CCA 安全な公開鍵暗号の概念と設計の指針 —より実用的な公開鍵暗号の実現に向けて—

Methodologies for Achieving Chosen-Ciphertext Security of Public Key Encryption
—Towards More Practical Public Key Encryption—

花岡 悟一郎 Goichiro HANAOKA

アブストラクト 本稿では、実用的な公開鍵暗号方式に求められる安全性の概念である CCA 安全性（選択暗号文攻撃に対する識別不可性）について紹介し、それを達成するための方法論を紹介する．特に、CCA 安全な公開鍵暗号を設計する上での具体的な技術的な障害を明らかにし、そのような障害が過去にどのように乗り越えてこられてきたかをできるだけ系統立てて紹介する．

キーワード 公開鍵暗号，選択暗号文攻撃，証明可能安全性

1. はじめに

より高度に安全な公開鍵暗号の追求は、暗号理論における最も重要な研究課題の一つである．しかしながら、一般的に安全性と効率性はトレードオフの関係にあり、大雑把にいうと、安全性を必要以上に高めることは効率性の低下につながるため、1990 年代半ばまでは、実運用の現場において CCA 安全性（IND-CCA と呼ばれる）のような高度な安全性は必ずしも求められてはいなかった．しかしながら、1998 年の Bleichenbacher⁽¹⁾により、PKCS#1 ver.1.5 における RSA 暗号の実装が現実的に攻撃可能であることが示されたことを契機として、CCA 安全性の実用上の重要性も強く社会に認識され、現在に至っては CCA 安全であることが実用的な公開鍵暗号であることの最低条件の一つとさえみなされている．興味深いことに、CCA 安全性の概念がほぼ“常識”として当該研究分野において広く認識される一方で、その設計のための方法論は決して理解が容易でない．

本稿の主たる目的は、CCA 安全性を達成する上での具体的な技術的困難性及びその解決方法の数々を系統立てて説明することで、CCA 安全な公開鍵暗号の設計方法について興味を持つ読者に有益な情報を提供することにある．

2. CCA 安全性とは？

CCA 安全性を実現するための方法論に先立ち、本章ではまず CCA 安全性の概念について説明を行う．CCA 安全性⁽²⁾⁽³⁾とは、選択暗号文攻撃に対する識別不可能性の意であり、その直感的な定義は次のとおりである： C^* を解読の対象となる暗号文とする．また、 C^* の解読を試みる攻撃者は、 C^* の正規受信者

に対して任意の暗号文を任意の回数だけ送信することを許され、それが C^* でない限り正規受信者からその正しい復号結果を得られるものとする．そのような（この上なく暗号解読に有利な）攻撃環境下においても、いかなる攻撃者であっても、 C^* の復号結果に関するいかなる部分情報すらも解読できないような安全性を CCA 安全性と呼ぶ．

当該研究分野になじみのない読者にとって、上記の CCA 安全性の概念は一見して不自然に見えるかもしれない．つまり、攻撃の被害者である正規受信者自身が、この上ない形で攻撃者の補助をするという攻撃環境が想定されており、余りに現実とはく離れた概念にも思える．したがって、そのような意味もなく高度な安全性を達成することで効率性を犠牲にすることがあれば、そのような安全性を目指すべきではない、と感じる読者もいることだろう（そして、実装の現場では、1990 年代半ばまで実際にそのように考えられていたであろうことがうかがえる．）

しかし、様々な細かな根拠を積み上げると、CCA 安全性が実用の意味でも極めて妥当な安全性の概念であることが分かる．以下では、そのような根拠の主な具体例を挙げる．

2.1 攻撃環境に関する一つの上界となる

一つ目の根拠は、正規利用者が任意の暗号文に対する復号結果を攻撃者に返答するという攻撃モデル（いわゆる、選択暗号文攻撃）は（復号鍵もしくは解読対象の平文の漏えい以外に）実際に生じ得るいかなる攻撃環境よりも攻撃者にとって有利であるという点になる．ここで注意すべきは、実際に生じ得る攻撃環境のうち最も強いものが何であるかを我々が知る由もなく（だからこそ、その間げきについて Bleichenbacher の攻撃が出現したと解釈できる）、そのため、当然、実際に生じ得る最強の攻撃を定義することはほとんど不可能である．一方、選択暗号文攻撃は、実際に生じ得るものとは到底考えられないが、実際に生じ得るすべての攻撃環境よりも強く、また、数学的な定義

花岡 悟一郎 独立行政法人産業技術総合研究所 情報セキュリティ研究センター
E-mail hanaoka-goichiro@aist.go.jp
Goichiro HANAOKA, Nonmember (RCIS, AIST, 1-18-13 Sotokanda, Chiyoda-ku, Japan, 101-0021).
Fundamentals Review Vol.3 No.1 pp.21-31 2009 年 7 月

が可能である．言い換えれば，攻撃環境の一つの上界になっており，この攻撃環境に対する安全性だけを考えていれば，いかなる実際の攻撃環境に対する安全性もおおのずと保証されることになる．

2.2 部分解読不可能性よりも高度な安全性も含意

次の根拠は，CCA 安全性が，その定義が直接的に示唆する安全性よりも更に高度な安全性も自動的に含んでいる点である．そのため，ほぼすべての暗号プロトコルに関する構成要素としての公開鍵暗号の安全性要件を満足するものとなっている．つまり，例えば，攻撃者の目的が平文の不正な解読ではなく，平文内の特定のビットを反転させる等の自分が意図した操作を加えることであった場合，一般的には単なる部分解読不可能性だけでは安全性として不十分である．電子入札のような暗号プロトコルにおいては，実際にそのような性質が求められることがある．また，そのような性質は頑強性などと呼ばれる⁽²⁾．興味深いことに，CCA 安全な公開鍵暗号は，必ず同時に（選択暗号文攻撃の下での）頑強性も満足することが示されている⁽⁴⁾．また，そのほか，CCA 安全な公開鍵暗号は，どのような暗号プロトコルの構成要素として用いても期待される安全性が損なわれない性質（所謂，はん用結合可能性⁽⁵⁾）を持つことも示されている．

2.3 安全性定義が簡潔

三つ目の根拠としては，CCA 安全性の定義自体がとても簡潔である点が挙げられる．それゆえ，この安全性の概念を満足することの現実的な意味合いをだれでも理解しやすく，また，この安全性を満足していると主張する根拠（すなわち，安全性証明）の検証を行いやすい．例えば，前述のように，元々部分解読不可能性よりも強い安全性の概念として頑強性が知られており，したがって（選択暗号文の下での）頑強性を満足するかどうかだけを判断すれば，公開鍵暗号の安全性についての議論は十分であった．しかしながら，頑強性の定義は，非常に複雑であるため，そのような性質を持つ方式を設計することも，また，そのような性質を持つことを検証することも容易ではなかった．それに対し，CCA 安全性の概念は簡潔であるばかりか自動的に頑強性（やはん用結合可能性）も含意しているため，高度に安全な公開鍵暗号の設計及びその安全性の検証を著しく簡略化するものとなっている．

3. CCA 安全性の定義

ここでは，CCA 安全性の具体的な定義について記述する．

3.1 公開鍵暗号

CCA 安全性の定義に先立ち，まずは，公開鍵暗号のモデル化を行う．

定義 1. 公開鍵暗号方式 Π は，鍵生成アルゴリズム GEN，暗号化アルゴリズム ENC，復号アルゴリズム DEC の三つのアルゴリズムの組として定義される．

GEN: 1^k を入力とし，復号鍵と公開鍵のペア (dk, pk) を出力する確率的アルゴリズム．ここで， k はセキュリティパラメータとする．

ENC: 平文 M と公開鍵 pk を入力とし，暗号文 C を出力する確率的アルゴリズム（もしくは，確定的アルゴリズム）．

DEC: 暗号文 C と復号鍵 dk を入力とし，平文 M （もしくは，失敗を表すシンボル “ $\perp$ ”）を出力する確定的アルゴリズム．

受信者は GEN により鍵ペアを生成し，また，このうち公開鍵を周知にする．送信者は ENC により平文を受信者の公開鍵で暗号化し，受信者に送信する．受信者は DEC により，復号鍵を用いて受信した暗号文の復号を行う．

3.2 CCA 安全性

上記のモデルにおいて，公開鍵暗号の CCA 安全性は次のように定義される．

定義 2. 任意の多項式時間アルゴリズム $A = (A_1, A_2)$ に対して， $\Pi = (\text{GEN}, \text{ENC}, \text{DEC})$ が次式を満足するとき， Π は選択暗号文攻撃に対して識別不可能（CCA 安全）であるという．

$$|\Pr[\text{Exp}_{\Pi, A}^{in, d-1} = 1] - \Pr[\text{Exp}_{\Pi, A}^{in, d-0} = 1]| < \epsilon$$

ここで， ϵ は無視できる値とし，また， $\text{Exp}_{\Pi, A}^{in, d-b}$ は， $b \in \{0, 1\}$ に対し，次のように定義される試行とする：

```

ExpΠ, Ain, d-b
   $(dk, pk) \leftarrow \text{GEN}(1^k); (M_0, M_1, s) \leftarrow A_1^{\mathcal{O}}(pk);$ 
   $C^* \leftarrow \text{ENC}(M_b, pk); b' \leftarrow A_2^{\mathcal{O}}(M_0, M_1, C^*, pk, s);$ 
  return  $b'$ .

