IMES DISCUSSION PAPER SERIES

量子コンピュータの脅威を考慮した高機能暗号：格子問題に基づく準同型暗号とその応用

四方順司（しかたじゅんじ）

Discussion Paper No. 2018-J-7

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2018-J-7
2018 年 5 月

量子コンピュータの脅威を考慮した高機能暗号：格子問題に基づく準同型暗号とその応用

四方順司（しかたじゅんじ）*

要　旨

近年、量子コンピュータの研究開発が進展する中、この技術を利用者もしくは攻撃者が利用できる環境において、情報セキュリティの安全性が確保されることが求められている。こうした観点から、現代のコンピュータに対してだけでなく、量子コンピュータに対しても安全性を有する暗号技術の研究開発が活発化している。その一方で、暗号化や認証といった基本的機能を拡張し、さらに高度な機能をもった暗号技術、例えば、暗号化したままさまざまな情報処理を可能とするような高機能暗号の研究開発が活発化している。高機能暗号は、クラウド計算、ビッグデータ分析、IoT（Internet-of-Things）等のセキュリティと親和性のある暗号技術として期待できる。本稿では、こうした暗号技術を取り巻く研究開発動向を踏まえ、量子コンピュータの影響を考慮した高機能暗号、とりわけ、格子問題に基づく完全準同型暗号とその応用に関して解説する。

キーワード：完全準同型暗号、高機能暗号、格子問題、耐量子計算機暗号、量子コンピュータ
JEL classification: L86、L96、Z00

* 横浜国立大学大学院環境情報研究院（E-mail: shikata@ynu.ac.jp）

本稿は、筆者が日本銀行金融研究所客員研究員の期間に行った研究をまとめたものである。本稿の作成に当たっては、筑波大学大学院の佐久間淳氏、および金融研究所スタッフから有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目 次

１．はじめに

近年の計算技術および通信技術の発展は著しく、情報社会は日々進歩している。すなわち、現代のコンピュータは、計算処理速度や記憶容量（メモリ）において目覚ましい性能向上がみられるほか、有線および無線それぞれの通信技術も著しく発展してきている。

近年、これまでの計算技術や通信技術とは異なる新たな技術として、量子コンピュータの研究開発が行われている。量子コンピュータとは、量子力学の性質を演算処理に利用したコンピュータの総称であり、現代のコンピュータと比較して極めて高速な演算処理を実現できるとされている。そのため、現代のコンピュータに対してだけでなく、量子コンピュータに対しても安全性を有する暗号技術の研究開発が活発化してきている。これは、量子コンピュータや量子通信の研究開発が進展する中、将来、これらを利用者もしくは攻撃者が利用できる環境においてセキュリティを確保することが求められているためである。

米国および欧州では、量子コンピュータに耐性を有する暗号技術の標準化へ向けた取組みが進められている。特に、米国立標準技術研究所（National Institute of Standards and Technology : NIST）は、「現在主流の RSA 暗号を数時間で解読可能な量子コンピュータが 2030 年までに実現できる可能性がある」との見解を示している。現在、米国政府は量子コンピュータでも解読できない公開鍵暗号の標準化を進めており、全世界から暗号アルゴリズムを募集し、その後、数年をかけて米国標準暗号を選定する予定としている（National Institute of Standards and Technology [2018]）。

その一方で、近年、暗号化や認証といった基本的機能を拡張し、さらに高度な機能を有する暗号技術、例えば、暗号化したまま各種の情報処理を可能とする高機能暗号の研究開発が活発化している。高機能暗号は、クラウド計算、ビッグデータ分析、IoT（Internet-of-Things）等のセキュリティと親和性のある暗号技術として期待されている。

本稿では、現代のコンピュータだけでなく量子コンピュータにも耐性を有し、かつ、多様で高度な情報処理を可能とする高機能暗号、特に、格子問題に基づく完全準同型暗号の仕組み、およびその応用について説明する。

