KDM 安全性—秘密鍵に依存した文書を暗号化したときの安全性について

Survey of Key Dependent Message (KDM) Security

寺西 勇 Isamu TERANISHI

アブストラクト KDM 安全性は暗号方式の安全性概念であり、秘密鍵に依存した文書を暗号化してもその文書の秘密が担保されることを指す。暗号方式の通常的应用では文書が秘密鍵に依存することがないため、これまでの暗号研究では KDM 安全性は非標準的な安全性概念であるとみなされてきたが、近年の研究により、この安全性概念が理論上も応用上も重要な概念であることが明らかにされた。本稿では、KDM 安全性の概念とその重要性を振り返り、近年の KDM 安全性に関する研究成果を紹介する。

キーワード 暗号方式, KDM 安全性

Abstract Key Dependent Message (KDM) security for an encryption scheme is based on the notion that ciphertexts can ensure the secrecy of the corresponding plaintexts even if the plaintexts depend on a secret key. Although KDM security was previously considered a nonstandard security concept, recent research has clarified its significance in both theoretical and practical areas. In this survey, we review the definition and applications of KDM security. We then review recent for KDM security.

Key words Encryption Scheme, KDM Security

1. はじめに

1.1 背景

暗号方式とその安全性: データを秘匿するための技術として暗号方式がある。古くは軍隊をはじめとした一部の組織でのみ用いられてきた技術だが、コンピュータとインターネットの普及に伴い、今では世界中で用いられるようになっている。

暗号方式を用いるには、そもそも何をもって暗号方式を「安全」とみなすかを定式化する必要があるが、安全性の概念を定式化するまでの道のりは決して平たんなものではなく、ある意味では現在も研究の途上にある。

現在、暗号方式の安全性として標準的とみなされている概念があり、識別不能性⁽¹⁾⁽²⁾と呼ばれている。これは直観的には「 M の暗号文と M' の暗号文を識別することは不可能である」ことを意味する概念である。公開鍵暗号方式・共通鍵暗号方式を問わず、暗号方式が単に安全であるといえはこの意味での安全性を指す。

安全性研究の近年の動向: しかし近年、暗号方式に要求する安

全性レベルや応用によっては識別不能性では不十分であると指摘されている。例えばコンピュータが放つ電磁波やその消費電力の計測により秘密鍵の部分情報が漏えいしてしまう状況を考慮していない。また暗号文送信後に誰と結託するのかを決められる状況も考慮していない。

現在、こうした状況を考慮した安全性概念やそれらを満たす方式の研究が活発に行われている。すなわち安全性概念の研究は、「標準的な安全性概念を確立する」第 1 のフェーズから「標準的な概念の存在を前提とした上でそれより更に強い安全性概念を研究する」第 2 のフェーズへとシフトしたといつてよい。

1.2 KDM 安全性

本稿の主題である KDM 安全性も、こうした第 2 フェーズの研究の一環として生まれた概念である。この概念は暗号化するメッセージが秘密鍵に依存している (Key Dependent Message) 状況—標準的な安全性概念 (識別不能性) では想定されていなかった状況—をも範ちゅうに含めており、それゆえ識別不能性よりも強い概念である。この安全性概念は理論上も応用上も重要な役割を果たすことが分かっており、それゆえ近年活発に研究されている。

本稿の目的は、KDM 安全性の既存研究を振り返り、KDM 安全性がなぜ重要であるか、KDM 安全な方式を作るのはなぜ困難であるのか、その困難をどうやって乗り越えるのかを解説することである。本稿の概要は以下のとおりである。

2. 歴史と現状: 本章ではまず KDM 安全性で考慮している状

寺西 勇 正員 日本電気株式会社情報メディア・プロセッシング研究所
E-mail teranisi@ah.jp.nec.com
Isamu TERANISHI, Member (Information and Media Processing Laboratories, NEC Corporation, Kawasaki-shi, 211-8666 Japan).
電子情報通信学会 基礎・境界サイエティ
Fundamentals Review Vol.6 No.1 pp.26–36 2012 年 7 月
©電子情報通信学会 2012

況—すなわち平文が秘密鍵に依存する状況—で暗号方式を用いるのは、単なる「誤用」であると長い間みなされてきたことを見る。次に 2000 年代初頭、KDM 安全性の応用例が見つかったことにより、この概念が注目を集めたことを見る。そして最後に、KDM 安全な方式⁽³⁾⁻⁽⁵⁾が構築され、KDM 安全性の研究は一つの到達点を迎えたことと現在はその到達点を基にして研究がなされていることを見る。

3. 応用: 通信の秘密を保つという本来の用途で暗号方式を利用している限り、秘密鍵依存な平文を暗号化しなければならない状況は起こり得ない。本章では、暗号方式を部品として別の暗号プロトコルを作成した場合には KDM 安全性が必須になる場合もあることを見る。更に応用例として鍵貸出対策方式⁽⁶⁾、Dolev-Yao モデル⁽⁷⁾⁻⁽⁹⁾、完全準同形暗号方式^{(10) (11)}、Agility⁽¹²⁾を紹介する。

以上の 2 章は公開鍵暗号方式の研究に詳しくない読者を想定し、可能な限り数式を使わずに記述した。残りの章は公開鍵暗号方式の基本的な知識を前提とする。

4. 厳密な定義: 本章では KDM 安全性の厳密な定義を紹介する。

5. CPA 攻撃に対して KDM 安全な方式: 本章ではまずランダムオラクル仮定の下では CPA 攻撃に対して KDM 安全な方式を簡単に作れることを見る。ここでランダムオラクル仮定とは、ある種の関数の出力が (本当はランダムではないのに) ランダムであるとみなせるという非現実的な仮定のことである。次にこの仮定なしで CPA 攻撃に対する KDM 安全な方式を構築する際、以下の障害があることを見る: 通常の安全性証明ではベースとなる問題を解く攻撃者で秘密鍵を知らないものを構成するが、KDM 安全性の場合には鍵依存暗号文を計算するためにそうした攻撃者が秘密鍵を知っていなければならない、通常の安全性証明テクニックが使えない。

本章ではその後、秘密鍵の代わりに暗号文作成時の乱数の秘密に頼ることで上述の障害を取り除くことができることを見る。そして最後に既存の方式の多くがこのアイデアに基づいて KDM 安全性を示していることを見る。

6. CCA 攻撃に対して KDM 安全な方式: 本章では Naor-Yung 法⁽¹³⁾に基づけば CCA 攻撃に対する KDM 安全性が達成できることを見る。

2. 歴史と現状

2.1 揺らんなり

最初の言及: 暗号化する平文が秘密鍵に依存している状況—KDM 安全性が考慮している状況—が初めて言及されたのは、識別不能性の概念が提案されたとき⁽²⁾である。しかし当時はこうした状況下で暗号方式を用いる用途が見当たらなかったため、このことは特に重要視されなかった。秘密鍵に依存した平文を暗号化するのには暗号方式の単なる「誤用」であるとみなされ、長

い間研究者の注目を集めてこなかった。

応用例の発見: KDM 安全性が初めて研究の表舞台に上ったのは 2000 年代初頭のことである。それは論文(2)で秘密鍵依存の平文の暗号化が初めて言及されてから既に四半世紀が過ぎた後のことであった。注目の契機となったのは、KDM 安全な方式の応用と KDM 安全性の理論的な意義とが同時期に見つかったことである。

応用の方は、Camenisch と Lysyanskaya⁽⁶⁾により発見されたもので、彼らは秘密鍵の暗号化が鍵貸出問題対策に適用できることを示した。理論的な意義は Abadi と Rogaway^{(8) (9)}により発見されたもので、彼らは秘密鍵の暗号化が Dolev-Yao モデル⁽⁷⁾と通常の安全性概念を「和解」させる際に用いることができることを示した。(これらの詳細は 3. で述べる。)

KDM 安全性の定式化: これらの事実は、秘密鍵を暗号化した状況下での安全性の定式化を促した。Black, Rogaway, Shrimpton の 3 人はこのようなモチベーションの下、そうした状況下での安全性—すなわち KDM 安全性—を定式化し、この安全性を満たす方式を提案した⁽¹⁴⁾。なお Camenisch と Lysyanskaya⁽⁶⁾は前述した鍵貸出問題に対処するために類似した概念 (循環暗号化) を論文(14)と同時期に独立に発表しているため、秘密鍵依存の文書を暗号化するという研究の創始は双方に帰される。