```

ここで， $\mathcal{O}$ は，任意の質問 $C(\neq C^*)$ に対して， $\text{DEC}(C, dk)$ を返答する復号オラクルとする．また， s は， A の内部状態を表すパラメータとする．

4. CCA 安全性達成への技術的障害

CCA 安全性の定義自体はとても容易であるにもかかわらず，その安全性を達成すること自体は決して容易でない．実際，ごく最近まで CCA 安全な実用的公開鍵暗号の構成方法は，極めて強い仮定（例えばランダムオラクルモデル）に依存するものを除くと，Cramer-Shoup 暗号⁽⁶⁾とその変形方式（例えば，Kurosawa-Desmedt 暗号⁽⁷⁾）ぐらいしか知られていなかった．そこで，本章では，議論の中心となる具体的な問題を明らかにすべく，CCA 安全な公開鍵暗号を設計する上での技術的障害をなるべく平易に説明することを目的とする．

図 1 一般的な安全性証明の流れ

図 2 CCA 安全性を証明する上での一般的障害

4.1 一般的な安全性証明手順

ここでは、まず、CCA 安全性に限定しない一般的な安全性証明の手順を振り返ってみる。ある公開鍵暗号方式 Π が安全性レベル L を持つことを証明するためには、 Π の L に関する安全性を破ることができるような攻撃者 A の存在を仮定して、それによって何らかの矛盾が引き出されることを示せば十分である。例えば、これまでに現在の人類の科学力では解くことが極めて困難である数学的問題が幾つか知られているが、 A の存在を仮定することでそのような数学的問題のどれか一つ（仮に P とする）を解くことが可能となることがあれば、(P を解く方法が発見されない限り) それは矛盾であり、 A の存在を仮定したことが間違っていたことになる。すなわち、暗号方式 Π を安全性 L の意味で破る攻撃者は一切存在しないことになる。

上記の議論によれば、つまり、安全性の証明（の一つの方針）としては、 Π を L の意味で破る攻撃者 A をサブルーチンとして、 P を解くアルゴリズムを構成してやればよいことが分かる。これを、図 1 を用いて大雑把に説明する：まず、与えられた問題 P （のインスタンス）を、現実の攻撃における A への入力と識別不可能なものになるように変換する。例えば、 Π の公開鍵等に変換されることになる。その上で、これを A に入力し（自分が置かれている環境が現実の攻撃環境と識別できない限り） A は与えられた入力に対する正しい解読結果 M を出力する。この M に更に変換を施し、問題 P の解 S を得ることができれば、安全性の証明がなされたことになる。

ここで注意しなければならないのは、 A はあくまで Π を L の意味で破るアルゴリズムであり、したがって、 A には実際に Π を L の意味で破る際の攻撃環境（と識別不可能な環境）を与えてやらなければならないことである。例えば、 A が Π を CCA 安全性の意味で破る攻撃者であるならば、 A から発せられる復号オラクル $\mathcal{O}$ への質問 C に対して、正しく $\text{DEC}(C, dk)$ を返答してやらない限り、 A は期待される動作を行うことはない。

4.2 CCA 安全性の証明上の一般的問題

前述のとおり、CCA 安全性を証明する際、 A には現実の選択暗号文攻撃環境と識別できないような環境を与えてやらない限り、 A からの正しい解読結果の出力は期待できない。つまり、 A の発する質問に正しく返答できない限り、問題 P の解 S を得ることはできないことになる。これを考慮した上で、図 1 を CCA 安全性についての議論に特化した形で修正を施したものが図 2 となる。

図 2 に示されるように、安全性証明の大きい流れは図 1 のとおりであるが、 A が M を正しく出力するためには、 A からの質問に対して正しく返答を行う必要がある。つまり、 A から発せられる暗号文 C に対して、その復号結果を返さなければならない。しかしながら、多くの場合において復号鍵は問題 P の解 S （もしくは容易に S を導出可能なある値）に相当するため、 S を知らない限りそのような返答を行うことは非常に困難となる。言い換えれば、 S を導出するためには、 S が必要というデッドロックともいえる状況が生じていることが分かる。またそれゆえ、1980 年代以前においては、CCA 安全性は達成不可能とさえ思われていた。

つまり、CCA 安全な公開鍵暗号やその安全性を証明する技術的障害とは、上記の一見不可避とも思えるデッドロックを回避しなければならないことである。次章から、そのようなデッドロックを乗り越える具体的な手法について順序立てて説明を行っていく。

5. エルガマル暗号を用いた失敗例

前述のデッドロックを乗り越えることの困難性をより深く理解するために、単純なエルガマル暗号ではどのように乗り越えることに失敗しているかを議論してみることにする。以下においては $\mathbb{G}$ を位数が素数 p となる乗法群とする。このとき、エルガマル暗号の構成は次のとおりとなる：

エルガマル暗号⁽⁸⁾

鍵生成: $g \in \mathbb{G}$ と $x \in_R \mathbb{Z}_p$ を選び、 $y = g^x$ を計算する。復号鍵 $dk = x$ 及び公開鍵 $pk = (g, y)$ を出力する。

図3 エルガマル暗号のCCA安全性の証明を試みる際に生じるデッドロック

暗号化: 平文 M 及び公開鍵 pk に対し, 乱数 $r \in_R \mathbb{Z}_p$ を選び $c_1 = g^r$ を求める. また, $K = y^r$ を計算し, 共通鍵 K を用いて M に共通鍵暗号化^(注1)を施した c_2 を導出し, 暗号文 $C = (c_1, c_2)$ を出力する.

復号: 暗号文 $C = (c_1, c_2)$ 及び復号鍵 dk に対し, まず, $K = c_1^x$ を計算し, K を共通鍵として用いて c_2 を復元し M を得る.

ここで, 上記のエルガマル暗号が CCA 安全性を持たないことを, 前章の表現に合わせて議論してみる. すなわち, CCA 安全性を証明する際の主たる技術的障害である前述のデッドロックがエルガマル暗号においてはどのように出現するのかを明らかにする. なお, 以下では, 直感的な理解を優先し, 攻撃者として, 与えられた公開鍵と解読対象の暗号文 (のうち共通鍵暗号化が施された部分以外) からその暗号文の内部で用いられている共通鍵 K^* を導出するもののみに限定して議論を行う. 本章以降においても, 同様に, 解読対象の暗号文に用いられる共通鍵 K^* を導出する攻撃者に限定して議論を行うものとする. また, 安全性の帰着先となる数学的問題 P として, ディフィ・ヘルマン計算 (CDH) 問題を考えるものとする. CDH 問題は次のように定義される.

定義 3 (CDH 問題). 群 $\mathbb{G}$ に対し, $(h, h^a, h^b) \in_R \mathbb{G}^3$ が与えられたとき, $h^{ab} \in \mathbb{G}$ を求める問題を $\mathbb{G}$ におけるディフィ・ヘルマン計算 (CDH) 問題と呼ぶ.

図3に, エルガマル暗号の CCA 安全性を CDH 問題の困難性の仮定 (すなわち, CDH 仮定) の下で証明しようと試みた場合に出現する問題の所在を示す. 今, 攻撃者 A として公開鍵 $pk = (g, y)$ と解読対象の暗号文 C^* の一部 c_1^* を入力すると, 選択暗号文攻撃を行った上で, C^* の内部で用いられている共通鍵 $K^*(= c_1^{*x})$ を導出するものを考える. そのような A に対し, CDH 問題において与えられた (h, h^a, h^b) を用いて,

$pk = (g, y) = (h, h^a)$, $c_1^* = h^b$ において, A に入力する (このとき, pk と c_1^* の分布は実際の攻撃環境と同一であることに注意されたい). このとき, A から発せられるすべての質問に正しく返答できれば, A は $c_1^{*a} = h^{ab}$ を出力する. また, これはそのまま CDH 問題の解となっている. つまり, A からの質問に正しくこたえることさえできれば, 安全性の証明がなされたことになる.

