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

スタンダードモデル PA の新しい特徴づけ
New Characterizations of Plaintext Awareness in the Standard Model

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 Plaintext Awareness (PA) を定義することに成功した．彼らは情報論的，統計的，計算量的の 3 種類のバージョンのスタンダードモデル PA を提案した．しかし彼らの定義は従来のランダムオラクルの PA の定義とはかなり異なる上，ランダムオラクルの PA の定義よりも難しい．その上，彼らの定義が従来のランダムオラクル PA の概念を「直接的にスタンダードモデル化した」ものと一致しているかどうかすら分かっていない．本論文ではスタンダードモデル PA のよりシンプルな特徴づけを 2 つ提案した．第一の特徴づけは ideal/real フレームワークに基づいたもので，情報論的，統計的，計算量的の全ての PA に対して適応できる．第二のものは統計的な PA にしか適応できない．この特徴づけはランダムオラクル KE の概念を「直接的にスタンダードモデル化した」ものをベースにしたものだが，我々はランダムオラクル PA の場合と同じ式では統計的スタンダードモデル PA を特徴付けられないことをも示す．我々はさらに，統計的スタンダードモデル PA に対するこの第二の特徴づけが計算量的スタンダードモデル PA の場合には拡張できないことをも示した．

キーワード Plaintext Awareness，スタンダードモデル，ideal/real フレームワーク，ランダムオラクル

1 はじめに

背景: **Plaintext Awareness**(PA) [BR94, BDPR98, HLM03, BP04] は暗号方式の安全性に関する概念である．直観的にいうと，公開鍵暗号方式が PA 安全であるとは，その方式が IND-CPA 安全性を満たしかつ以下の性質を満たすときにいう：いかなる攻撃者も平文を「知らずに」暗号文を作ることはできない．PA 安全性は IND-CCA2 安全性を含意する [BR94, BDPR98, BP04] ので，PA 安全性は公開鍵暗号の研究においてとても重要な概念である．

PA の概念自身はスタンダードモデルでも意味をもつにもかかわらず，PA のオリジナルの定義はランダムオラクルモデルで定式化され [BR94, BDPR98]，しかもこのモデルに強く依存していた．この為，PA の初期の研究においては，PA の定義をいかにしてスタンダードモデルに拡張するかが大きな課題の一つであった．

近年，Bellare と Palacio [BP04] がスタンダードモデルで PA を定義することに成功し，さらにスタンダードモデル PA も IND-CCA2 を含意することを証明した．その後 Dent [D06] は有名な Cramer-Shoup 暗号方式 [CS98] が PA 安全なことを示した．

Bellare 等によるスタンダードモデル PA の定義は，ランダムオラクル PA の場合と同じく，IND-CPA 安全性を満たすことおよび「いかなる攻撃者も平文を「知らずに」暗号文を作ることはできない」という性質を満たすことによって定義される．しかし後者の性質の定義がランダムオラクル PA におけるそれと大きく異なる上，より複雑である．(そこで以後両者を区別し，スタンダードモデル，ランダムオラクルにおける後者の性質をそれぞれ **Knowledge Indistinguishability** (**KI**)，**Knowledge Extractability** (**KE**) と呼ぶ)．実際例えば，KE 安全性の方は一つの実験を持って定義されるのに，KI 安全性の方は 2 つの実験の識別不能性をもって定義する等複雑である．しかも 2 つの実験の識別不能性が情報論的になのか，統計的になのか，計算量的になのかに応じて KI 安全性の方は 3 種類の定義ができてしまい，対応してスタンダードモデル PA も 3 種類できてしまう．このため，より簡単にスタンダードモデル PA を特徴づけることが望まれるし，3 種類のスタンダードモデル PA のうちどれがもとのランダムオラクル PA に対応するものなのかを調べる必要がある．

成果: 本論文ではスタンダードモデル PA のよりシンプルな特徴づけを 2 つ提案する．第一の特徴づけは ideal/real フレームワークに基づいたものであり，第二のものはラ

* 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

$\mathcal{A}$ および $\mathcal{K}$ の乱数テープ R，ρ をランダムに選ぶ．
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}^{\mathsf{Hash}}(1^\kappa)$.
$C_0 \leftarrow \mathcal{A}^{\mathsf{Hash}, \mathsf{Enc}^{\mathsf{Hash}}_{\mathsf{pk}}}(\mathsf{pk}; R)$.
$\mathsf{CList} \leftarrow$(オラクル $\mathsf{Enc}^{\mathsf{Hash}}_{\mathsf{pk}}$ の答えの全てからなるリスト)
$\mathsf{HList} \leftarrow$($\mathcal{A}$ のハッシュ・クエリと対応する答えとのリスト),
$M_0 \leftarrow \mathcal{K}(\mathsf{pk}, C_0, \mathsf{CList}, \mathsf{HList}; \rho)$.
If $M_0 = \mathsf{Dec}_{\mathsf{sk}}(C_0)$ return 1. Otherwise return 0.