この時期の研究の限界と未解決問題: こうして 21 世紀の到来とともに秘密鍵依存の文書を暗号化した場合の安全性に関する研究が始まったが、この時期の論文(6) (14)では「ランダムオラクル仮定」に頼って方式の KDM 安全性を示しているという限界があった。

ランダムオラクル仮定とは、ある種の関数の出力が (本当はランダムではないのに) ランダムに見えるという非現実的な仮定である。こうした仮定は方式の安全性を示すには都合の良い仮定であるものの、本来ランダムではないはずの出力をランダムであると仮定するという非現実的な仮定であるため、この仮定の下安全性が示されたとしても本当にその方式が安全であるかどうかは分からないという問題をはらむ。

実際、この仮定の下では、安全性が示されているのにもかかわらず、本当は安全ではない方式の実例も作られており⁽¹⁵⁾、近年はこの仮定に頼って安全性を示すことは敬遠される傾向にある。ランダムオラクル仮定に頼らず KDM 安全性を示せる方式を作るという課題はしばらくの間未解決のまま残されることになった。

その後秘密鍵依存の平文を暗号化することが実用上注目を集めた例があったため、先に進む前にこの例を紹介する。

ディスク暗号化: 一つ目の例は Windows VistaTM のディスク暗号化ソフト BitLocker が秘密鍵自身を暗号化してしまうという「誤用」を実際に犯したときである⁽³⁾。ディスク暗号化ソフトはこの種の「誤用」を犯しがちで、秘密鍵のバックアップが保存されているディスクを暗号化してしまうと、秘密鍵自身をも暗号化してしまうことになってしまう⁽³⁾。

セクターレベル暗号化: もう一つの例は IEEE P1619 の委員たちが「セクターレベル暗号化」というものの標準化を行ったと

きである．委員たちは論文(16)で提案された方式を標準として用いることを検討していたが，この方式は秘密鍵自身を暗号化した状況下には攻撃が可能なが知られていたため，こうした状況下での攻撃が実用上意味のあるものであるかどうか議論になったのである．その後委員たちは前述した BitLocker における実例を発見したため，別の方式⁽¹⁷⁾を標準として使うことにした^{(18)~(20)}．

2.2 成熟期～現在

未解決問題の解決: KDM 安全性の研究が本格的に脚光を浴びるのは定式化から 6 年後のことで，Boneh, Halevi, Hamburg, Ostrovsky の 4 人が，前述の未解決問題に対して大きな進展のある成果⁽³⁾を出したことによる．(それ以前に論文(21)が部分解を出している．)

彼らは「暗号化されるメッセージが秘密鍵の各ビットのアフィン結合で書ける」という仮定の下，前述の未解決問題を解決した．ここでデータ $x_1, \dots, x_n$ のアフィン結合とは，何らかの定数 $a_1, \dots, a_n, b$ と事前に定められたモジュラス N を用いて

$$a_1 x_1 + \dots + a_n x_n + b \bmod N$$

の形に書けるデータことである．

その後の研究はこの「暗号化される…」という仮定をなくす方へと進展し⁽²²⁾，最終的に「 f の回路サイズが事前に fix された値を越えない」という仮定が満たされさえすれば秘密鍵依存の任意のメッセージ $f(sk_1, \dots, sk_n)$ を暗号化しても KDM 安全性が示せる方式が Barak, Haitner, Hofheinz, Ishai の 4 人により作られた⁽⁵⁾．

この回路サイズに関する条件を外した場合には KDM 安全な方式を作れないことが (Blackbox-reduction の下) 示されている⁽²³⁾ため，前述の未解決問題は完全解決されたことになる．こうして KDM 安全な暗号方式の研究は一つの到達点を迎えた．

その後も KDM 安全性を示すことができる関数のクラスを広げる一般的方法⁽²⁴⁾や効率を落とさずにかなり多くの関数 f に対して KDM 安全性を達成する方式⁽²⁵⁾などが研究され，現在に至っている．

2.3 その他の既存の成果

最後に以上の歴史では説明し切れなかった成果を載せる．ただし 3. に載せたものはここでは省略する．

- 擬似ランダム関数に対する KDM 安全性の考察⁽¹⁸⁾
- tweakable 暗号方式に対する KDM 安全性の考察⁽¹⁸⁾
- OAEP 暗号方式が KDM 安全であることの証明⁽²⁶⁾
- CCA2 攻撃に対する KDM 安全性を保証する方法⁽⁴⁾
- Lattice ベースの安全性仮定に基づいて KDM 安全性を達成する方式⁽²⁷⁾
- 識別不能性を満たすが KDM 安全ではない方式の実例⁽¹²⁾(28)
- KDM 安全性と漏えい耐性の両立⁽²⁹⁾

- ポイント難読化への応用⁽³⁰⁾

3. 応用

3.1 鍵貸出問題への応用

鍵貸出問題: 鍵貸出問題とは，ユーザの属性を認証するシステムを用いる上で必然的に起こる次のような問題のことである．今例えば「自動車の運転免許を取得している」という属性を認証するシステムがあったとする．このシステムでは運転免許の取得者には事前に秘密鍵が配布されており，取得者たちはその鍵の知識を証明することで運転免許の保持を示す．

ここで問題になるのは，運転免許の取得者が取得者でないものに秘密鍵を貸し出すことができってしまうという事実である．免許取得の有無は鍵を用いて認証しているため，本来運転資格のない人物であっても誰かから鍵を借り受けさえすれば認証を通過できてしまう．

匿名の認証システム⁽⁶⁾では，この種の不正が特に大きな問題となった．その匿名性ゆえ，不正者を特定するのは不可能だからである．

KDM 安全性の応用: Camenisch と Lysyanskaya⁽⁶⁾は，循環暗号化 (circular encryption)⁽⁶⁾を用いることで鍵貸出を抑止できることを示した．ここで循環暗号化とは

$$\text{Enc}_{pk_1}(sk_2), \text{Enc}_{pk_2}(sk_3), \dots, \text{Enc}_{pk_{n-1}}(sk_n), \text{Enc}_{pk_n}(sk_1).$$

という形の暗号化のことである．ここで sk_1 は運転免許の保持を示す秘密鍵であり， $sk_2, \dots, sk_n$ は U のそれ以外の秘密鍵—例えば銀行口座から現金を引き出すための鍵や生命保険に加入していることを示す鍵—であり， $\text{Enc}_{pk_i}(\cdot)$ は sk_i に対応する公開鍵 pk_i による暗号化を示す．循環暗号化した場合には秘密鍵が暗号化されており，したがってその安全性は KDM 安全性の特殊な場合である．

循環暗号化により鍵貸出が抑止される理由は以下のとおりである．認証システムの各ユーザ U に自身の秘密鍵の循環暗号化した暗号文をあらかじめ公開させる． U が $sk_1, \dots, sk_n$ のうち一つでも別の人物 V に貸し出してしまうと， V は上述の循環暗号化した暗号文を順に復号していくことで全ての秘密鍵 $sk_1, \dots, sk_n$ を知ることができてしまう．すなわち U には，鍵を貸し出すのを諦めるか，あるいは全ての鍵を知られてしまうことを覚悟するかの二つしか選択肢がない．

これは U が運転免許に関する秘密鍵を V に貸し出すと，銀行口座から現金を引き出すための鍵すらも V に知られてしまうことを意味するため， U は鍵の貸し出しを渋るであろう．したがってユーザによる鍵貸出が抑止される．

3.2 Dolev-Yao モデルへの応用

Dolev-Yao モデル: Dolev-Yao モデル⁽⁷⁾は，暗号方式を部品

として作られたプロトコルの安全性を形式化する方法であり、安全性を形式的に検証できる。しかしこのモデルの提案当初、Dolev-Yao 的な安全性と通常の暗号学的な安全性との間の関係が明らかではなかったため、Dolev-Yao モデルの研究は通常の暗号学の研究とは独自の発展を遂げることとなった。

このモデルと通常の暗号学が「和解」したのは 20 世紀最後の年のことである。この年に Abadi と Rogaway⁽⁸⁾⁽⁹⁾ は共通鍵暗号方式の場合に対し、「もし秘密鍵に依存した情報をその秘密鍵自身を用いて暗号化していなければ、Dolev-Yao モデルにおいて安全なプロトコルは暗号学的にも安全である」という定理が示した「秘密鍵に依存した...」という制約が付くのは、従来の暗号研究においてはこのような制約のない状況での暗号化が想定されていなかったからである。