しかし, A からの質問にこたえるためには, $pk = (h, h^a)$ に対応する復号鍵が必要であり, それは a にほかならない. そして, a を用いることで, そもそも (A の協力を得るまでもなく) 容易に CDH 問題を解くことができる. 言い換えれば, A に (a を用いれば簡単に求まる値である) h^{ab} を求めさせるには, あらかじめ a を知っていることが必要というデッドロックが生じていることが確認できる.

6. Naor-Yung 方式

CCA 安全性の原型となる弱い概念は, Naor と Yung⁽⁹⁾によって定義がなされ, また, その具体的な達成方法も同時に提案されている^(注2). また, Naor-Yung 方式において用いられる非対話ゼロ知識 (NIZK) 証明として, より強い安全性を持つものに置き換えることで CCA 安全性が達成できることが Sahai によって示されている⁽¹⁰⁾. Naor-Yung (-Sahai) 方式の興味深い特徴の一つは, 選択平文攻撃に対して安全な任意の公開鍵暗号と NIZK 証明から, CCA 安全な公開鍵暗号を構成できることにあるが, 本稿においては方式同士の構造の比較のしやすさを考慮し, 構成要素となる公開鍵暗号をエルガマル暗号に限定する (エルガマル暗号に基づく) Naor-Yung 方式の構成は次のとおりである:

エルガマル暗号に基づく Naor-Yung 方式^{(9) (10)}

鍵生成: $g \in \mathbb{G}$ と $x_0, x_1 \in_R \mathbb{Z}_p$ を選び, $y_0 = g^{x_0}$, $y_1 = g^{x_1}$ を計算する. また, NIZK 証明のためのランダムビット列 R を適当に選ぶ. 復号鍵 $dk = (x_0, x_1)$ 及び公開鍵 $pk = (g, y_0, y_1, R)$ を出力する.

暗号化: 平文 M 及び公開鍵 pk に対し, 乱数 $r \in_R \mathbb{Z}_p$ を選び $c_1 = g^r$ を求める. また, $K \in_R \mathbb{G}$ を選び, $c_2 = K \cdot y_0^r$, $c_3 = K \cdot y_1^r$ を計算し, また R を用いてそのような手順にて (c_1, c_2, c_3) を作成したことを示す NIZK 証明 π を作成する. 次に, 共通鍵 K を用いて M に共通鍵暗号化^(注3)を施した c_4 を導出し, 暗号文として $C = (c_1, c_2, c_3, c_4, \pi)$ を出力する.

復号: 暗号文 $C = (c_1, c_2, c_3, c_4, \pi)$ 及び復号鍵 dk に対し, まず, π の正当性を検証し, C が正しい手順で作成された暗号文であることを確認する. これが確認できたら, $K = c_2 \cdot (c_1^{x_0})^{-1}$ を計算し (c_3 と x_1 を用いてもよい), c_4 を共通鍵 K で復元し M を得る.

(注1): ここでは, 安全でない例を議論しているので, この共通鍵暗号化の安全性の要件は特に問わない. ただし, この共通鍵暗号が暗号文単独攻撃に対して安全なものであれば, 暗号方式全体として選択平文攻撃への安全性が保証可能となる.

(注2): 文献によっては, 本稿で述べるところの CCA 安全性を IND-CCA2 と呼び, Naor と Yung の定義によるものを IND-CCA1 と呼んでいる.

(注3): ここでは, 共通鍵暗号として CCA 安全な DEM⁽¹¹⁾であることが求められる. 以降の方式についても同様.

図 4 Naor-Yung 方式の安全性証明の概観

次に、Naor-Yung 方式でどのように前述のデッドロックが解消されているかの直感的な説明を与える^(注4)。これまでと同様の図を用いて、いかにして安全性証明が可能となったのかを説明する。図 4 に証明の大きい流れを示す：Naor-Yung 方式では x_0 か x_1 のうちのどちらか一方を知っていれば復号できることがデッドロックを回避する大きな核となる。この際、NIZK 証明により x_0 と x_1 のどちらを用いて復号しても、同じ結果が得られることが保証されていることに注意されたい。つまり、 y_0, y_1 の一方を（上記のエルガマル暗号の場合と同様に） h^a としながら、それと同時に、自分自身で乱数 $t \in \mathbb{Z}_p$ を選んでやりもう一方を h^t として攻撃者に入力してやることで（図中では、NIZK 証明に関する記述は省略する）、上記のエルガマル暗号の場合と同様にして A に h^{ab} を解かせながら、 A から発せられる質問については“復号鍵” t を用いて正確に返答することが可能となる。つまり、エルガマル暗号の証明の試みの際に見られたデッドロックが回避されていることが分かる。なお繰り返し述べるが、この説明はあくまで直感的な理解を優先したものであり、厳密には誤りがある^(注5)。正確な証明に興味ある読者は、本稿を足掛かりとした上で、しかるべき文献に当たられるのがよいだろう。

ところで、上記のエルガマル暗号に基づく Naor-Yung 方式が下記のように効率化可能である。この変形方式は、後述の Cramer-Shoup 暗号との接点を議論する場合、有用となる。

エルガマル暗号に基づく変形 Naor-Yung 暗号

鍵生成: $g \in \mathbb{G}$ と $x_0, x_1 \in \mathbb{Z}_p$ を選び、 $y_0 = g^{x_0}, y_1 = g^{x_1}$ を計算する。また、NIZK 証明のためのランダムビット列 R を適当に選ぶ。復号鍵 $dk = (x_0, x_1)$ 及び公開鍵 $pk = (g, y_0, y_1, R)$ を出力する。

暗号化: 平文 M 及び公開鍵 pk に対し、乱数 $r \in \mathbb{Z}_p$ を選び $c_1 = g^r$ を求める。また、 $K = y_0^r$ 及び $c_2 = y_1^r \cdot y_1^r$ を計算し、また R を用いてそのような手順にて (c_1, c_2) を作成した

ことを示す NIZK 証明 π を作成する。次に、共通鍵 K を用いて M に共通鍵暗号化^(注6)を施した c_3 を導出し、暗号文として $C = (c_1, c_2, c_3, \pi)$ を出力する。

復号: 暗号文 $C = (c_1, c_2, c_3, \pi)$ 及び復号鍵 dk に対し、まず、 π の正当性を検証し、 C が正しい手順で作成された暗号文であることを確認する。これが確認できたら、 $K = c_1^{x_0}$ もしくは $K = c_2 \cdot (c_1^{x_1})^{-1}$ を計算し（どちらでも同じ計算結果になる）、 c_3 を共通鍵 K で復元し M を得る。

この変形方式においては、共通鍵 K をランダムに選ぶのではなく、 $K = y_0^r$ としてやることで、元々の方式における暗号文の一要素を取り除けることを意味している。

7. Cramer-Shoup 方式

前述の Naor-Yung 方式のアイデアは、どちらを用いても復号可能な二つの鍵を用意して、その一方に興味ある問題を埋め込み、もう一方を使って攻撃者からの質問にこたえていくというものであった。しかしながら、これら二つの鍵のどちらを用いても同じ復号結果が得られることを保証せねばならず、そのため NIZK 証明が必要であった。言い換えれば、この NIZK 証明に相当する部分を効率的に構成することができれば、暗号文全体のサイズも著しく小さくできるものと期待できる。

Cramer-Shoup 暗号⁽⁶⁾は著名な暗号方式であり、その解釈の方法は様々なものが存在するが、その一つとして上記のエルガマル暗号に基づく Naor-Yung 方式における NIZK 証明に相当する部分を効率化したものと説明付けすることもできる^(注7)。Cramer-Shoup 方式の構成は次のとおりである：

Cramer-Shoup 暗号⁽⁶⁾

鍵生成: $g, h \in \mathbb{G}$ と $w_0, w_1, w_2, w_3, w_4, w_5 \in \mathbb{Z}_p$ を選び、 $z_0 = g^{w_0}h^{w_1}, z_1 = g^{w_2}h^{w_3}, z_2 = g^{w_4}h^{w_5}$ を計算する。また、はん用一方向性ハッシュ関数 TCR を選ぶ。復号鍵 $dk = (w_0, \dots, w_5)$ 及び公開鍵 $pk = (g, h, z_0, z_1, z_2, \text{TCR})$ を出力する。