図 1: ランダムオラクル KE の概念を定義するのに使う実験

ンダムオラクル KE の概念を「直接的にスタンダードモデル化した」ものをベースにしたものである．第一の特徴づけは情報論的，統計的，計算量的の全ての PA に対して適応できるが，第一の特徴づけは統計的な PA にしか適応できない．

第一，第二の特徴づけはその有用性が互いに異なる．第一の特徴づけは PA から他の何らかの性質を証明するときに有用であり，第二の特徴づけは逆に他の何らかの性質から PA を証明するときに有用である．

第二の特徴づけはスタンダードモデル版の KE の概念に基づいており，しかもランダムオラクル PA は (ランダムオラクル版の)KE を用いて定義されていたのだから，この特徴づけはランダムオラクル PA と統計的スタンダードモデル PA の関係を示しているとも解釈できる．しかし我々は同時に，ランダムオラクル PA とは同じ方法では統計的スタンダードモデル PA を特徴付けられないことをも示す．すなわち，ランダムオラクル PA が「KE + IND-CPA」で定義されていたのに対し，統計的スタンダードモデル PA の場合は「KE + IND-CPA」とは同値にならないことを示す．そこで我々は PA の特徴づけとして「KE + IND-CPA」でなく「KE + IND-CCA2」を採用した．

我々はさらに，統計的スタンダードモデル PA に対するこの第二の特徴づけが計算量的スタンダードモデル PA の場合には拡張できないことをも示した．すなわち我々はスタンダードモデル KE の概念を計算量的な場合に拡張し，計算量的スタンダード KE と IND-CCA2 とをあわせたものが計算量的スタンダードモデル PA を含意しないことを示した．

2 準備

Definition 2.1 (ランダムオラクルにおける **KE** と **PA** [**BR94, BDPR98**])**.** $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開暗号方式でハッシュ関数を使うものとする．ハッシュ関数 Hash に対し，$\mathsf{Gen}^{\mathsf{Hash}}$，$\mathsf{Enc}^{\mathsf{Hash}}$，$\mathsf{Dec}^{\mathsf{Hash}}$ で Hash によって instantiate された鍵生成，暗号化，および復号アルゴリズムとする．$\mathcal{A}$ と $\mathcal{K}$ をそれぞれ**攻撃者**，**抽出器**と呼ばれる多項式時間機械とする．セキュリティ・パラメータ κ に対し，実験 $\mathbf{Exp}^{\mathsf{KE\text{-}RO}}_{\Pi,\mathcal{A},\mathcal{K},\mathsf{Enc}}(\kappa)$ を図 1 のように定義する．この実験において，C_0 は CList の元であってはならない．

Π がランダムオラクル **KE 安全**であるとは，Π が次を満たすときに言う：

$^{\exists}\mathcal{K}^{\forall}\mathcal{A} : \Pr(\mathbf{Exp}^{\mathsf{KE\text{-}RO}}_{\Pi,\mathcal{A},\mathcal{K},\mathsf{Enc}}(\kappa) = 1)$ は κ に関し圧倒的．

Π がランダムオラクル KE 安全で，しかも IND-CPA 安全であるとき，Π はランダムオラクル **PA 安全**であるという．

Theorem 2.2 (ランダムオラクル **PA** に関する基本定理 [**BR94, BDPR98**])**.** 公開鍵暗号方式 Π がランダムオラクル *PA* 安全であるなら Π はランダムオラクルモデルのもと *IND-CCA2* 安全である．

Definition 2.3 (スタンダードモデルにおける **KI** と **PA** [**BP04**])**.** $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とする．$\mathcal{A}$，$\mathcal{K}$，$\mathcal{P}$ をそれぞれ，**攻撃者**, **抽出器**, **平文生成器**と呼ばれる多項式時間機械とする．$\mathsf{St}_{\mathcal{P}}$，$\mu$ をそれぞれ，平文生成器 $\mathcal{P}$ の状態，および乱数テープとする．$\mathsf{Enc}_{\mathsf{pk}} \circ \mathcal{P}(Q; \mu)$ を以下の動作をするアルゴリズムとする：$(M, \mathsf{St}_{\mathcal{P}}) \leftarrow \mathcal{P}(Q, \mathsf{St}_{\mathcal{P}}; \mu)$，$C \leftarrow \mathsf{Enc}_{\mathsf{pk}}(M)$，$C$ を出力．κ をセキュリティ・パラメータとする．2 つの実験 $\mathbf{Exp}^{\mathsf{KI\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$，$\mathbf{Exp}^{\mathsf{KI\text{-}SM\text{-}}\mathcal{K}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ を図 2 のように定義する．

Π が**情報論的/統計的/計算量的に (スタンダードモデル) KI 安全**であるとは，

$^{\forall}\mathcal{A}^{\exists}\mathcal{K}^{\forall}\mathcal{P} : \mathbf{Exp}^{\mathsf{KI\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ と $\mathbf{Exp}^{\mathsf{KI\text{-}SM\text{-}}\mathcal{K}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ が κ に関して情報論的/統計的/計算量的識別不能