KDM 安全性の応用: 以上の議論から分かるように、自身の秘密鍵に依存した情報を暗号化しても安全性が示せる暗号方式—すなわち KDM 安全な方式—をベースにすれば、この制約は取り除くことができる⁽³¹⁾。

3.3 完全準同形暗号方式への応用

完全準同形暗号方式: 完全準同形暗号方式とは任意の関数 f に対して「 $\text{Enc}_{pk}(M)$ から $\text{Enc}_{pk}(f(M))$ を (秘密鍵を知らなくても) 計算できる」という性質が成り立つ暗号方式のことである。この性質は理論的にも興味深く、しかも暗号プロトコルを設計する際に非常に有益であるため、概念そのものは暗号研究最初期⁽¹⁰⁾に提案されている。実際にそのような方式を作ることは長年の未解決問題であったものの、2009 年、Gentry⁽¹¹⁾ は「 f を回路表現したときの段数が事前に定められた値以下である」という条件下、完全準同形暗号方式を実現した。

KDM 安全性の応用: Gentry はある種の性質を満たす暗号方式 Enc をベースとして完全準同形暗号方式 $\overline{\text{Enc}}$ を実現したが、 Enc が KDM 安全であれば、前述した回路の段数に関する制限をなくすることができることが知られている。

より正確に言うのと以下のとおりである。Gentry は「回路段数が定められた小さな値 ℓ 以下であるような f に対しては完全準同形性が成り立つ」暗号方式 Enc の公開鍵・秘密鍵ペアを $n+1$ 個用意することで「回路段数が $n\ell$ 段以下の f に対しては完全準同形性が成り立つ」提案方式 $\overline{\text{Enc}}$ を構築している。しかし Enc が前述の「回路段数が $n\ell$ 段以下...」という条件と KDM 安全性を同時に満たせば、回路段数が $n\ell$ 段以下でなければならないという制約を外せることが知られている (ただし現時点ではこの条件と KDM 安全性を同時に満たす方式は知られていない)。

完全準同形暗号と KDM 安全性が関係する理由の詳細を説明するため、Gentry のアイデアを復習する。 $(pk_0, sk_0), \dots, (pk_n, sk_n)$ を Enc の $n+1$ 個の鍵ペアとし、 $\text{PK} = (pk_0, \dots, pk_n)$, $\text{SK} = (sk_0, \dots, sk_n)$ を $\overline{\text{Enc}}$ の鍵ペアとする。 Enc から $\overline{\text{Enc}}$ を得る際 Gentry が用いたアイデアは、 $\text{Enc}_{pk_0}(M)$ から $C = \text{Enc}_{pk_0}(f_1(M))$ を計算した後、一旦復号して暗号文をリフレッシュすることで回路段数の制限に打ち勝つというものである。

すなわち $\text{Enc}_{pk_0}(C)$ から「リフレッシュされた暗号文」 $C' = \text{Enc}_{pk_1}(\text{Dec}_{sk_0}(C))$ を計算する。リフレッシュにより、 C は新しい暗号文 C' に生まれ変わるため、 C に課せられていた回路段数に関する制約は C' には適用されない。よって C' に対して ℓ 段の回路 f_2 を更に作用させ、 $\text{Enc}_{pk_1}(f_2(f_1(M)))$ を計算できる。

したがって回路段数が $n\ell$ 以下の回路 $F = f_n \circ \dots \circ f_1$ に対しても、「関数の適応 リフレッシュ」を n 回繰り返せば、 $\text{Enc}_{pk_0}(M), \text{Enc}_{pk_1}(f_1(M)), \dots, \text{Enc}_{pk_n}(f_n(\dots(f_1(M)))) = \text{Enc}_{pk_n}(F(M))$ が計算できる (話を簡単にするため、ここでは F が $F = f_n \circ \dots \circ f_1$ の形に表記できる場合のみ扱ったが、より一般の場合も同様である)。

上のアイデアではリフレッシュのたびに鍵ペアが $(pk_0, sk_0) \rightarrow (pk_1, sk_1) \rightarrow \dots \rightarrow (pk_n, sk_n)$ と変わるため、最大 n 回しかリフレッシュできず、 F の回路段数が $n\ell$ 以下でなければならないという制約が課せられてしまう。リフレッシュの際鍵ペアを変えなければこのような制約を取り除くことができるが、この場合 Enc が KDM 安全であることが必要となる。実際リフレッシュの前後で同じ鍵ペア (pk, sk) を使うことにした場合、 $\phi(sk) = \text{Dec}_{sk}(C)$ とすれば分かるように、「リフレッシュされた暗号文」 $\text{Enc}_{pk}(\text{Dec}_{sk}(C)) = \text{Enc}_{pk}(\phi(sk))$ は秘密鍵依存な暗号文になってしまう。よって回路段数に関する制約を取り除くには KDM 安全性が必須となる。

3.4 Agility との関係

Agility: Agility は Acar, Belenkiy, Bellare, Cash の 4 人⁽¹²⁾により提案された概念で、複数の暗号プリミティブに同一の鍵を与えたとしてもこれらプリミティブの安全性が担保できることを指す。複数の暗号プリミティブを用いる場合、通常なら個々のプリミティブに別々の鍵を与える必要があるが、あえて同一の鍵を与えた場合でも安全性を担保できることを保証するのが Agility である。

Acar 等は論文⁽¹²⁾で「弱擬似ランダム関数」というプリミティブに対する Agility を考察した。 K をランダムに選ばれた鍵とすると、関数 F_K が弱擬似ランダム関数であるとは攻撃者には二つのオラクル $\mathcal{O}[F_K]$ と $\mathcal{R}$ が識別不能であることを指す。ここで $\mathcal{O}[F_K]$ は攻撃者の要求に応じてランダムに選んだ x と $F_K(x)$ のペアを返すオラクルであり、 $\mathcal{R}$ は攻撃者の要求に応じてランダムに選んだ (x, y) を返すオラクルである。

$\mathcal{F}$ を弱擬似ランダム関数全体の集合とし、 k を自然数とすると、 $\mathcal{F}$ が k -agile であるとは、 $\mathcal{F}$ の任意の k 個の元 $F^{(1)}, \dots, F^{(k)}$ に対し、たとえ攻撃者が $\mathcal{O}[F_K^{(2)}], \dots, \mathcal{O}[F_K^{(k)}]$ にアクセスできたとしても $\mathcal{O}[F_K^{(1)}]$ と $\mathcal{R}$ が識別不能なことを指す。(全てのオラクルに同じ鍵 K を使っていることに注意。)

KDM 安全性の応用: $\mathcal{F}$ を弱擬似ランダム関数全体の集合とする。Acar 等⁽¹²⁾は KDM 安全性の概念を用いることで、 $k \geq 2$ に対し $\mathcal{F}$ が k -agile ではないことを (弱擬似ランダム関数が少なくとも一つ存在するという仮定の下) 示した。

証明は以下の背理法による。仮定より弱擬似ランダム関数

f_L が存在する．共通鍵暗号方式 $\Pi = (\text{Kg}, \text{Enc}, \text{Dec})$ と鍵 $\bar{K} = (L, K_1, K_2)$ と入力 x に対し，関数 $F_{\bar{K}}^{(1)}(x), F_{\bar{K}}^{(2)}(x)$ を以下のように定義する．

$$\begin{aligned} F_{\bar{K}}^{(1)}(x) &:= \text{Enc}_{K_1}(K_2; f_L(x)) \\ F_{\bar{K}}^{(2)}(x) &:= \text{Enc}_{K_2}(K_1; f_L(x)). \end{aligned}$$

ここで $\text{Enc}_K(M; R)$ は K を鍵， R を乱数として用いて M を暗号化した暗号文を指す．また K_1, K_2 は Kg によって選ばれた鍵， L は弱擬似ランダム関数 f で用いるためにランダムに選ばれた鍵（弱擬似ランダム関数が存在すれば安全な共通鍵暗号存在することが知られているため，証明に共通鍵暗号 Enc を用いることができる．）

そして Acar 等^[12]は以下を示した： $\{F^{(1)}, F^{(2)}\}$ が 2-agile で， Π が IND-R 安全（＝暗号文は乱数と識別不能）なら

$$(\text{Enc}_{K_1}(K_2), \text{Enc}_{K_2}(K_1)) \simeq (\text{Rand}_1, \text{Rand}_2) \quad (3.1)$$