暗号化: 平文 M 及び公開鍵 pk に対し、乱数 $r \in \mathbb{Z}_p$ を選び $c_1 = g^r, c_2 = h^r$ を求める。また、 $\alpha = \text{TCR}(c_1, c_2), \pi = (z_0 z_1^\alpha)^r, K = z_2^r$ を計算し、共通鍵 K を用いて M に共通鍵暗号化^(注8)を施した c_3 を導出し、暗号文として $C = (c_1, c_2, c_3, \pi)$ を出力する。

復号: 暗号文 $C = (c_1, c_2, c_3, \pi)$ 及び復号鍵 dk に対し、まず、 π の値が $c_1^{w_0} c_2^{w_1} c_1^{\alpha w_2} c_2^{\alpha w_3}$ と一致するかを検証する。ここで、 $\alpha = \text{TCR}(c_1, c_2)$ とする。これが確認できたら、 $K = c_1^{w_4} c_2^{w_5}$

(注4): これはあくまで直感的な説明であり、厳密には誤っている。ただし、本格的な理解をする上での導入としては、このような説明が優れていると考え、本稿ではそのような説明方法を採用している。

(注5): ここで述べている証明の方針を用いる場合、CDH 問題のような決定問題に安全性を帰着させることは実際には難しい。そのため、DDH 問題のような判定問題に強く依存することになる。

(注6): ここでは、共通鍵暗号として CCA 安全な DEM⁽¹¹⁾であることが求められる。

(注7): この解釈は、Cramer-Shoup 暗号の原論文⁽⁶⁾に記載の安全性証明の指針とは隔たりがある。しかし、このような解釈に基づいた異なる証明が実際に可能であり、また、このような解釈を用いた場合 Naor-Yung 方式との関係をより深く理解することができる。

(注8): 共通鍵暗号として CCA 安全な DEM⁽¹¹⁾であることが求められる。

を計算し、 c_3 を共通鍵 K で復元し M を得る。

上述のとおり、Cramer-Shoup 方式がどのように設計されているかについては、多様な解釈が可能であるが、ここでは、これをエルガマル暗号の性質を利用して更に効率化された Naor-Yung 方式とみなした上での説明を試みる。説明を容易にするべく、Cramer-Shoup 方式の構成について数学的表現を次のように改めるものとする：

表現を改めた Cramer-Shoup 暗号

鍵生成: $g \in \mathbb{G}$ と $x_0, x_1, w_0, w_1, w_2, w_3 \in_R \mathbb{Z}_p$ を選び、 $h = g^{x_0} g^{x_1}$, $z_0 = g^{w_0} h^{w_1}$, $z_1 = g^{w_2} h^{w_3}$, $z_2 = g^{x_0}$ を計算する。また、はん用一方向性ハッシュ関数 TCR を選ぶ。復号鍵 $dk = (x_0, x_1, w_0, \dots, w_3)$ 及び公開鍵 $pk = (g, h, z_0, z_1, z_2, \text{TCR})$ を出力する。

暗号化: 平文 M 及び公開鍵 pk に対し、乱数 $r \in_R \mathbb{Z}_p$ を選び $c_1 = g^r$, $c_2 = h^r$ を求める。また、 $\alpha = \text{TCR}(c_1, c_2)$, $\pi = (z_0 z_1^\alpha)^r$, $K = z_2^\alpha$ を計算し、共通鍵 K を用いて M に共通鍵暗号化^(注9)を施した c_3 を導出し、暗号文として $C = (c_1, c_2, c_3, \pi)$ を出力する。

復号: 暗号文 $C = (c_1, c_2, c_3, \pi)$ 及び復号鍵 dk に対し、まず、 π の値が $c_1^{w_0} c_2^{w_1} c_1^{\alpha w_2} c_2^{\alpha w_3}$ と一致するかを検証する。ここで、 $\alpha = \text{TCR}(c_1, c_2)$ とする。これが確認できたら、 $K = c_1^{x_0}$ もしくは $K = c_2 \cdot (c_1^{x_1})^{-1}$ を計算し（どちらでも同じ計算結果が得られる）、 c_3 を共通鍵 K で復元し M を得る。

この方式と、前述の Cramer-Shoup 方式は表現の違う本質的に同一の方式であることを確認されたい（その際、 h の選び方に有意な違いを感じる読者もいるかもしれないが、ランダムな $\mathbb{G}$ の元 h の分布と、ランダムな $\mathbb{Z}_p$ の元 x_1 を選び、 $h = g^{x_0} \cdot g^{x_1}$ とした h の分布は同一であり、攻撃者の視点からは全く区別がつかないことに注意されたい。）ここで、この方式と、前章の最後の部分にて述べたエルガマル暗号に基づく変形 Naor-Yung 方式との構成を比較してみることにする。すると、両者の違いは、 π の構成方法についてだけであり、それ以外は完全に一致していることに気が付く。つまり、Cramer-Shoup 方式とは、Naor-Yung 方式をエルガマル暗号に基づいて構成し、更に、NIZK 証明 π に相当する部分を極めて効率的に設計し直した方式と解釈できるのである。

この違いを更に深く掘り下げて考えてみよう。繰り返になるが、Naor-Yung 方式の核となるアイデアは、復号鍵を二つ準備し、そのどちらを用いても正しく復号ができるようにするものである。その際、どちらか一方の復号鍵しか知らなくとも、もう一方の復号鍵による復号結果との同一性を確信できるように NIZK 証明 π により、暗号文の構成要素のうち c_1, c_2 が正しい手順で構成されていることを保証するものとなっている。Cramer-Shoup 方式における暗号文の構成要素 π もまさしくこ

の機能を担っている。つまり、 c_1, c_2 が正しい手順によって作られているとは、要するに $\log_g c_1 = \log_h c_2$ となっていることを意味しており、Cramer-Shoup 方式の π はそれを保証するものである。

本章の最後として、 π がいかにして $\log_g c_1 = \log_h c_2$ を保証しているかの直感的な説明を与える。攻撃者 A が $\log_g c_1 \neq \log_h c_2$ となる質問 $C = (c_1, c_2, c_3, \pi)$ を発信しようとする状況を考えよう。ここで、 $r = \log_g c_1$, $r' = \log_h c_2$ とおくと、 C が正しい手順で作られたものとして（誤って）認識させるには、

$$\pi = g^{r w_0} h^{r' w_1} g^{r \alpha w_2} h^{r' \alpha w_3} = (z_0 z_1^\alpha)^r \cdot (h^{r' - r})^{w_1 + \alpha w_3}$$

を満足するような π を A は作成せねばならない（ただし、 $\alpha = \text{TCR}(c_1, c_2)$ ）。ところが、仮に攻撃者が無限の計算能力を持ってい（て離散対数問題が解け）たとしても、 $w_1 + \alpha w_3$ の値について一切情報を得ることができないため、無視できない確率で上記の等号を満足する π を導出することはできないことが分かる。 $(z_0 = g^{w_0} h^{w_1})$ の離散対数を求めることで、 w_1 が導出可能と思われる読者もあるかもしれないが、 $z_0 = g^{w_0} h^{w_1}$ を満足する (w_0, w_1) の組は無数に存在するため、特定は不可能である。 w_3 についても同様。）

8. Canetti-Halevi-Katz 方式

2000 年代初めまで、CCA 安全な実用的公開鍵暗号の構成方法は Cramer-Shoup 暗号とその改良方式（特に Kurosawa-Desmedt 暗号⁽⁷⁾が白眉と言えよう）しか知られていなかったが、2004 年に Canetti, Halevi, Katz⁽¹²⁾により ID ベース暗号⁽¹³⁾（⁽¹⁴⁾）を用いた構成方法が新たに示された。興味深いことにこの構成方法は従来とは一線を画するものであり、近年においてはむしろこちらの（背後にある）設計思想に基づいて、様々な新たな方式の提案が行われている。

本章では、Canetti-Halevi-Katz 方式の紹介と、その安全性の直感的な説明を行う。なお、ここまでの部分においてそうであったように、直感的な理解を優先し、厳密な証明の詳細には踏み込まないことにする。（興味ある読者は、文献 (12) や (15) など、しかるべき文献を当たられるのがよろしろう。）