であるときにいう．$\mathcal{K}$ が $\mathcal{A}$ に関して**圧倒的成功確率を誇る**(successful) とは，$\mathcal{K}$ が任意の $\mathcal{P}$ に関して上の関係式を満たすときにいう．さらに，Π が情報論的/統計的/計算量的 KI 安全で，しかも IND-CPA 安全であるとき，Π は**情報論的/統計的/計算量的に PA 安全である**という．

Theorem 2.4 (スタンダードモデル **PA** に関する基本定理 [**BP04**])**.** 公開鍵暗号方式 Π がスタンダードモデル *PA* 安全なら Π は *IND-CCA2* 安全である．

Theorem 2.5 (**Cramer-Shoup** は計算量的 **PA** [**D06**])**.** *DDH* 仮定と *DHK* 仮定 *[D91, BP04]* のもと，*Cramer-Shoup* 暗号方式 *[CS98]* は計算量的 *PA* を満たす．

3 第一の特徴づけ

この章ではスタンダードモデル PA(と KI) の概念の新しい特徴づけを与え，そしてこの特徴づけが PA の従来の定義 [BP04] と一致することを証明する．我々の特徴づけは情報論的，統計的，および計算量的な PA の概念の全てに適応することができる．

KI の概念は攻撃者自身が平文を知っていることを要請していた．しかし KI のもとの定義では，平文を出力

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

$\mathcal{A}$, $\mathcal{P}$ の乱数テープ R, μ をランダムに選ぶ.
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$.
停止するまで $\mathcal{A}(\mathsf{pk};R)$ を実行.
  オラクルへの質問には以下のように答える:
  If($\mathcal{A}$ が暗号化クエリ (enc,Q) を出す)
    $C \leftarrow \mathsf{Enc}_{\mathsf{pk}} \circ \mathcal{P}(Q;\mu)$, C を $\mathcal{A}$ に返信する.
  If($\mathcal{A}$ が復号クエリ (dec,Q) を出す)
    $M \leftarrow \mathsf{Dec}_{\mathsf{sk}}(Q)$, M を $\mathcal{A}$ に返信する.
Return $\mathcal{A}$ の出力 S.

—$\mathbf{Exp}^{\mathsf{KI\text{-}SM\text{-}}\mathcal{K}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$—

$\mathcal{A}$, $\mathcal{K}$, $\mathcal{P}$ のランダムテープ R, ρ, μ をランダムに選ぶ.
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$.
暗号化オラクルの返答のリスト CList を ε に初期化する.
$\mathcal{K}$ の状態 $\mathsf{St}_{\mathcal{K}}$ を ε に初期化する.
停止するまで $\mathcal{A}(\mathsf{pk};R)$ を実行.
  オラクルへの質問には以下のように答える:
  If($\mathcal{A}$ が暗号化クエリ (enc,Q) を出す)
    $C \leftarrow \mathsf{Enc}_{\mathsf{pk}} \circ \mathcal{P}(Q;\mu)$, $\mathsf{CList} \leftarrow \mathsf{CList}||C$,
    C を $\mathcal{A}$ に返信する.
  If($\mathcal{A}$ が復号クエリ (dec,Q) を出す)
    $(M,\mathsf{St}_{\mathcal{K}}) \leftarrow \mathcal{K}(\mathsf{pk},Q,R,\mathsf{CList},\mathsf{St}_{\mathcal{K}};\rho)$.
    M を $\mathcal{A}$ に返信する.
Return $\mathcal{A}$ の出力 S.

図 2: スタンダードモデル KI 安全性の定義で使う実験

するは攻撃者ではなく抽出者であった．我々は「攻撃者自身が平文を出力する」という直観をより直接的に定式化する．そしてこの定義は同時に,「復号オラクルは無意味である」という PA の直観をも同時に反映している．

我々の特徴づけの厳密な定義は ideal/real フレームワークを通して与えられる．より正確にいうと，我々の特徴づけは復号オラクルにアクセスできる実世界攻撃者の振る舞いと，復号オラクルにはアクセスできない理想世界攻撃者の振る舞いとの識別不能性をもって定義する．ただし，たとえ実世界攻撃者が知っている全てのデータを識別器に与えたとしても識別不能であることを要請する．さらに PA の概念を「PA = KI + IND-CPA」によって定義する．

KI の概念の我々の特徴づけはオリジナルの定義よりも簡単なので，我々の定義は KI(や PA) と他の安全性概念との関係を解析するのに適している．例えば，PA に関する最も基本的な関係式「KI + IND-CPA = PA ⇒ IND-CCA2」は我々の定義からほぼ自明に証明できる．なぜなら我々の KI の概念は「復号オラクルは無意味である」という直観を直に反映しているので，KI 安全な方式では CCA2 攻撃が CPA 攻撃と本質的に等価なことがすぐさま証明できるからである．同様に例えば「KI + Oneway-CPA ⇒ Oneway-CCA2」という関係式も自明に証明することができる．