である（すなわち Π を用いて暗号文数 2 の場合の循環暗号化を行っても安全である．）そして最後に (3.1) 式が成り立たない暗号方式の例を作った．これは矛盾であるため $\mathcal{E}$ は $k \geq 2$ に対し弱擬似ランダム関数に関して k -agile ではない．

4. 厳密な定義

これまで可能な限り数式を使わず KDM 安全性を説明してきたが，以降数式を用いたより詳細な説明に移る．

4.1 準備

KDM 安全性の説明に必要な事項を復習する．以下， $\mathbb{N}, \mathbb{R}$ をそれぞれ自然数全体の集合，実数全体の集合とする．

negligible: 関数 $f: \mathbb{N} \rightarrow \mathbb{R}$ が negligible であるとは，任意の自然数 n に対し

$$\lim_{\lambda \rightarrow \infty} \lambda^n \cdot f(\lambda) = 0$$

が成り立つことをいう．

公開鍵暗号方式： λ を安全性の強さを表す尺度（セキュリティパラメータ）とする．公開鍵暗号方式 Π は三つの多項式時間アルゴリズム Kg, Enc, Dec の組である．ここで Kg, Enc, Dec はそれぞれ鍵生成アルゴリズム，暗号化アルゴリズム，復号アルゴリズムと呼ばれ，それぞれ入出力は以下のとおりである．

- Kg: 1^λ を入力として受け取り，公開鍵 pk と秘密鍵 sk を出力する．

- Enc: 公開鍵 pk と平文 M を受け取り，暗号文 C を出力する．

- Dec: 秘密鍵 sk と暗号文 C を受け取り，平文を出力する．公開鍵，秘密鍵，平文の全体集合をそれぞれ公開鍵空間，秘密鍵空間，平文空間という．Kg の出力する公開鍵・秘密鍵が公開鍵・秘密鍵空間に属することと Enc に入力する平文が平文空間から選ばれることが暗に仮定されている．

公開鍵暗号方式は次の性質を満たさねばならない:

- 任意の λ ，Kg(1^λ) の任意の出力 (pk, sk) ，及び平文空間の任意の元 M に対し， $\text{Dec}_{sk}(\text{Enc}_{pk}(M)) = M$ である．

識別不能性の定義：公開鍵暗号方式の識別不能性は，以下のゲームによって定義される．ゲームは方式の安全性を破ろうとする攻撃者 A と，ゲームの主催者である実験者との間で執り行われる．まず実験者が公開鍵・秘密鍵のペア (pk, sk) を一つ生成し， pk のみ攻撃者 A に渡す．その後 A は平文 M を任意に選び，（チャレンジ）クエリ (M_0, M_1) を実験者に渡す．実験者は秘密のビット b を隠し持っており， b が 0 なのか 1 なのかに応じて，暗号化オラクルは M_0 の暗号文 $\text{Enc}_{pk}(M_0)$ か M_1 の暗号文 $\text{Enc}_{pk}(M_1)$ をクエリに対する返答（チャレンジ）として A に返す． A の目的は b が 0 なのか 1 なのかを当てることである．多項式時間のいかなる攻撃者 A であっても， b を当てられる確率が $(1/2) + \text{negligible}$ 以下なとき，公開鍵暗号方式は (CPA 攻撃に対して) 識別不能性を満たすという．

4.2 KDM 安全性の定義

本稿では公開鍵暗号方式の KDM 安全性のみを紹介する．また簡単のため特に断りがない限り，CPA 攻撃に対する KDM 安全性のみを議論する．

識別不能性からの変更点：KDM 安全性の定義は識別不能性の定義を以下の 3 点において変更することで得られる．ここで $\mathcal{F}$ は関数の集合である．

- (1) 最初に実験者が作る公開鍵・秘密鍵ペアは一つではなく複数個である．（以下これらの公開鍵，秘密鍵の組をそれぞれ $\vec{pk} = (pk_1, \dots, pk_n)$ ， $\vec{sk} = (sk_1, \dots, sk_n)$ と表記する．）
- (2) 攻撃者 A はクエリとして平文の組 (M_0, M_1) ではなく整数 $i \in \{1, \dots, n\}$ と関数 $f \in \mathcal{F}$ とを送信する．すると実験者は b に応じて $\text{Enc}_{pk_i}(f(\vec{sk}))$ か若しくは $\text{Enc}_{pk_i}(S)$ を A に返す．ここで S は事前に定められた（攻撃者にとって既知の）平文である．
- (3) A は 1 回ではなく任意回クエリを送信することができる．

上の変更を施した識別不能性を公開鍵暗号方式が満たす場合その方式は $\mathcal{F}$ -KDM 安全であるという．紛れがなければ $\mathcal{F}$ を省略し，単に KDM 安全であるという．

変更理由：変更 (1) は例えば $\text{Enc}_{pk_1}(sk_2)$ のような暗号文を考慮に入れるために施した．この変更がないと 3. で紹介した循環暗号化のようなケースがモデルに取り込めない．

変更 (2) は KDM 安全性の直観的定義から当然である．なお変更 (2) では一つの関数 f を選んで $\text{Enc}_{pk_i}(f(\vec{sk}))$ と $\text{Enc}_{pk_i}(S)$ とを識別する形で定式化した¹⁾が，二つの関数 (f, g) を選んで $\text{Enc}_{pk_i}(f(\vec{sk}))$ と $\text{Enc}_{pk_i}(g(\vec{sk}))$ とを識別するという，より識別不能性の定義に近い形で定式化しても同値な定義になる^(注1)．

変更 (3) は $\mathcal{F}$ の取り方によってはチャレンジクエリの回数が

(注1)： $\mathcal{F}$ が定数関数を含んでいるという仮定の下同値性が示せる．

一回である定義よりも任意回である定義の方が強い場合があるため施した。これは通常の識別不能性の定義の強さがクエリ回数によらないことと対照的である。

チャレンジクエリが一回の定義と任意回の定義で強さが異なる例は循環暗号化をベースにして構築できる。実際、循環暗号化の場合 n 個の秘密鍵依存暗号文 $\text{Enc}_{pk_1}(sk_2), \dots, \text{Enc}_{pk_{n-1}}(sk_n), \text{Enc}_{pk_n}(sk_1)$ 全てを (チャレンジクエリに対する返答として) 受け取った場合に初めて「循環」が発生するため、攻撃者が $n-1$ 個の暗号文しか受け取れない状況では、循環暗号化に対する KDM 安全性は単なる識別不能性と差異がない。したがってチャレンジクエリの回数が $n-1$ 回以下に制限されている場合とそうでない場合は安全性の強さが異なる。

最後に一つ細かい注意を述べる。KDM 安全性の定義は文献により公開鍵の数 n が事前に定められているものと攻撃者が n を自分で選べるものとがあり両者の定義の強さには若干の差があることが指摘されている⁽²⁵⁾。しかし両者の差が問題になるケースは少ないため、本稿では以下この点にこだわらないで解説を続けるものとする。

定義の形式的記述: λ をセキュリティパラメータとし、 $\Pi = (\text{Kg}, \text{Enc}, \text{Dec})$ を公開鍵暗号方式とする。更に $S_{pk}, \mathcal{M}_{pk}$ をそれぞれ Π の秘密鍵空間と平文空間とする。自然数 n を固定し、 $\mathcal{F}$ を S_{pk}^n から $\mathcal{M}_{pk}$ への関数の集合とし、更に平文 $S \in \mathcal{M}_{pk}$ を任意に選んで固定する。A を攻撃者、 b をビットとし、以下のゲームを考える。ここで $\vec{p}_k, \vec{s}_k$ はそれぞれ $(pk_1, \dots, pk_n), (sk_1, \dots, sk_n)$ の略記である。

- $(pk_1, sk_1) \leftarrow \text{Kg}(1^\lambda), \dots, (pk_n, sk_n) \leftarrow \text{Kg}(1^\lambda)$ を生成する。更に $b \xleftarrow{\$} \{0, 1\}$ を選ぶ。
- $A(\vec{p}_k, S)$ を実行し、以下の方法で A の任意回のクエリに答える。
 - A が $(i, f) \in \{1, \dots, n\} \times \mathcal{F}$ をクエリした場合、 $b = 0$ なら $\text{Enc}_{pk_i}(f(\vec{s}_k))$ を返し、 $b = 1$ なら $C = \text{Enc}_{pk_i}(S)$ を攻撃者に返す。
 - $d \leftarrow A$ を得る。