２．公開鍵暗号と量子コンピュータ

（１）公開鍵暗号の概要

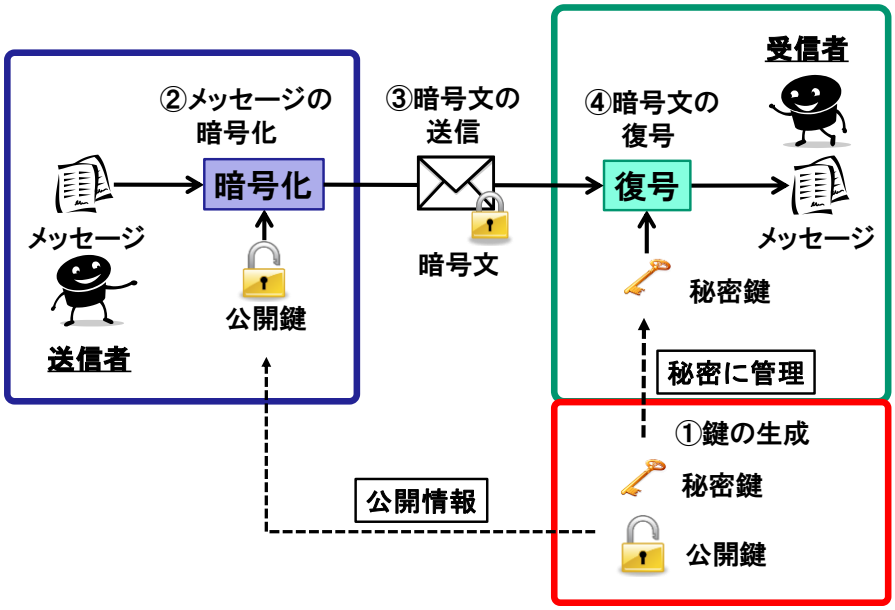
公開鍵暗号は、暗号化に利用する鍵（公開鍵）と復号に利用する鍵（秘密鍵）が異なり、復号に利用する鍵は各利用者が秘密に保管する必要がある一方、暗号化に利用する鍵を公開できるという特長を有する。ここで、受信者は、予め公開鍵と秘密鍵を生成し、送信者はこの公開鍵を入手しているものとする。送

信者は、メッセージを公開鍵を用いて暗号文に変換したうえで送信し、それを受信した受信者は秘密鍵を用いて元のメッセージに復号する（図表 1）。

公開鍵暗号では、公開鍵を有する攻撃者が当該公開鍵から秘密鍵を効率よく求められないように構成することが最低限必要であるが、それ以上の安全性要件を設定することが標準的である。具体的には、攻撃対象となる暗号文からメッセージの内容が攻撃者に漏えいしないことが安全性要件として設定される[1]。

代表的な公開鍵暗号として、RSA 暗号（Rivest, Shamir, and Adleman [1978]）や楕円曲線暗号（Koblitz [1987]、Miller [1985]）がよく知られている[2]。これらの暗号は、インターネット・バンキングの安全性を確保するために用いられる暗号通信プロトコル TLS（Transport Layer Security）において、利用可能な公開鍵暗号として規定されている（Dierks and Rescorla [2008]）。さらに、金融分野に関連する情報セキュリティ技術の国際標準、業界標準仕様や各種ガイドラインで規定されている（International Organization for Standardization [2007]、 American National Standards Institute [2005]、金融情報システムセンター［2015］等）。このように、RSA 暗号と楕円曲線暗号は、現在主流の公開鍵暗号として位置づけられている。

図表 1．公開鍵暗号のモデル



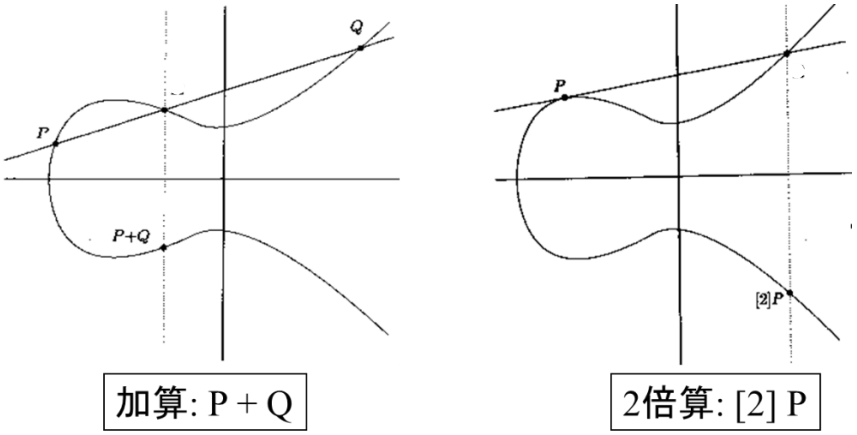
[1] 上記安全性要件は、さらにメッセージの内容全体が漏えいしないもの（一方向性）と、メッセージの部分情報さえも（1 ビットの情報さえも）漏えいしないもの（識別困難性）に分類される。識別困難性の方が一方向性よりも強い安全性要件である。なお、暗号文を改変し、本来とは異なる他のメッセージへ復号されることを防ぐ安全性要件も考えられるが、この要件を満たすには構成が複雑になることが多い。