Definition 3.1 (**スタンダードモデルにおける KI と PA の，Ideal/Real ベースの特徴づけ**). Π を公開鍵暗号方式とし，$\mathcal{A}$, $\mathcal{A}_*$，および $\mathcal{P}$ を，**実世界攻撃者** *(real adversary)*，**理想世界攻撃者** *(ideal adversary)*(または**シミュレータ** *(simulator)*)，および**平文生成機** *(plaintext creator)* と呼ばれる多項式時間機械とする．$\perp(\cdot)$ を以下のようなオラクルとする：暗号文と平文の連接を入力されると空文字列 ε を出力する．

以下の 2 つの実験を考える：

(1) : $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$, $R \leftarrow (rand)$,
  $S \leftarrow \mathcal{A}^{\mathsf{Dec}_{\mathsf{sk}},\mathsf{Enc}_{\mathsf{pk}}\circ\mathcal{P}}(\mathsf{pk};R)$, $(\mathsf{pk},R,\mathsf{List},S)$ を出力.
(2) : $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$, $R,\rho \leftarrow (rand)$,
  $S \leftarrow \mathcal{A}_*{}^{\perp,\mathsf{Enc}_{\mathsf{pk}}\circ\mathcal{P}}(\mathsf{pk},R;\rho)$, $(\mathsf{pk},R,\mathsf{List},S)$ を出力.

$\mathsf{Enc}\circ\mathcal{P}$ については定義 2.3 と同様に定義する．上の実験で List は (双方のオラクルへの) クエリと対応する答えとを連接したもののリストである．List の各エントリーはクエリされた順番にしたがって並べられる．オラクル $\mathcal{O}$ を Dec もしくは $\perp$ とするとき，$\mathcal{O} = \mathsf{Dec}$，$\mathcal{O} = \perp$ のいずれの場合も，$\mathcal{O}$-クエリとその返答を連接したものは，暗号文とメッセージを連接したものになることに注意されたい．

公開鍵暗号方式 Π が以下の成立を満たすとき，Π は**情報論的/統計的/計算量的に (スタンダードモデル)KI 安全である** という：

${}^\forall\mathcal{A}^\exists\mathcal{A}_*{}^\forall\mathcal{P}$: 上の 2 つの実験の出力は互いに
情報論的/統計的/計算量的に識別不能な分布を持つ.

Π が KI 安全でしかも IND-CPA 安全であるとき，Π は**情報論的/統計的/計算量的に PA 安全である**という.

上記の PA の特徴づけは従来のそれと同値である：

Theorem 3.2 (**PA の 2 つの特徴づけの同値性**). 公開鍵暗号方式 Π が定義 *3.1* の意味で情報論的/統計的/計算量的に *KI* 安全 *(resp. PA* 安全*)* である必要十分条件は，Π が従来の意味で意味で情報論的/統計的/計算量的に *KI* 安全 *(resp. PA* 安全*)* であることである.

定理 *3.2* の証明の概略. PA の同値性は KI の同値性から明らかに従うので，KI の同値性のみを示す.

まず用語と記号を定義する．我々の意味での KI(定義 3.1) と従来の意味での KI を区別する為，両者をそれぞれ KI-New，KI-Old と書く．さらに，$\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$, $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}}\perp}_{\Pi,\mathcal{A}_*,\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ でそれぞれ，定義 3.1 で与えた実験 (1)，(2) を表す.

(KI-Old ⇒ KI-New) $\mathcal{A}_*(\mathsf{pk},R;\rho) = \mathcal{A}^{\mathcal{K}(\mathsf{pk},\cdot;\rho)}(\mathsf{pk},R)$ とすればよい.

(KI-New ⇒ KI-Old) このパートの証明はもっと複雑である．ここでは統計的 KI-New 安全性が統計的 KI-Old 安全性を含意することのみを示す．情報論的，計算量的な場合も同じアイデアに基づいて証明できる．機械 $\mathcal{X}$, $\mathcal{Y}$ に対し，$\mathcal{X} \simeq_{\mathsf{stat}} \mathcal{Y}$ で分布 $\mathcal{X}(z)$ と $\mathcal{Y}(w)$ が (z と w を

ランダムに選べば) 統計的に識別不能なことを表す．以下簡単の為「統計的」という単語を略す．

$\mathcal{A}$ を KI-Old 安全性に対する攻撃者とする．$\mathcal{A}$ を KI-New 安全性に対する実世界攻撃者とみなすことができる．Π は KI-New 安全なので，$\mathcal{A}$ に対する理想世界攻撃者 $\mathcal{A}_*$ が存在する．

