されたい．そこで平文生成器 $\mathcal{P}_0$ に C_0 を作らせ，$\mathcal{A}_0$ は $\mathcal{P}_0$ から C_0 を受け取ることにする．このように C_0 を得た場合，$C_0 = \mathsf{Enc}_{\mathsf{pk}}(M_0)$ を作ったのは $\mathcal{A}_0$ でなく $\mathcal{P}_0$ なので，$\mathcal{A}_0$ は平文 M_0 を知ることなく C_0 を得ることができる．(注 : C_0 を作るのは $\mathcal{P}_0$ 自身であり暗号化オラクルではないことを強調する．暗号化オラクルが C_0 を作った場合には，$\mathcal{A}_0$ は C_0 を復号オラクルにクエリすることが許されなくなるので，前述した証明手法が使えなくなってしまう)．

上で説明した手法を使うには，$\mathcal{P}_0$ は C_0 を $\mathcal{A}_0$ に送信しなければならない．しかし $\mathcal{P}_0$ が $\mathcal{A}_0$ に直接 C_0 を送信できるような通信路は存在しない．そこで我々は，$\mathcal{P}_0$ から $\mathcal{A}_0$ への通信を可能にする「バーチャルな」通信路を構築する．ここで我々は公開鍵暗号方式 Π が IND-CPA 安全ではないという仮定を用いる．統計的 PA 安全性の定義より，$\mathcal{P}_0$ は暗号化オラクルに自分が選んだ平文を送信し，暗号化オラクルはその平文を暗号化して暗号文 c を $\mathcal{A}_0$ に送る．Π は IND-CPA 安全ではないので，c は平文の情報を漏らす．これは，$\mathcal{P}_0$ が c を通じて何らかの情報を $\mathcal{A}_0$ に送ることができることを意味する．すなわち，$\mathcal{P}_0$ は暗号文 c をバーチャルな通信路として用いることができるのである．

最後に，$\mathcal{P}_0$ がいかにして $\mathcal{A}_0$ に C_0 を「送る」のかをより詳細に述べる．pk_0 を公開鍵とし，sk_0 を対応する秘密鍵とする．Π は IND-CPA 安全ではないので，多項式時間機械 $\mathcal{B}$，その内部状態 $\mathsf{St}_{\mathcal{B}}$，平文の組 (m_0, m_1)，および non negligible な関数 $\mu = \mu(\kappa)$ が存在して，$\Pr(\mathcal{B}(\mathsf{pk}_0, m_0, m_1, \mathsf{Enc}_{\mathsf{pk}_0}(m_1), \mathsf{St}_{\mathcal{B}}) = 1)$ と $\Pr(\mathcal{B}(\mathsf{pk}_0, m_0, m_1, \mathsf{Enc}_{\mathsf{pk}_0}(m_0), \mathsf{St}_{\mathcal{B}}) = 1)$ の差は μ 以上である．