[2] RSA 暗号と楕円曲線暗号の実用化動向や安全性評価の詳細については、清藤・四方［2013］等を参照されたい。

図表 2.　RSA 暗号と楕円曲線暗号で利用される数学的問題

数学的問題の名称	概要
素因数分解問題	2 つの素数p、qとその積 $n = p \times q$に対して、nが与えられたとき、pとqを求める問題。
楕円曲線 離散対数問題	楕円曲線上の点 Pを s個足した点 $T = [s]P$ に対して、Pと Tが与えられたとき、sを求める問題。ここで、$[s]P$とは、P を s 個足すことを意味する。

図表 3.　楕円曲線上の演算の幾何学的イメージ



RSA 暗号は、上記の安全性要件を満たすために、桁数が大きな 2 つの素数の積（合成数）から元の素数を現実的な時間で求めることが困難であるという問題（素因数分解問題）の一種を利用している[3]。一方、楕円曲線暗号は、特殊な代数曲線（楕円曲線）上の点をある個数分足した点から、元の点を現実的な時間で求めることが困難であるという問題（楕円曲線離散対数問題）の一種を利用している（図表 2)。楕円曲線は、曲線上の点同士を足すという演算（加算）を行うことが可能という特長を有している。図表 3 は、楕円曲線上の異なる 2 点 P、Q を加算した結果（$P + Q$)、点 P 同士を加算した結果（$P + P$)（これを$[2]P$と書く）が当該曲線上でどのような点に対応しているかを幾何学的に示したものである。楕円曲線離散対数問題は、この特徴を利用して定義される数学的問題である。これらの問題は、現時点で最も高性能なスーパーコンピュータを利用したとしても、解を求めるためには膨大な時間が必要となることが知られている。

[3] 一般に、素因数分解問題は、2 以上の自然数を与えたときに、その素因数分解（素数の積による表現）を求める問題である。RSA 暗号で利用する素因数分解問題は、与えられた自然数が 2 つの異なる素数の積となることを既知として、それら 2 つの素数を求める（限定された）ものである。

（２）量子コンピュータが暗号技術に与える影響と対策

イ．量子ゲート型コンピュータ

量子コンピュータは、その原理の違いにより量子アニーリング型コンピュータと量子ゲート型コンピュータに分類される。量子ゲート型コンピュータは、任意の問題を解くことを目的としているのに対し、量子アニーリング型コンピュータは、特定の組合せ最適化問題を解くことを目的としている。現時点では、量子アニーリング型コンピュータを用いて、暗号を効率よく解読することは難しいと考えられている[4]。このため、本稿では、量子ゲート型コンピュータに注目する。

量子ゲート型コンピュータは、重ね合わせ状態と呼ばれる複数の状態が同時に存在する性質を演算に利用した、量子コンピュータの実装方式の 1 つである。従来のコンピュータにおいては、1 つのビットで 0 または 1 のどちらかの状態のみ表現できるのに対し、量子ゲート型コンピュータでは、重ね合わせ状態を利用することにより、1 つのビット（1 量子ビットと呼ばれる）で 0 と 1 の状態を同時に表現できる。そして、量子ビットに対して演算処理を行った後、量子ビットの観測を行うと、重ね合わせ状態が失われ、いずれかの状態が確率的に定まる[5]。

ロ．公開鍵暗号の安全性低下

近年、量子ゲート型コンピュータの実用化に向けた研究開発が活発化しており、処理性能が向上している。量子ゲート型コンピュータは人類にとってさまざまな恩恵をもたらすことが期待される。一方で、現在広く利用されている暗号技術の安全性にとっては脅威となりうる技術でもある。

量子ゲート型コンピュータ上で動作する量子アルゴリズムの 1 つにショア（Shor）のアルゴリズムがある（Shor [1994, 1997]）[6]。量子ゲート型コンピュータの処理性能が一定のレベルに達すると、このアルゴリズムを用いて、素因数分解問題や楕円曲線離散対数問題を現実的な時間で解読できることが知られて

---

[4] 量子アニーリング型コンピュータは、対象とする問題をある種の物理問題（スピングラス問題）に変換し、量子力学の性質を利用した装置を用いて行ったスピングラス問題の実験結果から、元の問題を求めるという量子コンピュータの実装方式である。