Π の KI-Old 安全性を示すには，$\mathcal{A}$ に対する抽出器 $\mathcal{K}_0$ で，圧倒的成功確率を誇るものを作る必要がある．$\mathcal{K}_0$ の構成方法のアイデアそれ自身は簡単である．$\mathcal{K}_0$ は $\mathcal{A}_*$ を実行し，$\mathcal{A}_*$ の $\perp$-クエリ $C'_1||M'_1, \ldots, C'_m||M'_m$ を得，$\mathcal{A}$ の i 番目の復号クエリに対する返答として M'_i を返す．より正確には，$\mathcal{A}$ が最初の復号クエリをしたときには $\mathcal{K}_0$ は $\mathcal{A}_*$ が $\perp$-クエリ $C'_1||M'_1$ を出すまで $\mathcal{A}_*$ を実行し，$\mathcal{A}_*$ の状態を $\mathcal{K}_0$ の状態の一部として保存し，M'_1 を出力する．$\mathcal{A}$ が二番目の復号クエリをしたときには $\mathcal{K}_0$ は (先ほど得た $\mathcal{A}_*$ の状態を使って) $\mathcal{A}_*$ を実行し，$\mathcal{A}_*$ が 2 つ目の $\perp$-クエリ $C'_2||M'_2$ を出したところで停止する．以下同様の方法で $\mathcal{A}$ の復号クエリに答えていく．$\mathcal{A}_*$ を実行するには，$\mathcal{K}_0$ は $\mathcal{A}_*$ の暗号化クエリに答えねばならない．これに答える為に $\mathcal{K}_0$ は $\mathcal{K}_0$ への入力 CList を使う．(CList は $\mathcal{A}$ の暗号化クエリとそれに対応する答えとの組からなるリスト)．すなわち，$\mathcal{A}_*$ が j 番目の暗号化クエリをしたら $\mathcal{K}_0$ は CList の j 番目の要素を $\mathcal{A}_*$ に返すのである．

しかし，$\mathcal{A}_*$ が暗号化クエリをする回数が CList のエントリーの数よりも多いかもしれない．この場合には $\mathcal{K}_0$ は $\mathcal{A}_*$ の暗号化クエリに答えることができなくなってしまう．よって我々は，$\mathcal{A}_*$ の暗号化クエリをする回数が CList のエントリーの数と同じであることを示す必要がある．

これを示す為に我々は，$\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ における List と $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}}\perp}_{\Pi,\mathcal{A}_*,\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ における List とが識別不能だという事実を使う．List の元は，クエリがなされた順番に従って並べられていたことを思い出されたい．よってもし $\mathcal{A}_*$ が i 番目の $\perp$-クエリをする前に j 個の暗号化クエリをしていたなら，$\mathcal{A}$ も i 番目の $\perp$-クエリをする前には j 個の暗号化クエリをしているはずである．従って $\mathcal{K}_0$ は常に $\mathcal{A}_*$ の暗号化クエリに答えることができる．

次に我々は，$\mathcal{K}_0$ が圧倒的成功確率を誇る抽出器だということを証明する．$\mathcal{A}^{\mathsf{Enc}\circ\mathcal{P},\mathsf{Dec}_{\mathsf{sk}}}$ と $\mathcal{A}_*{}^{\mathsf{Enc}\circ\mathcal{P},\perp}$ が統計的識別不能だったので，$\mathcal{K}_0$ の出力 M'_i は $\mathsf{Dec}_{\mathsf{sk}}(C'_i)$ と統計的識別不能である．よってもし C'_i が $\mathcal{A}$ のクエリ C_i と一致するなら，$\mathcal{K}_0$ は正しい平文を出力することになる．

もちろん，$C'_i \simeq_{\mathsf{stat}} C_i$ が成立することなら簡単に証明できる．なぜなら $\mathcal{A}$ の振る舞いと $\mathcal{A}_*$ の振る舞いは識別不能であるし，C_i と C'_i とはそれぞれ $\mathcal{A}$ と $\mathcal{A}_*$ の i 番目の復号化クエリであるから．しかし我々が要求しているのは性質 $C'_i \simeq_{\mathsf{stat}} C_i$ ではなく，より強い性質 $C_i = C'_i$ である．

一見，$C_i = C'_i$ という性質は $C'_i \simeq_{\mathsf{stat}} C_i$ という性質から自明に従うように思えるかもしれない．しかし実際にはそうではない．証明の続きを述べる前に，組 $(A(x), B(x))$ で $A \simeq_{\mathsf{stat}} B$ であるが $A(x) = B(x)$ はどんな x に対しても成り立たない例を挙げる：

$$A(0) = 0 \quad B(0) = 1$$
$$A(1) = 1 \quad B(1) = 0$$

さて $C_i = C'_i$ を示す．$\mathcal{A}$ および ($\mathcal{K}_0$ によって実行された)$\mathcal{A}_*$ は同じ入力 (pk, R) を与えられていることに注意されたい．(「同じ分布の入力」ではなく真に「同じ入力」であることに注意)．後でこの事実を $C_i = C'_i$ の証明に本質的に使う．

$C_i = C'_i$ が全ての i について成立することを証明する為，平文生成器 $\mathcal{P}$ を固定する．識別器 $\mathcal{D}_0$ で $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ の出力と $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}}\perp}_{\Pi,\mathcal{A}_*,\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ の出力を識別しようと試みるものを構成する．