$b = d$ となる確率と $1/2$ との差を A のアドバンテージという。任意の多項式時間攻撃者 A に対し A のアドバンテージが negligible になるとき、 Π は (CPA 攻撃に対し) $\mathcal{F}$ -KDM 安全であるという⁽³⁾。紛れがなければ単に KDM 安全であるともいう。

KDM 安全性の定義は S の取り方に依存しているため、KDM 安全性のことを「 S に関する KDM 安全性」と呼ぶ方が厳密であるが、 $\mathcal{F}$ が全ての定数関数を含んでいれば、 S の取り方によらず KDM 安全性の定義が同値になることを簡単に示せるため、以下単に「KDM 安全性」と呼ぶ。

識別不能性との関係: 以下の性質を簡単に示せる。

定理 4.1. $\mathcal{F}$ が全ての定数関数を含んでいれば、 $\mathcal{F}$ -KDM 安全性は識別不能性を含意する。

CCA 攻撃に対する KDM 安全性: CCA 攻撃に対する KDM 安全性の定義は上のゲームにおいて復号オラクルにアクセスすることを攻撃者に許すことで得られる。もちろん攻撃者は暗号化オ

ラクルの返答を復号オラクルに送信することは許されない。CPA 攻撃、CCA 攻撃に対し $\mathcal{F}$ -KDM 安全な方式を $\mathcal{F}$ -KDM-CPA 安全、 $\mathcal{F}$ -KDM-CCA 安全ともいう。

本稿では特に断りがない限り、単に $\mathcal{F}$ -KDM 安全といった場合は CPA 攻撃に対するものを指すものとする。

5. CPA 攻撃に対して KDM 安全な方式

本章では KDM-CPA 安全な既存方式を紹介する。なお、KDM-CPA 安全な既存方式を KDM-CCA 安全な方式に変換する方法が知られているため、本章で紹介した方式を基に KDM-CCA 安全な方式も実現できる。KDM-CCA 安全な方式に変換する方法は 6. で説明する。

5.1 ランダムオラクルに頼って KDM 安全性を示す方法

ランダムオラクル仮定とは、ある種の関数 $\mathcal{H}$ の出力が (本当はランダムではないのに) ランダムに見えるという非現実的な仮定である。そのような仮定を置いた関数 $\mathcal{H}$ のことをランダムオラクルという。 $\mathcal{H}$ がランダムオラクルだという仮定の下では以下⁽³²⁾の方式⁽³²⁾が全ての関数の集合 $\mathcal{F}_{\text{all}}$ に対して $\mathcal{F}_{\text{all}}$ -KDM 安全であることを示せる⁽¹⁴⁾。

$$\text{Enc}_{pk}(M) = (\phi_{pk}(R), \mathcal{H}(R) \oplus M).$$

ここで ϕ_{pk} はトラップドア方向性置換であり、 R は暗号化の際に選ぶ乱数である。

証明は容易である。 $\mathcal{H}$ をランダムオラクルとすると、 $\mathcal{H}(R)$ は乱数であるため、 $(M$ が sk に依存していたとしても) $\mathcal{H}(R)$ が M を情報論的に隠す。よってこの方式の暗号文は乱数と識別がつかず、したがって $\mathcal{F}_{\text{all}}$ -KDM 安全性が従う。

なお論文(6)ではここで紹介したのとは異なる方法でランダムオラクル仮定の下 $\mathcal{F}_{\text{all}}$ -KDM 安全な方式を実現している。

5.2 ランダムオラクルに頼らずに KDM 安全性を示す方法

ランダムオラクルに頼らずに KDM 安全な方式を実現するのは容易なことではなく、そのような方式を実現することは長らく未解決であった。最終的に Boneh 等⁽³⁾が突破口を切り開いて以降、様々な方式が提案されているが、本質的にはどの方式も Boneh 等のアイデアに基づいて KDM 安全性を示している。

本節ではまず KDM 安全な方式を実現しようとする際に立ちはだかるジレンマを説明し、そのジレンマに打ち勝つ Boneh 等⁽³⁾のアイデア (を論文(22)(25)(29)が拡張・整理したもの) を紹介する。

KDM 安全性を示す際に立ちはだかるジレンマ: KDM 安全な方式を構築するのがなぜ困難であるのかを説明するため、暗号学で典型的な安全性証明の手法を復習し、その手法が KDM 安全性の場合には破綻してしまうことを見る。暗号方式の安全性

は、典型的には次のように示される．まず我々は，証明のベースとなる計算量的仮定—例えば DDH 仮定—を一つ選ぶ．大抵の場合，こうした仮定は何らかの秘密情報 ω —DDH ならその離散対数—を知らない場合には問題のインスタンス a がランダムなものと識別不能であるという趣旨のものである．次に我々は方式に対する攻撃者 A を使って以下のようなシミュレータ S を構成する：

- 秘密情報 ω を秘密鍵 sk に埋め込む．
- 問題のインスタンス a を公開鍵 pk やチャレンジ暗号文 C 等の公開情報に埋め込む．

A が安全性を破ることに成功した場合には S がベースとなっている問題を解くことに成功し，安全性が証明される．

しかしこの典型的な安全性証明手法は，KDM 安全性の場合には使えない．これは以下のようなジレンマが立ち上がるからである（話を簡単にするため，以下公開鍵の数 n が 1 の場合のみ説明する．）

- (1) 暗号化オラクルをシミュレートするにはクエリ f から $\text{Enc}_{pk}(f(sk))$ を計算できねばならないため S は $f(sk)$ の計算のために秘密鍵 sk を知っていなければならない．
- (2) しかしベースとなる計算量的仮定に頼って安全性を示すには， S は秘密情報 ω の対応物である sk を知っていない．

Boneh 等⁽³⁾のアイデア：上で説明した典型的証明手法の場合，二つもある上述の条件を両方とも同時に満たさねばならないという制約の下， sk という一つの秘密に頼って KDM 安全性を示さねばならないわけだから，ジレンマに陥ってしまうのも無理からぬことだ．

そこで Boneh 等⁽³⁾はジレンマを解消するため，暗号方式には攻撃者には秘密にするデータが sk 以外にも，もう一つあることに着目した．すなわちそれは暗号化に使う乱数 r のことである．彼らのアイデアの核心は，この二つの秘密 r , sk それぞれに対応して安全性証明を二段階に分けるというものである．

証明を二段階に分ければ，ジレンマは自然に解消する．第一段階では条件 (1) のみ，第二段階では条件 (2) のみを満たすように証明を進めれば，これら二条件を「両方とも同時に」満たす必要がなくなるため，ジレンマが生じないからである．こうして二つの秘密に頼って二つある各段階でそれぞれ一つずつ条件を満たせばよいという制約の下示せば KDM 安全性が証明できることになる．

次に証明をどのように二段階に分けるのかを説明するため， Game_0 ， Game_1 ， Game_2 を以下のように定義する．ここで擬似暗号文 $\text{PEnc}_{pk}(f)$ とは，チャレンジ暗号文とは違い，公開鍵 pk とクエリ f さえ知っていれば sk を知らなくとも計算できるデータである．なお「擬似暗号文」という名称は論文 (25) に従った．

- Game_0 : KDM 安全性のゲーム
- Game_1 : Game_0 におけるチャレンジ暗号文 $\text{Enc}_{pk}(f(x))$ を擬似暗号文 $\text{PEnc}_{pk}(f)$ に置き換えたゲーム．
- Game_2 : Game_1 における擬似暗号文 $\text{PEnc}_{pk}(f)$ を乱数に置き換えたゲーム．

証明の第一段階は， Game_0 における攻撃者 A の view と

表 1 Boneh 等⁽³⁾による二段階証明． Game_0 と Game_1 の識別不能性は，シミュレータ S が sk を知っている状況で暗号化の乱数 r の秘匿性に頼って証明する． Game_1 と Game_2 の識別不能性は， S が sk を知らない状況で sk の秘匿性に頼って証明する．

	暗号文	sk への依存性	f への依存性
Game_0	チャレンジ暗号文	Yes.	Yes.
Game_1	擬似暗号文	No.	Yes.
Game_2	乱数	No.	No.