Canetti-Halevi-Katz 方式の説明に先立ち、ID ベース暗号を簡単に紹介しよう。ID ベース暗号とは四つのアルゴリズムの組 (GEN, EXT, ENC, DEC) からなり、GEN(1^k) によりマスター鍵 mk と共通パラメータ pk が出力され (k はセキュリティパラメータ)、EXT($mk, "ID = \text{ファンダム太郎}, pk$) により “ファンダム太郎” に対する復号鍵 dk が出力され、ENC($M, "ID = \text{ファンダム太郎}, pk$) により、“ファンダム太郎” にあてられた平文 M に対する暗号文 C が作成され、DEC(dk, C, pk) により M が復元される。この際、安全性に関する重要な性質は次のとおりである：基本的には、通常の公開鍵暗号の（選択平文攻撃に対する）安全性と同一。ただし（結託者数が k に関して多項式オーダーである限り）ファンダム太郎氏を除く任意の利用者の結託攻撃に対しても安全でなくてはならない。言い換えれば、“ファンダム太郎” に対応した復号鍵を除く、任意の復号鍵集合を与えられたとしても、通常の公開鍵暗号と同じ安全性要件を満足

(注9)：共通鍵暗号として CCA 安全な DEM⁽¹¹⁾であることが求められる。

していなければならない．このような強力な道具立てである ID ベース暗号を一たび得ることができれば，次のように CCA 安全な (ID ベースではない通常の) 公開鍵暗号を構成することができる：

Canetti-Halevi-Katz 方式⁽¹²⁾

鍵生成: $\text{GEN}(1^k)$ を計算し，マスター鍵 mk と共通パラメータ pk を得る．これらをそれぞれ復号鍵及び公開鍵として出力する．

暗号化: 平文 M 及び公開鍵 pk に対し，まず (使い捨て) 電子署名の署名鍵と検証鍵のペア (sk, vk) を作成し， $\text{ENC}(M, "ID = vk", pk)$ により c_1 を計算し，更に， (c_1, vk) に対する電子署名 σ を署名鍵 sk を用いて導出し，暗号文として $C = (c_1, vk, \sigma)$ を出力する．

復号: 暗号文 $C = (c_1, vk, \sigma)$ 及び復号鍵 mk に対し，まず， σ の正当性を vk を用いて検証する．これが確認できたら， $\text{EXT}(mk, "ID = vk", pk)$ を計算し “ vk ” に対応した復号鍵 dk を求め， $\text{DEC}(dk, c_1, pk)$ により M を得る．

以下では，このような構成でなぜ CCA 安全性が達成できているのかについて直感的な説明を与えよう．そのための準備として (Naor-Yung 方式の方針とは大きく異なる) 次のような設計方針を考えてみることにする: Naor-Yung 方式のアイデアによれば，二つの復号鍵のどちらを用いても正しく復号可能となるように設計することで CCA 安全性を達成していたが，ここではそれに反して膨大な数の復号鍵のうち，その都度指定される一つを用いることで復号可能となるように設計を行う．この方式を (これまでの方式との比較を容易にするためだけに) 特にエルガマル暗号を用いて具体的に書き下すと次のようになる：

エルガマル暗号に基づく (安全でない) 原始的方式

鍵生成: $g \in \mathbb{G}$ と $x_1, \dots, x_n \in_R \mathbb{Z}_p$ を選び， $y_i = g^{x_i}$ ($i = 1, \dots, n$) を計算する．復号鍵 $dk = (x_1, \dots, x_n)$ 及び公開鍵 $pk = (g, y_1, \dots, y_n)$ を出力する．

暗号化: 平文 M 及び公開鍵 pk に対し，乱数 $r \in_R \mathbb{Z}_p$ を選び $c_1 = g^r$ を求める．また，ランダムに $j \in \{1, \dots, n\}$ を選び， $K = y_j^r$ を計算し，共通鍵 K を用いて M に共通鍵暗号化を施した c_2 を導出し，暗号文 $C = (c_1, c_2, j)$ を出力する．

復号: 暗号文 $C = (c_1, c_2, j)$ 及び復号鍵 dk に対し，まず， $K = c_1^{x_j}$ を計算し， K を共通鍵として用いて c_2 を復元し M を得る．

この方式は CCA 安全にはならない．しかし，この方針を用いることで CCA 安全性にかなり近づくことができ，そしてそれを実際に CCA 安全性まで到達させた一つの実現方法が Canetti-Halevi-Katz 方式であったと解釈することができる．そこでまずは，このような方針で，CCA 安全性が達成でき (そうに見え) る根拠を述べる．図 5 に安全性の証明の流れを示す (図

図 5 原始的方式の安全性証明の方針 (実際には証明は失敗する)

1 などと比較されたし)．上記の方式の安全性の証明を次のような方針で行うことを試みる (実際には後述のように失敗する)：与えられた CDH 問題に含まれる h^a を $(y_1, \dots, y_n)$ のいずれかとし (例えば $y_r = h^a$ としよう)，それ以外の $y_1, \dots, y_n$ の値は，実際の鍵生成と同様に $x_i \in \mathbb{Z}_p$ を選び， $y_i = h^{x_i}$ を計算する．本方式における暗号化は，送信者が自由に $j \in \{1, \dots, n\}$ を選び，その上で (h, y_j) を用いて単なるエルガマル暗号化をしているだけであり，そのように暗号化された暗号文は当然 x_j を用いて復号できる．したがって，この安全性証明の方針においては，攻撃者 A が質問 $C = (c_1, c_2, j)$ を発信してきても， $j \neq r$ であれば x_j を用いることで質問に対して問題なく返答することができる．これらの質問にこたえることができれば，これまでの他の手法と同様の要領で攻撃対象暗号文の一部として h^b を埋め込むことで， A に $K^* = h^{ab}$ を出力させることができることになる．つまり， $j = r$ となる質問さえ A から発信されることがなければ， A からの質問に完璧に返答しつつ， A に h^{ab} を出力させることが可能になるのである．言い換えれば，仮に $j = r$ となる確率が無視できるものであれば，これで上記の方式の CCA 安全性の証明はほとんど完了しているといえる．

では， $j = r$ となる確率はいかにほどであろうか．賢明な読者であればお気付きであろうが，上記の試行において $j = r$ が起こる確率は，少なくとも $1/n$ あり (全くでたために $j \in \{1, \dots, n\}$ を選んだとしても，それが r と一致している確率は $1/n$ となる)， n は高々セキュリティパラメータの多項式オーダーのサイズであるため， $1/n$ は無視できる値とはなり得ない．すなわち，この方針による上記方式の安全性証明は失敗する．

上記方式と安全性証明の性質についてまとめると，要するに (他の本質的な機能に変更を加えることなく) $j = r$ となる確率を無視できる値まで小さくする手法さえ見いだせれば CCA 安全性を証明できることになる．そのような手法を実現するための一つの方向性は，鍵ペアの総数 n がセキュリティパラメータの指数オーダーのサイズとなるようにすることである．さすれば， $1/n$ は当然無視できる値となる．しかしながら，それはすなわち鍵生成アルゴリズムを指数オーダーの回数動作させることを意味しており，実行不可能である．この問題を解決する一つの手法が ID ベース暗号の利用となる．これは次のように考え

ると自然と理解できる: ID ベース暗号では, マスター鍵 mk さえ持っていれば, 任意の文字列 (ID) に対して, それを公開鍵とするような復号鍵を作成することができる. したがって, mk を用いることで, 任意の $j(\in \{1, \dots, n\})$ を公開鍵とする復号鍵も作成できる. ここで興味深い点 (というより, ID ベース暗号の最も注目すべき性質) は, n はセキュリティパラメータの指数オーダーのサイズとなることも許容されることである. この性質を利用し, 受信者は鍵生成時にすべての鍵ペアを作成せずとも, ID ベース暗号のマスター鍵 mk さえ用意しておけば, 送信者が自由に選んだ $j \in \{1, \dots, n\}$ (ただし, n はセキュリティパラメータの指数オーダーの値) に対しても, その都度それに対応する復号鍵を作成することができる. つまりは, ID ベース暗号を用いることで仮想的にセキュリティパラメータの指数オーダーの数の鍵ペアを作成できていることになり, したがって, 上述の $1/n$ の値は無視できるものなる. そのような発想に基づき, 上記の原始的 방식을再構成すると次のようになる:

ID ベース暗号に基づく原始的方式

鍵生成: $\text{GEN}(1^k)$ を計算し, マスター鍵 mk と共通パラメータ pk を得る. これらをそれぞれ復号鍵及び公開鍵として出力する.

暗号化: 平文 M 及び公開鍵 pk に対し, まずランダムな $j \in \{1, \dots, n\}$ を選び (ただし, $n \geq 2^k$ とする), $\text{ENC}(M, "ID = j", pk)$ により c_1 を計算し, 暗号文として $C = (c_1, j)$ を出力する.