$(\mathsf{pk}, R, \mathsf{List}, S'')$ で $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ もしくは $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}}\perp}_{\Pi,\mathcal{A}_*,\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ の出力を表す．$\mathcal{D}_0(\mathsf{pk}, R, \mathsf{List}, S'')$ はまず List を 2 つのパート DList と EList とに分割する．ここで DList は復号クエリとその答えの組からなるリストで，EList 暗号化クエリとその返答の組からなるリストである．次に $\mathcal{D}_0$ は DList をパースして $(C''_1||M''_1, \ldots, C''_{m''}||M''_{m''})$ とし，EList をパースして $(\hat{Q}''_1||\hat{C}''_1, \ldots, \hat{Q}''_{n''}||\hat{C}''_{n''})$ とする．$\mathcal{D}_0$ は次に $\mathcal{A}(\mathsf{pk}, R)$ を実行する．各 j に対し，$\mathcal{A}$ が j 番目の復号クエリ C_j を出したら，$\mathcal{D}_0$ は M''_j を $\mathcal{A}$ に返信する．

各 k に対し，$\mathcal{A}$ が k 番目の暗号化クエリ Q_k を出したら，$\mathcal{D}_0$ は $\hat{C}''_k$ を $\mathcal{A}$ に返信する．$\mathcal{A}$ は最後に何らかのデータ S を出力する．m，n をそれぞれ，$\mathcal{A}$ が復号クエリ，暗号化クエリを出した回数とする．もし $(m, n) = (m'', n'')$ と $(C_1, \ldots, C_m, S) = (C''_1, \ldots, C''_m, S'')$ が両方成立したら $\mathcal{D}_0$ は 1 を，そうでなければ 0 を出力する．

$\mathcal{D}_0$ への入力 $(\mathsf{pk}, R, \mathsf{List}, S'')$ が $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ の出力であるなら，$\mathcal{D}_0$ は明らかに 1 を出力する．

$\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ の出力と $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}}\perp}_{\Pi,\mathcal{A}_*,\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ の出力は互いに識別不能な分布を持っていた．よってたとえ $(\mathsf{pk}, R, \mathsf{List}, S'')$ が $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}}\perp}_{\Pi,\mathcal{A}_*,\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ の出力であったとしても，$\mathcal{D}_0$ は圧倒的な確率で 1 を出力する．

$\mathcal{D}_0$ や $\mathbf{Exp}^{\mathsf{New\text{-}KI\text{-}SM\text{-}}\perp}_{\Pi,\mathcal{A}_*,\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ の定義から分かるように，上の事実は以下のことを意味する：$\mathcal{A}_*$ の i 番目の復号クエリ C'_i と ($\mathcal{D}_0$ によって実行された)$\mathcal{A}$ の i 番目の復号クエリ C_i とは，もし $\mathcal{A}_*$ と $\mathcal{A}$ が全く同じ (pk, R) を入力されたなら，全く同じである．前述したように，実験 $\mathbf{Exp}^{\mathsf{KI\text{-}SM\text{-}}\mathcal{K}_0}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ においても $\mathcal{A}$ と ($\mathcal{K}_0$ によって実行された)$\mathcal{A}_*$ は全く同じ入力 (pk, R) を与えられる．よって実験 $\mathbf{Exp}^{\mathsf{KI\text{-}SM\text{-}}\mathcal{K}_0}_{\Pi,\mathcal{A},\mathsf{Enc}\circ\mathcal{P}}(\kappa)$ においてすら，C_i と C'_i は同じである．この事実は $\mathcal{K}_0$ が圧倒的な確率で正しい平文を出力できることを意味する．よって定理が成立する． □

—$\mathbf{Exp}^{\mathsf{KE\text{-}SM}}_{\Pi,\mathcal{A},\mathcal{K},\mathsf{Enc}}(\kappa)$—
$\mathcal{A}$，$\mathcal{K}$ のランダムテープ R，ρ をランダムに取る．
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$.
$C_0 \leftarrow \mathcal{A}^{\mathsf{Enc}_{\mathsf{pk}}}(\mathsf{pk}; R)$
$\mathsf{CList} \leftarrow$(オラクル $\mathsf{Enc}_{\mathsf{pk}}$ の答えの全てからなるリスト)
$M_0 \leftarrow \mathcal{K}(\mathsf{pk}, C_0, R, \mathsf{CList}; \rho)$.
If $M_0 = \mathsf{Dec}_{\mathsf{sk}}(C_0)$, return 1. Otherwise return 0.

図 3: スタンダードモデル KE の概念を定義するのに使う実験

4 第二の特徴づけ

この章では，ランダムオラクル KE 安全性の概念を「直接的な方法でスタンダードモデル化する」ことでスタンダードモデル KE 安全性の概念を定式化し，そしてスタンダードモデル KE 安全性を用いることで統計的スタンダードモデル PA をよりシンプルに特徴づける．ランダムオラクル PA は等式「PA = KE + IND-CPA」によって特徴付けられていたが，それに対し，我々は統計的スタンダードモデル PA がこの等式によっては特徴付けることができないことをも証明する．さらに統計的スタンダードモデル PA が「PA = KE + IND-CCA2」により特徴づけられる事を示す．