[5] 量子ビットは、外部から何らかの手段によって観測すると、重ね合わせ状態が失われ、従来のコンピュータのビットと同様に、0 と 1 のいずれかの状態に定まる。観測した際、どの状態に定まるかは、量子ビットに設定されている確率に依存する。

[6] 量子ゲート型コンピュータでは、量子ビットの重ね合わせ状態を維持したまま演算処理を行うとともに、処理結果の量子ビットを観測した際に、対象とする問題に対する最適な解を得られるように、量子ビットに設定されている確率を適切に操作する必要がある。量子アルゴリズムは、この操作を実現する仕組みである。

いる。そのため、公開鍵から秘密鍵を容易に導出できることとなり、安全性要件が満たされないこととなる。RSA 暗号や楕円曲線暗号で現在広く利用されている鍵サイズ（それぞれ、2,048 ビットと 256 ビット）に対応する素因数分解問題と楕円曲線離散対数問題は、現時点で実現している量子ゲート型コンピュータでは効率よくとくことはできない（Knight [2017]）。しかし、将来の量子ゲート型コンピュータの性能向上を見据え、高い処理能力を実現した量子ゲート型コンピュータでも容易に解読できない暗号の準備を進めておくことが重要である。また、公開鍵暗号だけでなくブロック暗号等の共通鍵暗号に対しても、量子ゲート型コンピュータを用いることにより、より効率的に攻撃を実行できるようになることも知られているため、量子ゲート型コンピュータの性能向上に伴う安全性低下についても留意する必要がある[7]。

ハ．量子ゲート型コンピュータに耐性を有する暗号

本稿では、量子ゲート型コンピュータでも容易に解読できない暗号を耐量子計算機暗号と呼ぶ。これまで、さまざまな種類の耐量子計算機暗号が提案されているが、これらは計算量型と情報理論型に大別される。

（イ）計算量型

計算量型に分類される耐量子計算機暗号は、量子ゲート型コンピュータを利用したとしても、現実的な計算時間で解くのは困難という数学的問題を利用している公開鍵暗号の総称である[8]。主な方式として、格子暗号、符号ベース暗号、多変数多項式暗号、同種写像暗号がある。

格子暗号は、高次元の格子（高次元空間上に規則正しく並んでいる点の集合）が得られたとき、ある条件を満たす格子上の点を探索する問題（格子問題）、あるいはその関連問題を利用する耐量子計算機暗号である。格子暗号は、耐量子計算機暗号としての性質を有するほか、データを暗号化したまま、さまざまな情報処理が可能な仕組みを実現できるなどの特長も有する（詳細は、次節以降を参照）。符号ベース暗号は、誤り訂正符号の復号問題の困難性を利用する耐量子計算機暗号である[9]。多変数多項式暗号は、多変数多項式による連立方程式が与えられたとき、その解を求める問題の困難性を利用する。同種写像暗号は、

---

[7] 量子コンピュータが共通鍵暗号の安全性に与える影響の詳細については、清藤・四方［2018］を参照されたい。なお、ブロック暗号とは、暗号化するデータを一定長のサイズのデータ（平文ブロック）に分割したうえで、各平文ブロックを暗号化鍵で変換する方式であり、その代表的な方式として、AES（Advanced Encryption Standard）が挙げられる。

[8] 耐量子計算機暗号の構成において広く利用されている数学的問題は NP 困難問題と呼ばれる。この問題は量子ゲート型コンピュータを利用しても現実的な時間で解けないと考えられている。

[9] 誤り訂正符号は、データを送信する際に通信路上で生じた誤り（エラー）を訂正するための技術である。

最近提案された計算量型の耐量子計算機暗号であり、2 つの楕円曲線が与えられたとき、これらの曲線間の対応関係（同種写像）を探索する問題の困難性を利用している[10]。

（ロ）情報理論型

情報理論型の耐量子計算機暗号は、攻撃者に対してデータの推測に必要な情報を与えない仕組みを実現することで、攻撃者が量子コンピュータを利用したとしても、解読が原理的に不可能であるという特長を有するものである（Shannon [1949]、Shikata [2015]等）。代表的な方式として、ワンタイムパッド暗号（Vernam [1926]）が挙げられる[11]。もっとも、この方式では送信者と受信者の間で予め暗号化と復号に用いる鍵を共有する必要があり、攻撃者が量子ゲート型コンピュータを利用可能な状況下において、どのように安全に共有するかが実用上の課題となる。この課題を解決する方法として、量子状態の特性を利用して鍵を共有する方式（量子鍵配送と呼ばれる）が提案されている（Bennett and Brassard [1984]等）。この方式は、量子ゲート型コンピュータに耐性を有することが知られている。