Game_1 におけるそれが識別不能なことを示す段階である．これを示すにはチャレンジ暗号文と擬似暗号文が識別不能なことを示せばよい．チャレンジ暗号文と擬似暗号文の識別不能性は，暗号化に使う乱数 r の秘匿性に頼って証明する．例えば論文 (29) では，計算量的な問題の秘密情報を r に埋め込むという方法で証明している．このフェーズでは sk の秘匿性に頼る必要はないため，シミュレータ S は秘密鍵 sk を使ってチャレンジ暗号文 $\text{Enc}_{pk}(f(sk); r)$ （かそれと識別不能な擬似暗号文）を計算できる．すなわち前述した条件 (1) が満たされる．

証明の第二段階は， Game_1 における攻撃者 A の view と Game_2 におけるそれが識別不能なことを示す段階である．これを示すには擬似暗号文が乱数と識別不能なことを示せばよい．ここで擬似暗号文 $\text{PEnc}_{pk}(f)$ は sk を知らなくとも計算できたことを思い出されたい．したがってこの第二段階は「 sk を知らないまま」，「 sk の秘匿性に頼って」ベースとなる問題を埋め込むという条件 (2) を満たすことができる．

Game_2 で暗号文は乱数に置き換わっているため，オラクルからの返答は攻撃者がクエリした f に依存しない．したがって Game_2 における攻撃者のアドバンテージは 0 であるため，KDM 安全性が示されることとなる．

以上の二段階証明を表 1 にまとめた．

5.3 簡単な具体例

5.2 のアイデアが実際にどのように用いられるのかを説明するため，エルガマル暗号方式がある種の $\mathcal{F}$ に対して $\mathcal{F}$ -KDM 安全であることを証明する．あくまでこれは分かりやすさのためにもち出した例であるため， $\mathcal{F}$ はかなり人工的なものである．しかしながら我々がここで与える証明は多くの方式における KDM 安全性の証明のひな形になっており，Boneh 等の論文⁽³⁾はもちろぬ，論文 (25) (27) (29) も本質的にはここで述べる証明と同種の方法で KDM 安全性を示している．

エルガマル暗号方式の復習： $\mathbb{G}$ を有限巡回群とし， g をその生成元とする．エルガマル暗号方式 (Kg, Enc, Dec) は以下のような方式である．

- Kg(1^λ) : ランダムに $x \xleftarrow{\$} \mathbb{Z}_p$ を選び， $sk \leftarrow x$ ， $pk \leftarrow h \leftarrow g^x$ とする．
- $\text{Enc}_{pk}(M)$ for $M \in \mathbb{G}$: ランダムに $r \xleftarrow{\$} \mathbb{Z}_p$ を選び， $C \leftarrow (u, v) \leftarrow (g^r, Mh^r)$ を出力する．
- $\text{Dec}_{sk}(C)$: $C = (u, v)$ と書き， v/u^x を出力する．

関数集合 $\mathcal{F}$: 我々が KDM 安全性を示す関数の集合 $\mathcal{F}$ は, 秘密鍵 $x_1, \dots, x_n$ の線型結合 $\sum_i a_i x_i$ を g の肩に乗せたものの集合である. すなわち,

$$\mathcal{F} = \{g^{\sum_i a_i x_i} \mid a_i \in \mathbb{Z}_p\}$$

である.

特に $n = 1$ であれば,

$$\mathcal{F} = \{g^{ax} \mid a \in \mathbb{Z}_p\}$$

となる.

$n = 1$ の場合の KDM 安全性: 我々はまず $n = 1$ の場合にエルガマル暗号方式が $\mathcal{F}$ -KDM 安全であることを示す. x を秘密鍵とし, $h = g^x$ を対応する公開鍵とする. $n = 1$ であるため, $f \in \mathcal{F}$ は $f(x) = g^{ax}$ の形で表記できる.

証明は前述した Boneh 等⁽³⁾の二段階証明法に基づく. 二段階証明法における擬似暗号文 $\text{PEnc}_{pk}(f)$ は,

$$\text{PEnc}_{pk}(f) = (g^{-a} g^t, h^t)$$

である. ここで $t \in \mathbb{Z}_p$ は乱数である. $\text{Game}_0, \text{Game}_1, \text{Game}_2$ を二段階証明法の説明のときと同様に定義する. すなわち $\text{Game}_0, \text{Game}_1, \text{Game}_2$ において, A が関数 f をオラクルにクエリしたときの返答はそれぞれチャレンジ暗号文 $\text{Enc}_{pk}(f(x)) = (g^r, g^{ax} h^r)$, 擬似暗号文 $\text{PEnc}_{pk}(f) = (g^{-a} g^t, h^t)$, 乱数である.

二段階証明法の第一段階は, Game_0 における攻撃者 A の view が, Game_1 のそれと識別不能なことを, 暗号化の乱数 r の秘匿性に頼って示すというものである. 二つのゲームにおける view が (統計的に) 識別不能であることは, $t = r + a \bmod p$ とすると以下のように示せる:

$$\begin{aligned} \text{Enc}_{pk}(f(sk)) &= (g^r, g^{ax} (g^x)^r) = (g^r, g^{x(a+r)}) \\ &= (g^{t-a}, g^{xt}) = (g^{-a} g^t, h^t) = \text{PEnc}_{pk}(f). \end{aligned}$$

証明の第二段階は, Game_1 における A の view と, Game_2 におけるそれが識別不能なことを, 秘密鍵 x の秘匿性に頼って示すというものである. これは DDH 仮定から容易に導くことができる. というのも秘密鍵 x は秘匿されているという事実があったため, DDH 問題のインスタンスの秘密情報—すなわち離散対数—を x に埋め込むことができるからである. より正確にいうと, (g_*, h_*, u_*, v_*) を DDH 問題のインスタンスとすると, 公開鍵 (g, h) , 暗号文 (u, v) をそれぞれ $(g, h) \leftarrow (g_*, h_*)$, $(u, v) \leftarrow (g^{-a} u_*, v_*)$ とすればよい.

こうして二段階証明により KDM 安全性のゲームのチャレンジ暗号文が乱数と識別不能ことが示されたことになる. よってエルガマル暗号方式は $\mathcal{F}$ -KDM 安全である.

n が一般の場合の KDM 安全性: 最後に我々は, 鍵の数 n が 1 とは限らない一般の場合に対してエルガマル暗号方式の $\mathcal{F}$ -KDM 安全性を示す. この一般の場合には我々は, 未知の乱数 x_0 と既知の乱数 $k_1, \dots, k_n$ を取り, $i = 1, \dots, n$ に対して秘密鍵 x_i を

$$x_i = x_0 + k_i \bmod p$$

とセットする. このようにすると鍵の数が n 個の場合の KDM 安全性は実質的には一つの鍵 x_0 しかない場合の KDM 安全性と大差がないことが分かる. よって前述した安全性証明を上アイデアに従って改変すれば鍵の数が n 個の場合の $\mathcal{F}$ -KDM 安全性が示せる.

5.4 KDM 安全な既存の方式^{(3) (25) (27) (29)}

本節では既存の方式^{(3) (25) (27) (29)}を復習し, これらが「自己暗号化」 $\text{Enc}_{pk}(sk)$ に対して KDM 安全であることをみる. (本節では簡単のため自己暗号化のみを扱うが, 論文^{(3) (25) (27) (29)}はより広い関数のクラスに対して KDM 安全性が示されている.)

そのために基本となるアイデアは, 5.3 で与えたエルガマル暗号方式の $\mathcal{F}$ -KDM 安全性の証明方法である. しかし 5.3 の場合, 関数集合 $\mathcal{F}$ が含んでいるのは $x \mapsto g^{ax}$ という形の関数のみで, 恒等写像 $\text{id}: x \mapsto x$ を含んでいないため, 自己暗号文 $\text{Enc}_{pk}(\text{id}(sk)) = \text{Enc}_{pk}(sk)$ はこの KDM 安全性では対象外になってしまっている.

そこで論文^{(3) (25) (27) (29)}では暗号方式を改良して, g^{ax} の肩 ax を g から降ろしている. こうすれば 5.3 の方法で KDM 安全性が示せる暗号文 $\text{Enc}_{pk}(g^{sk})$ において sk が g の肩から降り, 自己暗号化 $\text{Enc}_{pk}(sk)$ に対する KDM 安全性が示せる. 論文^{(3) (25) (27) (29)}のアイデアの詳細は以下のとおりである.

論文^{(25) (29)}の方式: 論文^{(25) (29)}では, エルガマルそれ自身の代わりに Paillier 風⁽³³⁾のエルガマル暗号文

$$(g^r, (1+N)^M h^r) \bmod N^2$$

を考えている. ここで M は明文, N は RSA モジュラス.