まずスタンダードモデル KE 安全性の定義を与える．前に述べたように，我々の定義はランダムオラクル KE 安全性の定義を「直接的な方法でスタンダードモデル化する」ことによって得られる．ここで「直接的な方法でスタンダードモデル化する」とは以下の操作を行うことを意味する：

- ランダムオラクルを取り除く
- 抽出者に，non-black box な方法で平文を抽出することを認める．

スタンダードモデル KE 安全性の厳密な定義を与える：

Definition 4.1 (**スタンダードモデルにおける KE 安全性**)**.** $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とする．$\mathcal{A}$，$\mathcal{K}$ を多項式機械とし，それぞれ**攻撃者**，**抽出器**と呼ぶ．κ をセキュリティ･パラメータとする．実験 $\mathbf{Exp}^{\mathsf{KE\text{-}SM}}_{\Pi,\mathcal{A},\mathcal{K},\mathsf{Enc}}(\kappa)$ を図 3 のように定義する．この実験において，C_0 は CList のエントリーであってはならない．

Π が以下を満たすとき，Π は**スタンダードモデル** *KE* **安全性**を満たすという：

$^\forall\mathcal{A}\,^\exists\mathcal{K} : \Pr(\mathbf{Exp}^{\mathsf{KE\text{-}SM}}_{\Pi,\mathcal{A},\mathcal{K},\mathsf{Enc}}(\kappa) = 1)$ は κ に関して圧倒的．

$\mathcal{K}$ が上述の性質を満たすとき，$\mathcal{K}$ は $\mathcal{A}$ に関して**圧倒的な成功確率を誇る** *(successful)* という．

次にスタンダードモデル KE の性質を調べる．ランダムオラクルモデルの場合，PA 安全性，KE 安全性，および IND-CCA2 安全性は以下の基礎的な関係式「PA = KE + IND-CPA ⇒ IND-CCA2」を満たしていた。しかしスタンダードモデルでは「KE + IND-CPA ⇒ PA」や「KE + IND-CPA ⇒ IND-CCA2」が成立しないことが証明できる。(証明略)

Theorem 4.2 (**KE + IND-CPA は PA よりも真に弱い**)**.** スタンダードモデル *KE* 安全性と *IND-CCA2* 安全性をともに満たす公開鍵暗号方式が少なくとも一つ存在したとする．このとき公開鍵暗号方式で，スタンダードモデル *KE* 安全かつ *IND-CPA* 安全であるにもかかわらず，情報論的 *PA*，統計的 *PA*，計算量的 *PA*，および *IND-CCA2* 安全性のいずれも満たさないものが存在する．

上述の定理はスタンダードモデルにおける KE 安全性，PA 安全性，および IND-CCA2 安全性の関係がランダムオラクルモデルにおける関係とは全く異なることを意味する．さらに，統計的 PA 安全性が等式「PA = KE + IND-CCA2」によって特徴付けられることを見る。(証明略)

Theorem 4.3 (**KE + IND-CCA2 = 統計的 PA**)**.** 公開鍵暗号方式 Π が *KE* 安全性と *IND-CCA2* 安全性を共に満たすための必要十分条件は，Π が統計的 *PA* 安全であることである．

この定理は，PA に関する基本定理「PA ⇒ IND-CCA2」がある意味トートロジーであることを意味している．なぜなら，特徴づけ「PA = KE + IND-CCA2」の中に IND-CCA2 安全性自身が登場しているからである。

5 計算量的 PA に対する否定的事実

4 章で我々は統計的 PA 安全性はスタンダードモデル KE 安全性によって特徴づけることができることを証明した．それに対しこの章では，上で説明した事実の計算量バージョンは成立しないことを示す．すなわち我々は，計算量 PA 安全性はスタンダードモデル KE 安全性の計算量バージョンでは特徴づけることができないことを証明する．

この事実を示す為，まず我々は定義 2.3 で与えた (スタンダードモデル)KE 安全性の概念を計算量の場合に拡張しなければならない．しかし，KE 安全性の概念をいかにして計算量の場合に拡張すればよいかは判然としない．そこで我々は，まず KE 安全性の概念の別定義を与え，その別定義を拡張することで KE 安全性の計算量バージョンを定義する．

KE 安全性の別定義は、KE 安全性のもとの定義を与える際に使用した実験 $\mathbf{Exp}^{\mathsf{KE\text{-}SM}}_{\Pi,\mathcal{A},\mathcal{K},\mathsf{Enc}}(\kappa)$ を利用して定義される．pk，C_0，M_0，M_0' をそれぞれ $\mathbf{Exp}^{\mathsf{KE\text{-}SM}}_{\Pi,\mathcal{A},\mathcal{K},\mathsf{Enc}}(\kappa)$ における公開鍵，$\mathcal{A}$ の出力，$\mathsf{Dec}_{\mathsf{sk}}(C_0)$，および $\mathcal{K}$ の出力と

$\mathbf{Exp}^{\mathsf{KE\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}}(\kappa)$ —
$\mathcal{A}$ のランダムテープ R をランダムに選ぶ.
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$.
$C_0 \leftarrow \mathcal{A}^{\mathsf{Enc}_{\mathsf{pk}}}(\mathsf{pk}; R)$

$M_0 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(C_0)$.
Return (pk, C_0, M_0).