３．準同型暗号の概要

（１）高機能暗号

高機能暗号は、基本的な暗号機能（データの機密性の確保）に加えて高度な暗号機能を実現する技術であり、近年、公開鍵暗号にさまざまな高度な機能を持たせるための研究開発が盛んである。これまでに提案されている高機能暗号の主な方式とその機能を図表 4 にまとめる。

高機能暗号を構成するにあたっては、要素技術として楕円曲線上のペアリングや格子等の数学的構造が利用されることが多い[12]。特に、格子の構造は、高機能

---

[10] 同種写像とは、ある楕円曲線上の点と他の楕円曲線上の点同士を対応させる写像である。この写像は、一方の楕円曲線上の 2 つの点について、これらを加算した後で写像した（もう一方の楕円曲線上の）点と、これらを個別に写像した後、もう一方の楕円曲線上でこれらを加算した点が同一のものとなる特徴（準同型性）を有する。

[11] ワンタイムパッド暗号は、メッセージをビット列とみなし、同じ長さのランダムなビット列を秘密鍵としたうえで、これらのビットごとの排他的論理和をとることで暗号化を行う。暗号文を復号する際は、暗号化に用いた秘密鍵と暗号文の排他的論理和をとればよい。この暗号は、バーナム暗号とも呼ばれる。

[12] ペアリングは、楕円曲線上の 2 点から、四則演算が可能な要素の集合（体と呼ばれる）上の 1 つの要素へ対応させる写像であり、その実現手法として、ヴェイユ・ペアリング（Weil Pairing）やテイト・ペアリング（Tate Pairing）が挙げられる（詳細については、清藤・四方［2013］を参照されたい）。これらのペアリングは、もともと楕円曲線暗号への攻撃手法に用いられていたが、近年、高機能暗号等を構成する基礎技術として利用されている。また、格子の構造は暗号の安全性解析（國廣［2011］）で利用されることが多かったが、近年、耐量子計算機暗号等の構成にも

図表 4．主な高機能暗号

方式の名称		機能の概要		主な参考文献
検索可能暗号		データを暗号化したままキーワード検索を実行。		Boneh *et al.* [2004]等
準同型暗号	単演算型	データを暗号化したまま演算を実行。	加算または乗算のどちらか一方のみ可能。	Rivest, Shamir, and Adleman [1978]等
	サムホワット（Somewhat）型		加算と乗算（回数制限あり）が可能。	Boneh, Goh, and Nissim [2005]等
	完全型		加算と乗算が可能。	Gentry [2009]等
代理人再暗号化方式		データを暗号化したまま、復号権限を有するエンティティを変更。		Blaze, Bleumer, and Strauss [1998]等
属性ベース暗号	鍵ポリシー型	データを復号できるエンティティを制御。	属性に基づくアクセス構造を秘密鍵に組み込む。	Sahai and Waters [2005]等
	暗号文ポリシー型		属性に基づくアクセス構造を暗号文に組み込む。	Bethencourt, Sahai, and Waters [2007]等
鍵漏えい耐性暗号	フォワード・セキュア（Forward-Secure）型	秘密鍵を定期的に更新することによって、あるタイミングで秘密鍵が漏洩した際に、そのタイミングよりも前に生成された暗号文の安全性を保証。		Canetti, Halevi, and Katz [2007]等
	鍵隔離（Key-Insulated）型	秘密鍵を定期的に更新することによって、あるタイミングで秘密鍵が漏洩した際に、それ以外の秘密鍵で生成された暗号文の安全性を保証。		Dodis *et al.* [2002]等
	リーケージ・レジリエント（Leakage-Resilient）型	秘密鍵の一部が漏洩しても暗号文の安全性を保証。		Naor and Segev [2009]等
しきい値暗号		暗号文の復号権限を複数のエンティティに分割。一定数以上のエンティティの協力により暗号文を復号可能。		Desmedt [1994]等

暗号を実現可能な数学的構造を有しているだけでなく、量子ゲート型コンピュータを用いても現実的な時間で解くのが困難な数学的問題として利用できると考えられている。現在、NIST によって推進されている耐量子計算機暗号の米国政府標準暗号の選定過程においては、公開鍵暗号の候補として 49 方式が公表されている。それらのうち、格子問題に基づく方式は 23 方式であり、全体の約半分を占めている（National Institute of Standards and Technology [2018]）。このように、格子問題に基づく高機能暗号は、たとえ処理性能の高い量子ゲート型