$\lceil 1/\mu \rceil$ を N と書き，さらに $C_0 = \mathsf{Enc}_{\mathsf{pk}_0}(M_0)$ の i 番目のビットを b_i と書き、$1 - b_i$ を $\bar{b}_i$ と書く．暗号化クエリを行う通信路を用いて，$\mathcal{A}_0$ は $\mathsf{pk}_0||m_0||m_1||N$ を $\mathcal{P}_0$ に事前に送っておく．各 i に対し，$\mathcal{P}_0$ は m_{b_i} と $m_{\bar{b}_i}$ を暗号化オラクルに N 回ずつ送る．すると暗号化オラクルは暗号文 $c_1^{(i)} = \mathsf{Enc}_{\mathsf{pk}_0}(m_{b_i}), \ldots, c_N^{(i)} = \mathsf{Enc}_{\mathsf{pk}_0}(m_{b_i})$ と $\bar{c}_1^{(i)} = \mathsf{Enc}_{\mathsf{pk}_0}(m_{\bar{b}_i}), \ldots, \bar{c}_N^{(i)} = \mathsf{Enc}_{\mathsf{pk}_0}(m_{\bar{b}_i})$ とを $\mathcal{A}_0$ に送信する．$\{c_j^{(i)}\}$ を受け取ったら，$\mathcal{A}_0$ は各 i，j に対し $\mathcal{B}(\mathsf{pk}_0, m_0, m_1, c_j^{(i)}, \mathsf{St}_{\mathcal{B}})$ を実行し，$\mathcal{B}$ の出力 $u_j^{(i)}$ を得、同様に $\mathcal{B}(\mathsf{pk}_0, m_0, m_1, \bar{c}_j^{(i)}, \mathsf{St}_{\mathcal{B}})$ を実行し，$\mathcal{B}$ の出力 $\bar{u}_j^{(i)}$ を得る．$u_1^{(i)}, \ldots, u_N^{(i)}$ の平均値 $(u_1^{(i)} + \cdots + u_N^{(i)})/N$ の方が $\bar{u}_1^{(i)}, \ldots, \bar{u}_N^{(i)}$ の平均値 $(\bar{u}_1^{(i)} + \cdots + \bar{u}_N^{(i)})/N$ の方が大きければ $b'_i = 1$ とし，そうでなければ $b'_i = 0$ とする．$\mathcal{B}$ は non negligible なアドバンテージをもっているので，圧倒的な確率で $b'_i = b_i$ が成立する．これはすなわち，$\mathcal{A}_0$ が暗号文 C_0 の i 番目のビット b_i を圧倒的な確率で再構成できることを意味する．よって $\mathcal{A}_0$ は暗号文 $C_0 = b_1||\cdots||b_n$ を再構成できる．すなわち，$\mathcal{A}_0$ は $\mathcal{P}_0$ から C_0 を「受信」できたことになる．以上の議論より，定理が成立する． □

次に Π が計算量的 PA な場合を考察する．

計算量的な場合に対する定理 4.1 の証明の概略. 統計的 PA の場合における証明と同様，計算量的 PA 安全だが IND-CPA 安全ではない公開鍵暗号方式 Π が存在すると仮定して，Π が一方向性を満たさないことを示す．このことを示す為に，統計的 PA の場合の証明で使った $\mathcal{A}_0$ や $\mathcal{P}_0$ に似たアルゴリズムを用い，類似の議論を行う．しかし，Π が計算量的 PA の場合は，抽出器 $\mathcal{K}$ は $M_0 = \mathsf{Dec}_{\mathsf{sk}_0}(C_0)$ 自身を出力するとは限らず，M_0 と計算量的に識別不能な別の平文を出力するかもしれない．そこで，M_0 自身を得る為に，$\mathcal{A}_0$ や $\mathcal{P}_0$ のアルゴリズムを修正する．

まず我々は $\mathcal{A}_0$ を改造して攻撃者 $\mathcal{A}_1$ を作る．するとある抽出器 $\mathcal{K}$ が存在して，任意の平文生成器 $\mathcal{P}'$ に対し $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}'}(\kappa)$ の出力と $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}'}(\kappa)$ の出力とは計算量的識別不能. 次に我々は $\mathcal{P}_0$ を改造して、$\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ と $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$ が (計算量的識別不能であるのみならず)，統計的識別不能であるような $\mathcal{P}_1$ を作る。ただし後で見るように，我々の作る $\mathcal{P}_1$ は M_0 の抽出には利用できない．そこで最後に我々は $\mathcal{P}_1$ を改造することで M_0 の抽出に利用できる $\mathcal{P}_2$ を作る．

実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$ を記述することを通して，$\mathcal{A}_1$ と $\mathcal{P}_1$ とのアルゴリズムを与える．実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$ において，実験者はまず鍵生成アルゴリズム $\mathsf{Gen}(1^\kappa)$ を実行し，Gen の出力として公開鍵･秘密鍵ペア $(\mathsf{pk}, \mathsf{sk})$ を得る．そして実験者は $\mathcal{A}_1$ と暗号化オラクルと復号オラクルに pk を入力し，復号オラクルにはさらに sk も入力する．$\mathcal{A}_1$ は $\mathcal{B}(\mathsf{pk})$ を実行し，$\mathcal{B}$ の出力 $(m_0, m_1, \mathsf{St}_{\mathcal{B}})$ を得る．ここで $\mathcal{B}$ は統計的 PA の場合の証明にでてきたアルゴリズムと同じもので、IND-CPA に対する攻撃者．そして $\mathcal{A}_1$ は暗号クエリ用の通信路を使って，$\mathsf{pk}||m_0||m_1||N$ を $\mathcal{P}_1$ に送る．ただし $N = \lceil 1/\mu \rceil$.