よく知られているように⁽³³⁾, $(1+N)^M$ から M を計算するのは容易である. つまり明文 M が「肩から降りる». よって前述した理由により, 自己暗号文 $\text{Enc}_{pk}(sk)$ に関する KDM 安全性が示せる. 論文^{(25) (29)}はこれに更なる改良を図ることで, より大きな関数集合 $\mathcal{F}$ に対して KDM 安全性を示している.

論文⁽²⁷⁾の方式: 一方, 論文⁽²⁷⁾では LWE 風⁽³⁴⁾のエルガマル暗号文

$$C = (Gr, Hr + Mp + e) \bmod p^2,$$

を考えている. ここで M は明文, G と H は行列, r は乱数, e は「エラー項». 上式から e と p を消し去れば, エルガマル暗号方式の加法表記とよく似たものになることが分かる. 前節で説明したエルガマルの KDM 安全性の証明と同様の議論でこの方式の KDM 安全性を示せる⁽²⁷⁾. しかもエルガマル暗号方式の場合と違い, HM から M を計算すること (「離散対数問題」に相当) は困難ではないため, 前述した「肩から降ろす」操作はそもそも必要ない.

論文⁽³⁾の方式: 最後に Boneh 等⁽³⁾自身の方式の詳細を述べる.

この方式は，

$$\begin{aligned} sk &= (g_1^{x_1}, \dots, g_\ell^{x_\ell}), \\ pk &= (g_1, \dots, g_\ell, h = \prod_i g_i^{x_i}) \\ \text{Enc}_{pk}(M) &= (g_1^r, \dots, g_\ell^r, Mh^r) \end{aligned}$$

である．ここで $x_1, \dots, x_n$ はランダムに選ばれた 1 ビットである． x_i は 1 ビットであるため秘密鍵 $(g_i^{x_i})_i$ から $(x_i)_i$ を容易に復元できる．すなわち秘密鍵を「肩から降ろす」のは容易である（にもかかわらず $(x_i)_i$ でなく $(g_i^{x_i})_i$ を秘密鍵にしているのは秘密鍵を群の元の組にするためである．）

復号の際は sk から $(x_1, \dots, x_\ell)$ を復元し，これを使って暗号文を復号できる．

また 5.3 と同様のアイデアで秘密鍵の一部 g^{x_i} を暗号化して $\text{Enc}_{pk}(g^{x_i})$ を計算しても KDM 安全であることが示せることが示せる． ℓ 個の暗号文 $\text{Enc}_{pk}(g^{x_1}), \dots, \text{Enc}_{pk}(g^{x_\ell})$ を考えれば実質的には秘密鍵を自己暗号化したも同然であるため，本方式は実質的には自己暗号化に対して KDM 安全であるといえる．

6. CCA 攻撃に対して KDM 安全な方式

これまで本稿では CPA 攻撃に対する KDM 安全性のみを対象にしてきたが，この章では CCA 攻撃に対する KDM 安全性を達成する方法⁽⁴⁾を述べる．この章で紹介する方法は Camenisch, Chandran, Shoup の 3 人⁽⁴⁾によって提案された．彼らの方法は本質的には古典的な Naor-Yung 法⁽¹³⁾と同様である．

既存のテクニックの大半が失敗する理由：まず Naor-Yung 法以外の既知の CCA 達成テクニックがいずれも KDM 安全性の場合には使えないことを，Cramer-Shoup 暗号方式^{(35) (36)}のテクニックを例に説明する．

そのために Cramer-Shoup 暗号方式の暗号化アルゴリズムを簡単に復習する．Cramer-Shoup 暗号方式の暗号化アルゴリズムはエルガマル風の暗号文 $C = \text{Enc}_{pk}(M)$ に $\text{Enc}_{pk}(M)$ が正しい方法で作られていることを証明するチェック機構 w を付け加えた $\overline{\text{Enc}}_{pk}(M) = (\text{Enc}_{pk}(M), w)$ を暗号文とすることで CCA 攻撃に対する耐性を実現している．このチェック機構の追加に伴って秘密鍵にもデータ追加を行う必要があり，元々の Enc の秘密鍵 sk にチェック用のデータ α を付け加えた $\overline{sk} = (sk, \alpha)$ を $\overline{\text{Enc}}$ の秘密鍵としている．公開鍵の方も同様にチェック関連のデータが加わる．

さて，CPA 攻撃の下自己暗号化に対し KDM 安全な暗号化アルゴリズム Enc^{KDM} に Cramer-Shoup 風のチェック機構 w を付け加えることで CCA 攻撃の下自己暗号化に対して KDM 安全な暗号方式（の暗号化アルゴリズム） $\overline{\text{Enc}}^{\text{KDM}}$ を作るうとしてもうまくいかない．なぜなら Enc^{KDM} を $\overline{\text{Enc}}^{\text{KDM}}$ に変更した時点で「自己暗号化」の意味が変わってしまうからである．実際 Enc^{KDM} の場合「自己暗号化」とは sk を暗号化した $\text{Enc}_{pk}^{\text{KDM}}(sk)$ のことであるがそれに対し $\overline{\text{Enc}}^{\text{KDM}}$ の場合「自己暗号化」は $\overline{sk} = (sk, \alpha)$ を暗号化した $\overline{\text{Enc}}_{pk}^{\text{KDM}}(\overline{sk})$ のことを意味する．

Enc^{KDM} の KDM 安全性と Cramer-Shoup のテクニックが

保証しているのは， sk を暗号化した場合の KDM-CCA 安全性のみで， $\overline{sk} = (sk, \alpha)$ を暗号化した場合には KDM-CCA 安全性が保証されとは限らない．（少なくとも α の情報論的秘匿性に頼った Cramer-Shoup の議論^{(35) (36)}は破綻する．）

もちろん $\overline{\text{Enc}}_{pk}^{\text{KDM}}(\overline{sk})$ でなく $\overline{\text{Enc}}_{pk}^{\text{KDM}}(sk)$ を作成した場合の KDM-CCA 安全性なら証明できるが，これでは秘密鍵 $\overline{sk} = (sk, \alpha)$ の一部分 sk を暗号しても安全だといったにすぎず，かなり弱い KDM 安全性がいたにすぎない．

以上の考察から，秘密鍵長を変えないことが自己暗号化に対する KDM-CCA 安全性を達成する上で重要なことが分かる．Camenisch, Chandran, Shoup の 3 人⁽⁴⁾は，Naor-Yung 法⁽¹³⁾—これは秘密鍵長を変えない—を使えば自己暗号化に対する KDM-CCA 安全性を達成することができることを示した．

Naor-Yung 法⁽¹³⁾ 次に Naor-Yung 法を復習する．Naor-Yung 法は，CPA 攻撃に対し識別不能性を満たす二つの暗号方式 Enc, Enc' を用意し，

$$\overline{\text{Enc}}_{pk}(M) = (\text{Enc}_{pk}(M), \text{Enc}'_{pk'}(M), \text{pf})$$

を暗号文とすることで CCA 攻撃に対する識別不能性を達成している．ここで pf は $\text{Enc}_{pk}(M)$ と $\text{Enc}'_{pk'}(M)$ が同じ平文 M を暗号化していることを示す Publicly Verifiable なゼロ知識証明文であり， $\overline{pk} = (pk, pk')$ （ゼロ知識証明文に用いる公開情報）である．

$\overline{\text{Enc}}_{pk}(M)$ を復号するには， pf の正当性を確認した後， pk に対応する秘密鍵 sk を使って $\text{Enc}_{pk}(M)$ を復号すればよい．

以上で分かるように，復号の際に使うのは pk に対応する秘密鍵 sk のみで， pk' に対応する秘密鍵は必要ない（しかも pf は Publicly Verifiable なので， pf の検証にいかなる秘密情報も必要ない．）によって自己暗号化に対する KDM 安全性を達成するのに必要な前述した性質（ $\overline{\text{Enc}}$ の秘密鍵 = Enc の秘密鍵）を Naor-Yung 法は満たしている．

CCA 攻撃に対する KDM 安全性: Camenisch 等⁽⁴⁾の成果は以下のとおりである．

定理 6.1. $\mathcal{F}$ を関数集合とする． Enc が $\mathcal{F}$ -KDM-CPA 安全であり， Enc' が CCA 攻撃に対し識別不能性を満たせば $\overline{\text{Enc}}$ は $\mathcal{F}$ -KDM-CCA 安全．

元々の Naor-Yung 法⁽¹³⁾では Enc' に CPA 耐性しか求めないのに対し，上述の定理では Enc' に CCA 耐性を求めていることに注意されたい．