積極的に利用されるようになった。

コンピュータが実現されたとしても、さまざまな情報処理におけるセキュリティ上の課題を解決しうる技術として注目されている。以下では、このような高機能暗号の中でも、格子問題に基づく準同型暗号（Homomorphic Encryption）に焦点を当てて解説する。準同型暗号は、その演算機能の有用性と汎用性から、将来の情報社会におけるクラウド計算、ビッグデータ分析、IoT 等、さまざまな情報処理におけるセキュリティ上の課題を解決しうる暗号技術として注目されている。

（２）準同型暗号

イ．モデル

準同型暗号は、データを暗号化したまま、さまざまな演算処理（四則演算や論理演算等）を実行できる機能を有しており、クラウド・サービス等への応用が検討されている。本稿では、一般的なユースケースを想定し、登録者、利用者、外部サーバの 3 つのエンティティから構成されるモデルを考える（図表 5）。利用者は、予め公開鍵と秘密鍵を生成し、公開鍵を公開するとともに秘密鍵を秘密に管理する。登録者はその公開鍵を用いてデータの暗号文を生成する。登録者は、この暗号文を外部サーバに送信し預託する。その後、利用者は、外部サーバに対して暗号化したデータへの演算処理を要求し、外部サーバは対応する処理を暗号文の状態のまま行う（このような処理を準同型演算処理と呼ぶ）[13]。そして、利用者は、その処理結果（暗号文）を外部サーバから受信し、秘密鍵を用いて復号する。

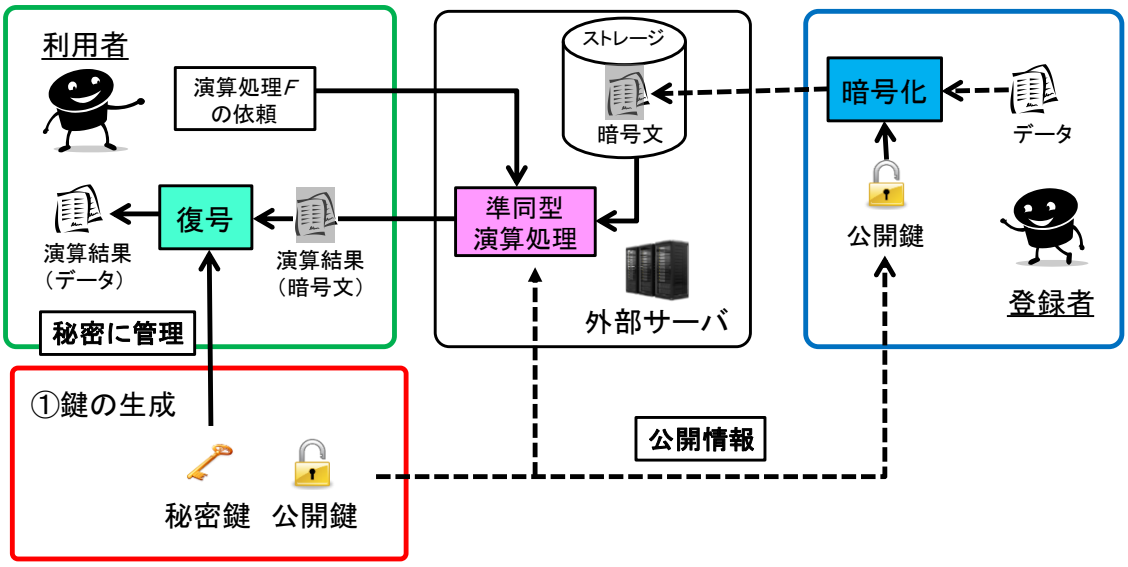
このような準同型暗号のモデルは、例えば、金融分野では、クラウド・サービス上で提供される営業支援システムにも適用できる（清藤・青野・四方［2017］）。営業支援システムは、顧客データを暗号化してクラウド・サービス事業者（外部サーバに相当）に預託し、金融機関の営業担当者（利用者や登録者に相当）が必要に応じて演算処理した結果を入手するというシステムである。