$\mathcal{P}_1$ はメッセージ M_1 をランダムに選び，$C_1 = \mathsf{Enc}_{\mathsf{pk}}(M_1)$ を計算する．そして $\mathcal{A}_1$ と $\mathcal{P}_1$ は，C_0 の変わりに C_1 を使って $\mathcal{A}_0$ や $\mathcal{P}_0$ と同じ手続きを実行する．すなわち，$\mathcal{P}_1$ は「バーチャルな」通信路を用いて C_1 を $\mathcal{A}_1$ に送る．C_1 を「受信」したら，$\mathcal{A}_1$ は C_1 を復号クエリし，その返答 M' を受け取る．(注 : クエリに返答したのが復号オラク

ルであれば $M' = M_1 = \mathsf{Dec}_{\mathsf{sk}}(C_1)$ が成立するが，返答したのが抽出器であればその限りではない)．

その後 $\mathcal{A}_1$ は暗号化クエリ用の通信路を用いて M' を $\mathcal{P}_1$ に送信する．M' を受信したら $\mathcal{P}_1$ は $M_1 = M'$ が成立するかどうかをチェックし，$M_1 = M'$ なら $S = 1$ とし，そうでなければ $S = 0$ とする．そして $\mathcal{P}_1$ は「バーチャルな」通信路を用いて S を $\mathcal{A}_1$ に「送信」する．最後に $\mathcal{A}_1$ は S を出力する．

以上のようにして構成した $\mathcal{A}_1$ に対し，ある抽出器 $\mathcal{K}$ が存在して，任意の平文生成器 $\mathcal{P}'$ に対し，$\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}'}(\kappa)$ の出力と $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}'}(\kappa)$ の出力は計算量的識別不能．特に，$\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ の出力は $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$ の出力と計算量的識別不能である．(注：ここでは $\mathcal{A}_1$ と $\mathcal{P}_1$ の記述を同時に与えたが、実際にはまず $\mathcal{A}_1$ を決めると適切な $\mathcal{K}$ が存在し、そして任意の平文生成器の具体例として $\mathcal{P}_1$ を与える．実際，$\mathcal{P}_1$ に依存せずに $\mathcal{K}$ を定義できることを簡単にチェックできる)．

我々は $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ の出力と $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$ の出力が実際には**統計的に**識別不能なことを示す．$\mathcal{A}_1$ と $\mathcal{P}_1$ の定義より，実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$ において $\mathcal{A}_1$ の出力 S は常に 1 である．$\mathcal{A}_1$ は実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ と実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$ を計算量的に識別することはできないので，実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ においても $S = 1$ が圧倒的な確率で成立する．$\mathcal{A}_1$ と $\mathcal{P}_1$ の定義より，$S = 1$ が成立する必要十分条件は $M' = M_1$ が成立することである．以上のことは，$\mathcal{K}$ が $C_1 = \mathsf{Enc}_{\mathsf{pk}}(M_1)$ に対応する正しい平文 M_1 出力する確率が圧倒的なことを意味する．これはすなわち，$\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ の出力と $\mathbf{Exp}^{\mathsf{PA\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$ の出力が統計的に識別不能なことを意味する．

次に $\mathcal{P}_1$ を改造して平文生成器 $\mathcal{P}_2$ を作る．(pk_0, C_0) を $\mathsf{Enc}_{\mathsf{pk}}$ に対する一方向性ゲームのインスタンスとし，sk_0 を pk_0 に対応する未知の秘密鍵とする．我々の目標は $M_0 = \mathsf{Dec}_{\mathsf{sk}_0}(C_0)$ を計算することである．$\mathcal{P}_2$ のアルゴリズムは，以下の点を除いて $\mathcal{P}_1$ のそれと同じである：(1) $\mathcal{P}_2$ は入力として C_0 を受け取る，(2) $\mathcal{P}_2$ は自分で暗号文 C_1 を生成せず，C_0 を C_1 の変わりに用いる，(3) $\mathcal{P}_2$ は常に S を 1 にセットする．