復号: 暗号文 $C = (c_1, j)$ 及び復号鍵 mk に対し, $\text{EXT}(mk, "ID = j", pk)$ を計算し “ j ” に対応した復号鍵 dk を求め, $\text{DEC}(dk, c_1, pk)$ により M を得る.

この方式は, いわゆる IND-CCA1 の安全性しか持たないが, j として単なる乱数ではなく使い捨て電子署名の検証鍵を選び, 更に, 同検証鍵に対応する署名鍵にて署名を施すことで CCA 安全性を達成することができる. その方式こそ Canetti-Halevi-Katz 方式にほかならない. つまり, Canetti-Halevi-Katz 方式とは, 上記の安全でない (が非常に CCA 安全に近い) 原始的方式において用いられる多数 (だが高々多項式オーダー数) の鍵ペアを, ID ベース暗号を用いて仮想的に指数オーダー数あるかのような状態を作り, CCA 安全性まで高めた方式なのである.

なお, 現在, 暗号文長と計算コストの両方に関して最も効率性が高い方式の一つである Boyen-Mei-Waters 方式⁽¹⁶⁾は, Canetti-Halevi-Katz 方式における具体的な ID ベース暗号方式として Boneh-Boyen 方式⁽¹⁷⁾を適用し, 更にその代数的な性質も活用して効率性を高めたものである.

9. Bounded CCA 安全な方式

前章では, Canetti-Halevi-Katz 方式を深く理解するため, その本質的なアイデアを抽出した (安全ではない) 原始的方式を導入し, それを介して説明を行った. それによれば, n 個の公開鍵

を準備して, その中から適当に一つを選んで暗号化を行うとき, もしも $1/n$ が無視できる値であれば CCA 安全を (ほぼ) 証明できるというものであった. また, Canetti-Halevi-Katz 方式とは, ID ベース暗号を用いることで仮想的に指数オーダーの鍵ペアがあるかのような状況を作り出し, それにより $1/n$ を無視できる値となるようにする手法であると述べた.

それに対して, ID ベース暗号を用いることなく, $1/n$ を無視できるようにすることができるかが疑問として自然に生じてくる. これは, 果たして可能であろうか. 本章と次章では, その疑問に対して (肯定的に) こたえることを主な目的としている.

本章では, 特に, 選択平文攻撃に対して安全 (CPA 安全) な公開鍵暗号のみを用いて, どこまで上記の原始的方式の安全性を高められるかについて議論していこう. ただし, 結論をいえば, 文献 (18) で示されているように, 一般的には, CPA 安全な公開鍵暗号のみを用いて CCA 安全な公開鍵暗号を構成することは絶望的に難しい. しかし, それにもかかわらず CCA 安全性に関するある要件を若干緩めることで, 状況が一変してくるのである. 具体的には, 攻撃者 A の質問回数の上限があらかじめ分かっているならば, そのような条件下で CCA 安全 (以降では, 通常の CCA 安全性と区別すべく, “Bounded CCA (BCCA) 安全” と呼ぼう) な公開鍵暗号を, CPA 安全な公開鍵暗号のみから一般的に構成可能であり, また, CPA 安全な方式として具体的にエルガマル暗号を用いて (て, なおかつ, その代数的性質も活用す) ると, 従来のエルガマル暗号と暗号文長が等しい BCCA 安全な公開鍵暗号が構成可能であることが, Cramer, 花岡, Hofheinz, 今井, Kiltz, Pass, shelat, Vaikuntanathan⁽¹⁹⁾ によって示されている.

文献 (19) では, 多項式オーダーの数の公開鍵ペアを用いて, 仮想的に指数オーダーの数の鍵ペアが存在しているかのように振る舞うトリックとして, 組合せ論を利用している. 特に, 次に述べる Cover Free 族が重要な役割を担っている:

定義 4 (Cover Free 族). $\mathcal{L}$ を $|\mathcal{L}| = u$ なる有限集合とし, $\mathcal{F} = \{\mathcal{F}_1, \dots, \mathcal{F}_n\}$ を $\mathcal{L}$ の部分集合の族とする. このとき, 任意の $i \in \{1, \dots, n\}$ と $\mathcal{S}_i \subseteq \{1, \dots, n\} \setminus \{i\}$ (ただし, $|\mathcal{S}_i| \leq q$) について, $\mathcal{F}_i \not\subseteq \bigcup_{j \in \mathcal{S}_i} \mathcal{F}_j$ となるとき, $(\mathcal{L}, \mathcal{F})$ を (u, n, q) -Cover Free 族と呼ぶ.

特筆すべき事実として, u と n がそれぞれ q の多項式オーダーと指数オーダーになる Cover Free 族の構成方法が知られている⁽²⁰⁾. 以下では, そのような性質を持つ Cover Free 族に限定して議論を行う. Cover Free 族とエルガマル暗号 (の代数的性質) を用いて, 次のように BCCA 安全な方式を構成できる:

エルガマル暗号に基づく BCCA 安全な方式⁽¹⁹⁾

鍵生成: 質問回数の上限 q に対し, (u, n, q) -Cover Free 族 $(\mathcal{L}, \mathcal{F})$ (ただし, $\mathcal{L} = \{1, \dots, u\}$) を作成し, また, $g \in \mathbb{G}$ を選ぶ. 次に, $x_i \leftarrow \mathbb{Z}_p$ を選び, $y_i = g^{x_i}$ を計算する ($1 \leq i \leq u$). 更に, はん用一方向性ハッシュ関数 $\text{TCR}: \mathbb{G} \rightarrow \mathcal{F}$ を適当に選択する. 復号鍵 $dk = (x_1, \dots, x_u)$ 及び公開鍵 $pk = (g, y_1, \dots, y_u, \text{TCR})$ を出力する.

暗号化: 平文 M 及び公開鍵 pk に対し, 乱数 $r \in_R \mathbb{Z}_p$ を

選び $c_1 = g^r$ を求める．また， $\text{TCR}(c_1) = \mathcal{F}_j$ を選び， $K = \prod_{i \in \mathcal{F}_j} y_i^r$ を計算し，共通鍵 K を用いて M に共通鍵暗号化^(注10)を施した c_2 を導出し，暗号文 $C = (c_1, c_2)$ を出力する．

復号：暗号文 $C = (c_1, c_2)$ 及び復号鍵 dk に対し，まず， $\text{TCR}(c_1) = \mathcal{F}_j$ を求め， $K = \prod_{i \in \mathcal{F}_j} c_1^{x_i}$ を計算し， K を共通鍵として用いて c_2 を復元し M を得る．

上記の方式においては，特にその暗号文サイズに着目されない．この方式は，攻撃者による質問回数が q 回を上回らない限り (B)CCA 安全な方式であり，つまり，CPA 安全性よりもはるかに高い安全性を持っているにもかかわらず，暗号文サイズがエルガマル暗号のものと等しくなっている（なお，数学的仮定に関して一切強まっていない）

以下では，上記の方式の安全性の直感的説明を行う．前章で述べたとおり，前章の原始的方式の CCA 安全性の証明を試みる上での（ほぼ唯一の）問題点は，公開鍵ペアの総数 n がセキュリティパラメータの多項式オーダーであることであった．上記の方式では，ID ベース暗号を用いずに，次の方針にて仮想的に指数オーダーの公開鍵ペアを作り出そうとしている：仮に $2k$ 個の公開鍵ペアがあるものとする．そのうち k 個の公開鍵をランダムに選び，平文 M を多重暗号化するものとする．この際，暗号化に用いた公開鍵に対応するすべての復号鍵を用いない限り M を復元できないように多重暗号化を施す（そのような多重暗号化は容易である）．すると，そのような k 個の公開鍵の選び方は 2^k とおり以上存在し，つまり，実際の公開鍵ペア数の指数オーダーの暗号化が行えていることになる．言い方を換えれば，これはセキュリティパラメータの多項式オーダーの数の公開鍵ペアしかなくとも，多重暗号化を行うことで，仮想的に指数オーダーの数の鍵ペアがあるかのように振る舞えることを意味している．上記の方式はまさにこの方針にて設計がなされたものである．特に， u 個の公開鍵ペアのみを用いて， n とおりの多重暗号化を行っている点に注意されたい．なお，Cover Free 族の性質は， q 回異なる多重暗号化を行ったとしても， $q+1$ 回目の多重暗号化の安全性に影響を及ぼさないことを保証するために用いられている．ただし，あくまでその本質的には多項式オーダーの個数の公開鍵ペアしかなくとも，その部分集合の取り方は指数オーダーとれるという発想に変わりはない．