また、上記の準同型暗号のモデルは、2 節（1）で説明した公開鍵暗号のモデルを拡張したものとなっている。具体的には、登録者を送信者、利用者を受信者とみなし、登録者が利用者に直接暗号文を送信する処理フローを想定すると、公開鍵暗号と同じになる。従来の公開鍵暗号と準同型暗号の違いとして、準同型暗号には、公開鍵暗号のモデルで要求される処理に加えて、データの準同型演算処理の機能が加わっている。

---

[13] 外部サーバが利用者から秘密鍵を預託されていれば、外部サーバは暗号文から複数のデータを復号し、演算処理 F を適用することで所望のデータを生成し、その後、公開鍵で暗号化すれば準同型演算処理に相当する処理を実現することができる。この場合、外部サーバは暗号文を復号することができてしまう。しかし、準同型暗号では、外部サーバに秘密鍵を預託することなく、このような処理を実現している点が重要である。

図表 5. 準同型暗号のモデル



ロ．3 つの分類

準同型暗号は、実現できる準同型演算処理の種類により、単演算型、サムホワット（Somewhat）型、完全型に分類される。単演算型は、暗号化したデータ同士の単一演算（加算、乗算等の演算のうち 1 つだけ）を実現できる方式であり、1970 年代に提案されている。例えば、乗算のみ可能な方式としては RSA 暗号やエルガマル（ElGamal）暗号（ElGamal [1985]）、加算のみ可能な方式としてはパイリア（Paillier）暗号（Paillier [1999]）やゴールドワッサー＝ミカリ（Goldwasser-Micali）暗号（Goldwasser and Micali [1984]）が知られている。

その後、2005 年に、乗算の回数に制限があるものの、暗号化したデータに対して乗算と加算を組み合わせた演算処理を実行可能なサムホワット型が提案され（Boneh, Goh, and Nissim [2005]）、2009 年には、加算と乗算の回数に制限のない完全型が提案された（Gentry [2009]）。これらの方式を活用して、近年では、線形回帰計算、財務計算、データマイニング、ゲノム解析等への準同型暗号の適用も検討されている（詳細は 5 節を参照）[14]。また、サムホワット型や完全型は、検索可能暗号や代理人再暗号化方式等、他の高機能暗号に変換できることが知られており、この意味で汎用性を有している（Yasuda *et al.* [2013]、Boneh *et al.* [2004]、清藤・中野・四方［2014］等）[15]。

---

[14] 回帰とは、統計学において、従属変数（目的変数）と独立変数（説明変数）の間に定量的な関係を当てはめることである。特に、従属変数が各独立変数の 1 次式で表されるとき、線形回帰という。

[15] 他の高機能暗号への変換については、例えば、清藤・四方［2014］を参照されたい。

ハ．安全性要件と機能要件

準同型暗号においては、公開鍵を入手した攻撃者に対して、データの機密性を確保するために、2 節（1）で示した安全性要件が設定される。この安全性要件が満たされれば、外部サーバは秘密鍵を持っていないため、利用者は外部サーバに対してデータを安全に預託することができる。また、外部サーバのマルウェア感染等により暗号文が外部に漏えいしたとしても、安全性要件によりデータの内容が漏えいすることを防ぐことができる。

サムホワット型や完全型の準同型暗号を実装する際、当該暗号を安全に利用するための格子問題のパラメータ選択（例えば、格子の次元数等）に留意する必要がある。サムホワット型や完全型の準同型暗号を安全に利用できる格子問題のパラメータについては、これまでもさまざまな知見が示されている（清藤・青野・四方［2015］、Albrecht [2017]等）。格子問題に対しては、いくつかの攻撃アルゴリズムが既に提案されているが、今後も新たな攻撃法が提案される可能性があるため、パラメータ選択にかかる学会等での最新の報告に留意する必要がある。

準同型暗号における機能要件として、演算処理の結果となるデータ（暗号文）のサイズが、当該処理に使用した暗号文の個数や演算処理の回数等に比例して増加せず、演算前の暗号文とほぼ同じサイズであること（コンパクト性）を設定するケースが多い。コンパクト性は、外部サーバのストレージ容量や通信量の削減につながるため、実用上の観点からも重要な要件と考えられる。

４．耐量子計算機暗号に分類される準同型暗号に関する研究動向

本節では、クラウド・サービス等において多くの用途が期待される準同型暗号、特に完全型の準同型暗号（完全準同型暗号と呼ぶ）に注目し、その仕組みと研究動向について説明する。一般に、この方式は格子問題を安全性の根拠として利用されることが多く、その場合、耐量子計算機暗号に分類される。