Enc' に CCA 耐性が必要な理由：理由を説明するために，Naor-Yung 法で作られた $\overline{\text{Enc}}$ が CCA 攻撃に対し識別不能性を満たすことの証明を振り返る．この証明では Enc の安全性に頼るため， Enc の秘密鍵を知らないシミュレータを構成する．このシミュレータが復号オラクルのシミュレートする際に使うのが Enc' の秘密鍵 sk' である．証明文 pf により， $\overline{C} = \overline{\text{Enc}}_{pk}(M) = (C, C', \text{pf})$ の第一成分 C の復号結果と第二成分 C' の復号結果は同一であることが保証されているため， Enc' の秘密鍵 sk' を知ってさえいれば $\text{Dec}'_{sk'}(C')$ を計算することで $\overline{C}$ を復号できる．よって

シミュレータは sk を知らなくて済む。

しかし KDM-CCA 安全性の場合は以上のアイデアがうまくいかない。 $\overline{\text{Enc}}$ が自己暗号化に対する KDM-CCA 安全性を満たしていることを示す場合には、シミュレータはチャレンジ暗号文

$$\overline{C}_* = \overline{\text{Enc}}_{pk}(sk) = (\text{Enc}_{pk}(sk), \text{Enc}'_{pk'}(sk), \text{pf})$$

を計算する必要があるからである。ここで CCA 攻撃に対する識別不能性の証明の場合と同様 sk' を使って復号オラクルをシミュレートしようとするとき失敗する。なぜなら sk' を使うにはシミュレータが sk' を知っていなければならないわけだが、そうするとシミュレータは C_* の第二成分 $\text{Enc}'_{pk'}(sk)$ を復号することで sk を得ることができてしまう。よって「 sk を知らないままシミュレーションを行う」という大前提が崩れてしまう。

以上の議論から分かるように KDM-CCA 安全性を示すには、 sk のみならず sk' すらも知らない状態でシミュレーションを行う必要がある。

これを可能にするのが Enc' の CCA 耐性である。 Enc' に CCA 耐性があれば、 sk 、 sk' のいずれも知らなくとも Enc' の復号オラクルに C' をクエリすることで $\overline{C} = (C, C', \text{pf})$ を復号できるからである。こうして前述の問題は解決され、 $\overline{\text{Enc}}$ の KDM-CCA 安全性が示されることとなる。

7. ま と め

本稿では KDM 安全性の既存研究をサーベイした。KDM 安全性は暗号方式の安全性の再考察という近年注目されている研究課題の一つである。理論上、応用上の重要性も次第に明らかになりつつある概念のため、今後もこの概念は注目され続けるであろう。

謝 辞 本稿を書く機会を下さった IEICE Fundamental Review の関係者の方々、特に伊豆哲也氏、國廣昇先生に深く感謝致します。本稿に対する有益なご指摘を下さった吉田真紀先生、國廣昇先生、KDM 安全な暗号方式を研究した際に有益な御意見を下さった Moti Yung 先生、Tal Malkin 先生にも深く感謝致します。

文 献

- (1) S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial information," STOC, pp.365–377, 1982.
- (2) S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol.28, no.2, pp.270–299, 1984.
- (3) D. Boneh, S. Halevi, M. Hamburg, and R. Ostrovsky, "Circular-secure encryption from decision diffie-hellman," CRYPTO, pp.108–125, 2008.
- (4) J. Camenisch, N. Chandran, and V. Shoup, "A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks," EUROCRYPT, pp.351–368, 2009.
- (5) B. Barak, I. Haitner, D. Hofheinz, and Y. Ishai, "Bounded key-dependent message security," EUROCRYPT, pp.423–444, 2010.
- (6) J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," EUROCRYPT, pp.93–118, 2001.
- (7) D. Dolev and A.C.-C. Yao, "On the security of public key protocols," IEEE Trans. Inf. Theory, vol.29, no.2, pp.198–207, 1983.
- (8) M. Abadi and P. Rogaway, "Reconciling two views of cryptography (the computational soundness of formal encryption)," IFIP TCS, pp.3–22, 2000.
- (9) M. Abadi and P. Rogaway, "Reconciling two views of cryptography (the computational soundness of formal encryption)," J. Cryptol., vol.20, no.3, p.395, 2007.
- (10) R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms. in foundations of secure computation," Foundations of Secure Computation, pp.169–180, Academic Press, 1978.
- (11) C. Gentry, "Fully homomorphic encryption using ideal lattices," STOC, pp.169–178, 2009.
- (12) T. Acar, M. Belenkiy, M. Bellare, and D. Cash, "Cryptographic agility and its relation to circular encryption," EUROCRYPT, pp.403–422, 2010.
- (13) M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," STOC, pp.427–437, 1990.
- (14) J. Black, P. Rogaway, and T. Shrimpton, "Encryption-scheme security in the presence of key-dependent messages," Selected Areas in Cryptography, pp.62–75, 2002.
- (15) R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," J. ACM, vol.51, no.4, pp.557–594, 2004.
- (16) M. Liskov, R.L. Rivest, and D. Wagner, "Tweakable block ciphers," CRYPTO, pp.31–46, 2002.
- (17) P. Rogaway, "Efficient instantiations of tweakable blockciphers and refinements to modes ocb and pmac," ASIACRYPT, pp.16–31, 2004.
- (18) S. Halevi and H. Krawczyk, "Security under key-dependent inputs," ACM Conference on Computer and Communications Security, pp.466–475, 2007.
- (19) IEEE P1619, "Standard for cryptographic protection of data on block-oriented storage devices," 2007.
- (20) IEEE P1619 email archive 2007, <http://grouper.ieee.org/groups/1619/email>.
- (21) D. Hofheinz and D. Unruh, "Towards key-dependent message security in the standard model," EUROCRYPT, pp.108–126, 2008.
- (22) Z. Brakerski, S. Goldwasser, and Y. Kalai, "Circular-secure encryption beyond affine functions," Cryptology ePrint Archive, Report 2009/485, 2009. <http://eprint.iacr.org/>.
- (23) I. Haitner and T. Holenstein, "On the (im)possibility of key dependent encryption," TCC, pp.202–219, 2009.
- (24) B. Applebaum, "Key-dependent message security: Generic amplification and completeness," EUROCRYPT, pp.527–546, 2011.
- (25) T. Malkin, I. Teranishi, and M. Yung, "Efficient circuit-size independent public key encryption with kdm security," EUROCRYPT, pp.507–526, 2011.
- (26) M. Backes, M. Dürmuth, and D. Unruh, "OAEP is secure under key-dependent messages," ASIACRYPT, pp.506–523, 2008.
- (27) B. Applebaum, D. Cash, C. Peikert, and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems," CRYPTO, pp.595–618, 2009.
- (28) M. Green and S. Hohenberger, "Cpa and cca-secure encryption systems that are not 2-circular secure," Cryptology ePrint Archive, Report 2010/144, 2010. <http://eprint.iacr.org/>.
- (29) Z. Brakerski and S. Goldwasser, "Circular and leakage resilient public-key encryption under subgroup indistin-

guishability - (or: Quadratic residuosity strikes back),” CRYPTO, pp.1–20, 2010.

- (30) R. Canetti, Y.T. Kalai, M. Varia, and D. Wichs, “On symmetric encryption and point obfuscation,” TCC, pp.52–71, 2010.
- (31) P. Adão, G. Bana, J. Herzog, and A. Scedrov, “Soundness of formal encryption in the presence of key-cycles,” ESORICS, pp.374–396, 2005.
- (32) M. Bellare and P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols,” ACM Conference on Computer and Communications Security, pp.62–73, 1993.
- (33) P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” EUROCRYPT, pp.223–238, 1999.
- (34) O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” J. ACM, vol.56, no.6, pp.84–93, 2009.
- (35) R. Cramer and V. Shoup, “A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack,” CRYPTO, pp.13–25, 1998.
- (36) R. Cramer and V. Shoup, “Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack,” SIAM J. Comput., vol.33, pp.167–226, 2001.

(ISEC 研究会提案 , 平成 24 年 3 月 14 日受付

5 月 7 日最終受付)

寺西 勇 (正員)

2000 東工大・理・数学卒, 2002 同大学院数学専攻修士課程了, 同年, 日本電気入社。2008 同大学院集積システム専攻博士課程了。現在, 日本電気にて暗号の研究に従事。2005 SCIS 論文賞受賞。