— $\mathbf{Exp}^{\mathsf{KE\text{-}SM\text{-}}\mathcal{K}}_{\Pi,\mathcal{A},\mathsf{Enc}}(\kappa)$ —
$\mathcal{A}$, $\mathcal{K}$ のランダムテープ R, ρ をランダムに選ぶ.
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$.
$C_0 \leftarrow \mathcal{A}^{\mathsf{Enc}_{\mathsf{pk}}}(\mathsf{pk}; R)$
$\mathsf{CList} \leftarrow$(オラクル $\mathsf{Enc}_{\mathsf{pk}}$ の答えの全てからなるリスト)
$M_0 \leftarrow \mathcal{K}(\mathsf{pk}, C_0, R, \mathsf{CList}; \rho)$.
Return (pk, C_0, M_0).

図 4: KE安全性の別定義に用いる実験

する．KE安全性の別定義は (pk, C_0, M_0) と (pk, C_0, M_0') の識別不能性をもって定義する．より正確には，以下のようにしてKE安全性の別定義を与える：

Definition 5.1 (**スタンダードモデルKE安全性の，シミュレーションベースの定義**). $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とする．$\mathcal{A}$ と $\mathcal{K}$ を多項式時間機械とし，それぞれ**攻撃者**，**抽出者**と呼ぶ．二つの実験 $\mathbf{Exp}^{\mathsf{KE\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}}(\kappa)$, $\mathbf{Exp}^{\mathsf{KE\text{-}SM\text{-}}\mathcal{K}}_{\Pi,\mathcal{A},\mathsf{Enc}}(\kappa)$ を図 4 のように定義する．Π が**情報論的/統計的/計算量的KE安全**であるとは次が成立するときにいう：

> $\forall\mathcal{A}\exists\mathcal{K}$: $\mathbf{Exp}^{\mathsf{KE\text{-}SM\text{-}Dec}}_{\Pi,\mathcal{A},\mathsf{Enc}}(\kappa)$ の出力の分布と
> $\mathbf{Exp}^{\mathsf{KE\text{-}SM\text{-}}\mathcal{K}}_{\Pi,\mathcal{A},\mathsf{Enc}}(\kappa)$ の出力の分布は
> 情報論的/統計的/計算量的に識別不能.

上で定義した統計的KE安全性がもとのKE安全性の定義と一致することを簡単に確かめることができる．

Proposition 5.2 (**2つのKEの定義の同値性**). 公開鍵暗号方式 Π が定義 *4.1* の意味で *KE* 安全である必要十分条件は，Π が定義 *5.1* の意味で統計的 *KE* 安全なことである．

また，Π が定義 *5.1* の意味で情報論的 *KE* 安全である必要十分条件は，定義 *4.1* の意味での *KE* 安全性の定義に「抽出器 $\mathcal{K}$ が平文抽出に失敗することは絶対にない」という条件をつけ加えたものを Π が満たすことである．

よって特に以下の命題が成り立つ：

Proposition 5.3 (**統計的KE + IND-CCA2 = 統計的PA**). 公開鍵暗号方式 Π が統計的 *KE* と *IND-CCA2* と満たす必要十分条件は，Π が統計的 *PA* 安全性を満たすことである．

しかし上の命題は計算量的PAの場合には成立しない．

Theorem 5.4 (**計算量的KE + IND-CCA2 $\not\Rightarrow$ 計算量的PA**). 一方向性置換と統計的 *PA* 安全な公開鍵暗号方式が存在したとする．このとき，計算量的 *KE* 性と *IND-CCA2* 性を両方あわせても，計算量的 *PA* 安全性を含意しない．すなわち，計算量的 *KE* 安全かつ *IND-CCA2* 安全な公開鍵暗号方式で，計算量的 *PA* 安全でないものが存在する．

計算量的KI安全性と計算量的KE安全性との根本的違いは，攻撃者が抽出者に対して適応的に復号クエリを行えるか否かにある．実際，攻撃者が抽出者に適応的には復号クエリを投げることができないことを要請しさえすれば，定理 5.4 は計算量的KE安全性の他のバージョンに対しても成立する．たとえば，定理 5.4 は以下のように改変したより強いバージョンの計算量的KE安全性に対しても成立する：

- $\mathcal{A}$ は平文生成器に暗号化クエリを投げるよう命令することができる．
- 識別器は「攻撃者 $\mathcal{A}$ の知っているデータ」を全て見ることができる．ここで「攻撃者 $\mathcal{A}$ の知っているデータ」とは，たとえば $\mathcal{A}$ のランダムテープや暗号化オラクルからの返答など．

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 and 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.

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

[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.

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

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

[TO06] Isamu Teranishi, Wakawa Ogata. Relationship between Standard Model Plaintext Awareness and Message Hiding. ASIACRYPT 2006. (日本語版：スタンダードPA + 一方向性 $\Rightarrow$ IND-CPA, SCIS 2007).