10. 花岡-黒澤方式

前々章では，Canetti-Halevi-Katz 方式の構成の根底にある考え方をとらえた（安全でない）原始的方式を紹介し，Canetti-Halevi-Katz 方式とは ID ベース暗号を用いることでその原始的方式に残された問題を克服したものであるとの解釈を示した．前章では，CCA 安全性に関する要件を若干緩めることで，ID ベース暗号のような強力な構成要素を用いずとも，CPA 安全な公開鍵暗号のみを用いて，やはり同様に問題を克服できること

を示した．本章では，それに対し，ID ベース暗号よりも弱くなくかつ自然な暗号プリミティブのみを用いて，CCA 安全性の要件を緩めることなく，原始的方式の問題を克服する花岡-黒澤方式⁽¹⁵⁾を紹介する．

花岡-黒澤方式の根底となるアイデアは次のとおりである：前章及び前々章によれば，要するに，多項式オーダーサイズの資源のみを用いて指数オーダーの暗号化方法を実現する手法があれば，上述の原始的方式の安全性を CCA 安全まで高められる．つまり，非常に多数の鍵の管理を行うことが可能な暗号プリミティブであれば，ID ベース暗号に限らず，この問題を解決するのに有用となるものと予想できる．そのような暗号プリミティブとして，真っ先に放送暗号が思い出される．放送暗号とは，多数の受信者のうち，その任意の部分集合にのみあてた暗号文を作成可能な暗号方式である．ここで，利用者の部分集合の選択の仕方は利用者総数の指数オーダーとなるため，これをうまく利用してやることで原始的方式における問題の解決が可能となるものと期待できるのである．このアイデアを厳密に議論していくと検証可能な放送暗号から一般的に CCA 安全な公開鍵暗号を構成できることを示すことができる．なお，正当な受信者が単に復号を行えるだけでなく，他の正当な受信者も同じ復号結果を得ていることが確信できるような放送暗号を，検証可能であると呼ぶことにする．

検証可能な放送暗号は，ID ベース暗号よりも有意に弱い暗号プリミティブであり，例えば拡張落戸付置換や DDH 仮定のような弱い仮定からも構成できることが知られている．一方，ID ベース暗号をこれらの仮定から構成する方法はこれまでに知られていない．また，花岡，黒澤は実際に Naor-Pinkas 放送暗号⁽²¹⁾を検証可能となるように変形することで，CDH 仮定に基づく CCA 安全な実用的公開鍵暗号の設計も行っている．以下では，特にこの方式を例について説明を行う．

簡単のため受信を許されない利用者が一人のみの場合を想定すると，Naor-Pinkas 放送暗号は次のように構成される：有限体 $\mathbb{Z}_p$ 上の一次式 $f(x) = a_0 + a_1x$ に対し， $g \in \mathbb{G}$ を選び $y_0 = g^{a_0}$ ， $y_1 = g^{a_1}$ を計算する．また， (g, y_0, y_1) を公開鍵とする．各利用者 i に対しては，復号鍵として $f(i)$ を与える．利用者 j のみを排除して，それ以外の利用者全員にあてた暗号文を送る際は，乱数 $r \in \mathbb{Z}_p$ を選択し， $K = y_0^r$ を計算し， K を用いて平文を暗号化し，この暗号化された平文とともに $(g^r, (y_0 y_1^j)^r)$ を同報送信する．このとき， $(y_0 y_1^j)^r = g^{r \cdot f(j)}$ であるので， j 以外の利用者 i はまず $(g^r)^{f(i)}$ を計算し，更にラグランジュ補間により $(g^r)^{f(0)} = y_0^r = K$ を導出する．最後にこれを用いて，平文を復元する．

Naor-Pinkas 放送暗号とハードコアビット⁽²²⁾を用いることで，CDH 仮定に基づく放送暗号は容易に構成可能であるが，残念なことに，そのままでは検証可能とはならない．したがって，なんらかの手法により Naor-Pinkas 放送暗号を検証可能となるように変形することが残された大きな技術的課題となる．花岡，黒澤はこの問題を次の要領にて解決している：（同様に受信を許されない利用者が一人のみの場合を想定すると，）有限体 $\mathbb{Z}_p$ 上の三次式 $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ に対し， $g \in \mathbb{G}$ を選び

(注10)：共通鍵暗号として CCA 安全な DEM⁽¹¹⁾であることが求められる．

$y_\ell = g^{a_\ell} (0 \leq \ell \leq 3)$ を計算する。また、 $(g, y_0, \dots, y_3)$ を公開鍵とする。各利用者 $i (= (i_0, i_1))$ に対しては (ここでは利用者の識別子が $\mathbb{Z}_p$ 上の固有の二つの値で表現されているものとする)、乱数 $rnd \in \mathbb{Z}_p$ を選び、復号鍵として $(f(i_0), f(i_1), f(rnd), rnd)$ を与える。利用者 $j (= (j_0, j_1))$ のみを排除して、それ以外の利用者全員にあてた暗号文を送る際は、乱数 $r \in \mathbb{Z}_p$ を選択し、 $K = y_0^r$ を計算し、 K を用いて平文を暗号化し、この暗号化された平文とともに $(g^r, (\prod_{0 \leq \ell \leq 3} y_\ell^{j_0})^r, (\prod_{0 \leq \ell \leq 3} y_\ell^{j_1})^r) (= (g^r, g^{r \cdot f(j_0)}, g^{r \cdot f(j_1)}))$ を同報送信する。このとき、 $f(x)$ は三次式であるので、 $(j_0, f(j_0)), (j_1, f(j_1))$ 以外の $f(x)$ 上の任意の二つの点を知っていれば、従来の Naor-Pinkas 放送暗号の要領で $K = y_0^r$ を復元することができる。それに対し、 j 以外の利用者 i は $(i_0, f(i_0)), (i_1, f(i_1)), (rnd, f(rnd))$ の三点を知っているため、3通りの方法でラグランジュ補間を行うことができる (三点のうち二点を選択する方法が3通りなので)。もしも、これら3通りの計算結果が異なっていれば暗号文が正しい手順で作成されていないことが検知でき、一方、暗号文が正しい手順で作成されていれば j 以外の利用者は必ず同一の $K = y_0^r$ を復元できる。したがって、検証可能な放送暗号となっていることが分かる。この放送暗号を用いて次のように CCA 安全な公開鍵暗号が構成できる:

変形 Naor-Pinkas 放送暗号に基づく花岡-黒澤方式⁽¹⁵⁾

鍵生成: $g \in \mathbb{G}$ と $a_0, \dots, a_{k+2} \in_R \mathbb{Z}_p$ を選び (k はセキュリティパラメータ)、 $y_i = g^{a_i} (i = 0, \dots, k+2)$ を計算する。また、はん用一方向性ハッシュ関数 $\text{TCR}_1, \text{TCR}_2$ を適当に選ぶ。その際、 TCR_1 と TCR_2 の値域は重ならないものとする。更に、 $\mathbb{G}$ におけるディフィ・ヘルマン鍵のハードコアビットを出力する関数を H とする (例えば、文献 (22) ~ (24) など)。復号鍵 $dk = (a_0, \dots, a_{k+2})$ 及び公開鍵 $pk = (g, y_1, \dots, y_{k+2}, \text{TCR}_1, \text{TCR}_2)$ を出力する。

暗号化: 平文 M 及び公開鍵 pk に対し、乱数 $r \in_R \mathbb{Z}_p$ を選び $c_1 = g^r$ を求める。また、 $c_2 = \prod_{0 \leq \ell \leq k+2} y_\ell^{t_1^\ell}$ 、 $c_3 = \prod_{0 \leq \ell \leq k+2} y_\ell^{t_2^\ell}$ を計算し (ただし、 $t_1 = \text{TCR}_1(c_1)$ 、 $t_2 = \text{TCR}_2(c_1)$)、更に $K = (H(y_0^r) || \dots || H(y_{k-1}^r))$ を求め、共通鍵 K を用いて M に共通鍵暗号化^(注11)を施した c_4 を導出し、暗号文 $C = (c_1, c_2, c_3, c_4)$ を出力する。