さらに実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa)$ の以下のような改造版 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$ を作る：実験者は $\mathsf{Gen}(1^\kappa)$ によって作られた pk の変わりに一方向性ゲームのインスタンス (pk_0, C_0) の一部である pk_0 を用いる．また $\mathcal{A}_1$ の出力 S のみならず、C_0 に対する $\mathcal{K}$ の返答 M' をも出力する．今まで示したように，実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ における $\mathcal{P}_1$ も実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$ における $\mathcal{P}_2$ も，圧倒的な確率で S を 1 にセットする．しかも (pk_0, C_0) の分布はランダムに選ばれた (pk, C) の分布と同じである．よって $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ における $\mathcal{P}_1$ の振る舞いは $\mathbf{Exp}^{\mathsf{PA\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$ における $\mathcal{P}_2$ の振る舞いと統計的に識別不能である．しかも $\mathcal{K}$ は平文生成器の乱数テープを見ることができないので，$\mathcal{K}$ は $\mathcal{P}_1$ の振る舞いと $\mathcal{P}_2$ の振る舞いを識別できない．

したがって $\mathbf{Exp}^{\mathsf{PA\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$ が出力した S の分布と $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ の出力の分布は統計的に識別不能である．実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ における $\mathcal{K}$ の出力 M' は圧倒的な確率で $M_1 = \mathsf{Dec}_{\mathsf{sk}_0}(C_1)$ に等しかったことを思い出されたい．したがって実験 $\mathbf{Exp}^{\mathsf{PA\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$ においても，$\mathcal{K}$ の出力 M' は圧倒的な確率で $M_0 = \mathsf{Dec}_{\mathsf{sk}_0}(C_0)$ に等しい．これはすなわち，$\mathbf{Exp}^{\mathsf{PA\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$ を利用すれば，圧倒的な確率で $M_0 = \mathsf{Dec}_{\mathsf{sk}_0}(C_0)$ を計算できることを意味する．□

5 まとめ

本論文ではスタンダードモデル PA と IND-CPA の関係を調べた．一見この 2 つの概念は全く独立なものに見えるが，我々は暗号化関数が一方向性を満たすという仮定のもと，情報論的，統計的，計算量的スタンダードモデル PA がいずれも IND-CPA 性を満たすことを示した．この成果を PA の基本定理「PA + IND-CPA ⇒ IND-CCA2」と組み合わせることで，より強いバージョンの基本定理「PA + 一方向性 ⇒ IND-CCA2」を証明できる．この事実は PA 安全な方式の平文秘匿性が「全てか無か」であることを意味する．すなわち，(情報論的，統計的，もしくは計算量的に) PA 安全な方式は最強の平文秘匿性である IND-CCA2 を満たすか，最弱の平文秘匿性である一方向性すら満たさないかのいずれかであることを意味する．

さらに我々は，計算量的 PA の概念が統計的 PA の概念よりも真に弱いことを示した．この成果を藤崎 [F06] の成果と比較することで，スタンダードモデルにおける統計的 PA と計算量的 PA がそれぞれランダムオラクルにおける PA と PS [F06] とに対応していることが分かる．

参考文献

[BDPR98] Mihir Bellare, Anand Desai, David Pointcheval, Phillip Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. CRYPTO 1998, pp.26-45.

[BP04] Mihir Bellare, Adriana Palacio. Towards plaintext-aware public-key encryption without random oracles. ASIACRYPT 2004, pp. 48-62.

[BR94] Mihir Bellare, Phillip Rogaway. Optimal Asymmetric Encryption. EUROCRYPT 1994, pp.92-111.

[BR96] Mihir Bellare, Phillip Rogaway. The Exact Security of Digital Signatures: How to Sign with RSA and Rabin. EUROCRYPT 1996, pp.399-416.

[B01] Dan Boneh. Simplified OAEP for the RSA and Rabin Functions. CRYPTO 2001, pp.275-291.

[BF01] Dan Boneh, Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. CRYPTO 2001, pp.213-229.

[CHJPPT98] Jean-Se'bastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, Christophe Tymen. Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages. PKC 2002, pp. 17-33.

[CJNP02] Jean-Se'bastien Coron, Marc Joye, David Naccache, Pascal Paillier. Universal Padding Schemes for RSA. CRYPTO 2002, pp. 226-241.

[CS98] Ronald Cramer, Victor Shoup. A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack. CRYPTO 1998, pp.13-25.

[CS01] Ronald Cramer, Victor Shoup. Design and Analysis of Practical Public-Key Encryption Schemes. manuscript, 2001. Full version: SIAM J. Comp. 2004, 33(1), pp.167-226.

[D91] Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In CRYPTO'91, pp.445-456.

[D06] Alexander W. Dent. Cramer-Shoup is Plaintext-Aware in the Standard Model. EUROCRYPT 2006.

[DDN00] Danny Dolev, Cynthia Dwork, Moni Naor. Nonmalleable Cryptography. SIAM J. Comp. 2000, 30(2), pp. 391-437.

[DY83] Danny Dolev, Andrew Chi-Chih Yao. On the security of public key protocols. IEEE Transactions on Information Theory, 1983, 29(2) pp.198-207.

[F06] Eiichiro Fujisaki. Plaintext Simulatability. IEICE Trans. Fundamentals 2006, E89-A, pp.55-65, doi:10.1093/ietfec/e89-a.1.55. Preliminary version is available at http://eprint.iacr.org/2004/ 218.pdf

[FO99] Eiichiro Fujisaki, Tatsuaki Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. PKC'99, pp. 53-68.

[FOPS01] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, Jacques Stern. RSA-OAEP Is Secure under the RSA Assumption. CRYPTO 2001, pp.260-274. J. Cryptology 2004, 17(2), pp.81-104.

[HLM03] Jonathan Herzog, Moses Liskov, Silvio Micali. Plaintext Awareness via Key Registration. CRYPTO 2003, pp.548-564

[JN03] Antoine Joux, Kim Nguyen. Separating Decision Diffie-Hellman from Computational Diffie-Hellman in Cryptographic Groups. J. Cryptology, 2003,16(4), pp.239-247. http://eprint.iacr.org/2001/003

[KI01] Kazukuni Kobara, Hideki Imai. Semantically Secure McEliece Public-Key Cryptosystems-Conversions for McEliece PKC. In PKC 2001, pp. 19-35.

[KO03] Yuichi Komano, Kazuo Ohta. Efficient Universal Padding Techniques for Multiplicative Trapdoor One-Way Permutation. CRYPTO 2003, pp. 366-382.

[M01] James Manger. A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0. CRYPTO 2001, pp.230-238.

[MOV93] Alfred Menezes, Tatsuaki Okamoto, Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. on Information Theory 1993, 39(5), pp.1639-1646.

[OP01] Tatsuaki Okamoto, David Pointcheval. REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. CT-RSA 2001, pp.159-175.

[PP04] Duong Hieu Phan, David Pointcheval. OAEP 3-Round: A Generic and Secure Asymmetric Encryption Padding. In Asiacrypt 2004. pp. 63-77.

[SOK01] Ryuichi Sakai, Kiyoshi Ohgishi, Masao Kasahara. Cryptosystems Based on Pairings. SCIS 2001.

[S00] Victor Shoup. Using Hash Functions as a Hedge against Chosen Ciphertext Attack. EUROCRYPT 2000, pp.275-288.

[S01] Victor Shoup. OAEP Reconsidered. CRYPTO 2001, pp.239-259. J. Cryptology, 2002, 15(4), pp. 223-249.

[TO06] Relationship between Standard Model Plaintext Awareness and Message Hiding. Asiacrypt 2006, pp 226-240. (本論文の英語版).