復号: 暗号文 $C = (c_1, c_2, c_3, c_4)$ 及び復号鍵 dk に対し、まず、 $c_2 = c_1^{f(\text{TCR}_1(c_1))}$ 及び $c_3 = c_1^{f(\text{TCR}_2(c_1))}$ が成立しているかを検証し、これが確認できれば $K = (H(c_1^{a_0}) || \dots || H(c_1^{a_{k-1}}))$ を計算し、 K を共通鍵として用いて c_4 を復元し M を得る。

CDH 問題の困難性の仮定の下、上記の方式は CCA 安全性を証明可能である。また、この方式の暗号文長は Cramer-Shoup 方式のものと同等であることに注意されたい。つまり、Cramer-Shoup 方式の暗号文長を増加させることなく、安全性だけを顕著に高めていることが分かる (Cramer-Shoup 方式は DDH 仮定の下でのみ安全性が証明可能)。

(注11): 共通鍵暗号として CCA 安全な DEM⁽¹¹⁾であることが求められる。

花岡-黒澤方式とは、要するに、前々章の (安全でない) 原始的方式を CCA 安全なまでに高めるには、Canetti-Halevi-Katz 方式のように ID ベース暗号を用いずとも、検証可能な放送暗号を用いればよいことを示すものであり、その具体例の一つが上記の (検証可能となるように変形を施された) Naor-Pinkas 放送暗号に基づく方式である。興味深いことに、既存の CCA 安全な方式の多くも、異なる放送暗号に基づく花岡-黒澤方式の特殊な例とみなすことができる。例えば、ID ベース暗号は受信者が一人に限定された放送暗号とみなすことができるが、そのようにみなして ID ベース暗号を花岡-黒澤方式に適用すると、Canetti-Halevi-Katz 方式が得られる。また、検証可能な放送暗号を構成する最も単純な方法は、単に各利用者ごとに個別の公開鍵ペアを使用し、更に、復号結果の同一性を保証する NIZK 証明を添付する手法であるが、この放送暗号を花岡-黒澤方式に適用すると、Dolev-Dwork-Naor 方式⁽²⁾が得られる。つまり、CCA 安全を達成するための最初の手法と最新の手法の両方が特殊な例として同時に包含されていることが分かる。他にも様々な既存方式が特殊な例として包含されており、また、上記の CDH 仮定に基づく方式を含む様々な新たな方式も設計可能である (例えば、Boneh-Gentry-Waters 放送暗号⁽²⁵⁾に花岡-黒澤方式を適用すると、また別の新たな CCA 安全な実用的公開鍵暗号を得ることができる⁽¹⁵⁾)。

11. おわりに

本稿では、CCA 安全な公開鍵暗号を設計するための方法論をできるだけ系統立てて説明を行った。また、特に、Canetti-Halevi-Katz 方式の本質的な性質を説明付けるために (安全でない) 原始的方式を示し、この原始的方式を CCA 安全なまでに安全性を高めるためには、多項式オーダーのサイズの資源のみを用いて指数オーダーどおりの暗号化を行うことが可能であるような状況を作り出す必要があることを議論した。また、そのような状況を作り出す一つの方法が ID ベース暗号を用いることであり、それが Canetti-Halevi-Katz 方式にほかならないことを示した。その後、ID ベース暗号を用いずに同様の状況を作り出す方法を議論し、最終的に、検証可能な放送暗号を利用することでそれが実際に可能であることを示した花岡、黒澤の結果を紹介した。Canetti-Halevi-Katz 方式を含め多くの既存方式は花岡-黒澤方式の特殊な例になっており、このことから、CCA 安全な公開鍵暗号を設計する際は、放送暗号を出発点とするのが極めて見通しが良いことが分かる。

謝辞 本稿の執筆にあたり有益な議論や御指摘を頂きました、太田 和夫先生、國廣 昇先生、大久保 美也子氏、縫田 光司氏、崔 洋氏、Bagus Santoso 氏、松田 隆宏氏に深く感謝致します。

文献

- (1) D. Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1," Proc. of CRYPTO 1998, LNCS vol.1463, pp.1-12,

- 1998.
- (2) D. Dolev, C. Dwork and M. Naor, "Non-malleable cryptography (Extended Abstract)," Proc. of STOC 1991, pp.542-552, 1991.
 - (3) C. Rackoff and D.R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," Proc. of CRYPTO 1991, LNCS vol.576, pp.433-444, 1991.
 - (4) M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, "Relations among notions of security for public-key encryption schemes," Proc. of CRYPTO 1998, LNCS vol.1462, pp.26-45, 1998.
 - (5) R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," Proc. of FOCS 2001, pp.136-145, 2001.
 - (6) R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," Proc. of CRYPTO 1998, LNCS vol.1462, pp.13-25, 1998.
 - (7) K. Kurosawa and Y. Desmedt, "A new paradigm of hybrid encryption scheme," Proc. of CRYPTO 2004, LNCS vol.3152, pp.426-442, 2004.
 - (8) T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," Proc. of CRYPTO 1984, LNCS vol.218, pp.10-18, 1985.
 - (9) M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," Proc. of STOC 1990, pp.427-437, 1990.
 - (10) A. Sahai, "Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security," Proc. of FOCS 1999, pp.543-553, 1999.
 - (11) V. Shoup, "Using hash functions as a hedge against chosen ciphertext attack," Proc. of EUROCRYPT 2000, LNCS vol.1807, pp.275-288, 2000.
 - (12) R. Canetti, S. Halevi and J. Katz, "Chosen-ciphertext security from identity-based encryption," Proc. of EUROCRYPT 2004, LNCS vol.3027, pp.207-222, 2004.
 - (13) D. Boneh and M.K. Franklin, "Identity-based encryption from the weil pairing," Proc. of CRYPTO 2001, LNCS vol.2139, pp.213-229, 2001.
 - (14) A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. of CRYPTO 1984, LNCS vol.196, pp.47-53, 1985.
 - (15) G. Hanaoka and K. Kurosawa, "Efficient chosen ciphertext secure public key encryption under the computational diffie-Hellman assumption," Proc. of ASIACRYPT 2008, LNCS vol.5350, pp.308-325, 2008.
 - (16) X. Boyen, Q. Mei and B. Waters, "Direct chosen ciphertext security from identity-based techniques," Proc. ACM CCS 2005, pp.320-329, 2005.
 - (17) D. Boneh, X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," Proc. of EUROCRYPT 2004, LNCS vol.3027, pp.223-238, 2004.
 - (18) Y. Gertner, T. Malkin and S. Myers, "Towards a separation of semantic and CCA security for public key encryption," Proc. of TCC 2007, LNCS vol.4392, pp.434-455, 2007.
 - (19) R. Cramer, G. Hanaoka, D. Hofheinz, H. Imai, E. Kiltz, R. Pass, A. Shelat and V. Vaikuntanathan, "Bounded CCA2-secure encryption," Proc. of ASIACRYPT 2007, LNCS vol.4833, pp.502-518, 2007.
 - (20) P. Erdős, P. Frankl and Z. Füredi, "Families of finite sets in which no sets is covered by the union of r others," Isr. J. of Math., vol.51, pp.79-89, 1985.
 - (21) M. Naor and B. Pinkas, "Efficient trace and revoke schemes," Proc. of Financial Cryptography 2000, LNCS vol.1962, pp.1-20, 2000.
 - (22) O. Goldreich and L.A. Levin, "A hard-core predicate for all one-way functions," Proc. of STOC 1989, pp.25-32, 1989.
 - (23) D. Boneh and I. Shparlinski, "On the unpredictabil-

ity of bits of the elliptic curve diffie-hellman scheme," Proc. of CRYPTO 2001, LNCS vol.2139, pp.201-212, 2001.

- (24) D. Boneh and R. Venkatesan, "Hardness of computing the most significant bits of secret keys in diffie-hellman and related schemes," Proc. of CRYPTO 1996, LNCS vol.1109, pp.129-142, 1996.
- (25) D. Boneh, C. Gentry and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," Proc. of CRYPTO 2005, LNCS vol.3621, pp.258-275, 2005.

(平成 21 年 4 月 16 日受付 平成 21 年 5 月 17 日最終受付)

花岡 悟一郎

1997 東大・工・電子卒 . 2002 同大学院工学系研究科博士課程了 . 2002-2005 日本学術振興会特別研究員 (PD) . 2005-現在 産業技術総合研究所研究員 . 暗号理論, 情報セキュリティの研究に従事 . 博士 (工学) . The Wilkes Award (2006) , 平 19 年度本会論文賞, SCIS 論文賞 (2005) , 電気通信普及財団賞 (2004) , SCIS20 周年記念賞 (2004) , SITA 奨励賞 (2000) 各賞受賞 .