（１）ブートストラッピング

完全準同型暗号は、サムホワット型の準同型暗号（サムホワット型準同型暗号と呼ぶ）にブートストラッピング（Bootstrapping）と呼ばれる手法を組み合わせることにより実現される。

サムホワット型準同型暗号の構成では、暗号文はメッセージに乱数およびノイズを足し合わせて生成されるケースが多い。ここでは、簡単に、暗号文 C が平文 M、乱数 R、ノイズ E によって構成される場合を考える。すなわち、

$$\text{暗号文 } C = \text{平文 } M + \text{乱数 } R + \text{ノイズ } E$$

とする。ただし、復号処理では、秘密鍵によって乱数 R は巧みに除去でき、ノ

イズ E はある一定範囲にある場合にだけ除去できると仮定する[16]。このとき、2つのメッセージM_1、M_2に対する暗号文をそれぞれ$C_1 = M_1 + R_1 + E_1$、$C_2 = M_2 + R_2 + E_2$とすると、加算に対応する準同型演算処理により、$C_1+C_2 = (M_1 + M_2) + (R_1 + R_2) + (E_1+E_2)$が得られ、ノイズに関係する項が$E_1+E_2$に膨らむことがわかる。また、乗算に対応する準同型演算処理$C_1 \times C_2 = (M_1 + R_1 + E_1)(M_2 + R_2 + E_2)$においても、ノイズに関係する項が$E_1E_2 + E_2(M_1 + R_1) + E_1(M_2 + R_2)$に膨らむことがわかる。以上のように、準同型演算処理を繰り返す度にノイズが処理結果（暗号文）に蓄積していくことがわかる（図表 6)。一般に、サムホワット型準同型暗号においては、ノイズが予め定められた範囲を超えてしまうと正しい復号結果を得られなくなる。そのため、この方式では準同型演算処理の回数に上限がある。

完全準同型暗号を実現するためには、いったん、サムホワット型準同型暗号を構成し、準同型演算の回数がその上限に近づく度に、データに蓄積したノイズを除去する必要がある。暗号文に蓄積したノイズを除去する手法として提案されたのがブートストラッピングである（Gentry [2009])。この手法は、外部サーバに秘密鍵を預託することなく、暗号文に蓄積したノイズを除去することができる。以下では、その手法について説明する。

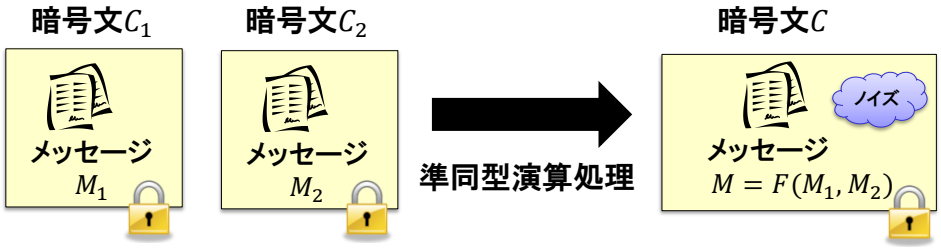
まず、利用者は公開鍵と秘密鍵のペアを 2 つ生成することとし、これらをそれぞれ(*PK*, *SK*)、(*PK*', *SK*')とする。そして、*PK* と *PK*'を公開する。登録者は、複数のデータを *PK* で暗号化し、外部サーバに送信する。外部サーバは利用者の要求により準同型演算処理を行うことで、(あるデータを演算処理した結果である）データ *M* の暗号文 *C* を計算したとする。その暗号文内のノイズを除去するため、以下のブートストラッピング処理を行う（図表 7)。

① 利用者は、秘密鍵 *SK* を *PK*'で暗号化したうえで、外部サーバに送信する。
② 外部サーバは、暗号文 *C* を *PK*'で改めて暗号化し新たな暗号文 *C*'を生成する。
③ 外部サーバは、上記①で得た暗号文と、上記②で得た暗号文 *C*'を入力とし、準同型演算処理 *F* として復号処理（図表 7 の DEC）に対応する処理を行う。

このとき、外部サーバが結果として得られるものは、データ *M* を *PK*'で暗号化した時に生ずる暗号文であることに注意する。上記の処理は、*PK*'により暗号化された状態のまま、秘密鍵 *SK* による *M* の復号処理を行っているためである。復号を行うとノイズは除去されるため、結果として *C* に蓄積されていたノイズが除去されたことになる。このように、暗号文内に一定量のノイズが蓄積する度に、上記のブートストラッピングを適用してノイズを除去することで、準同

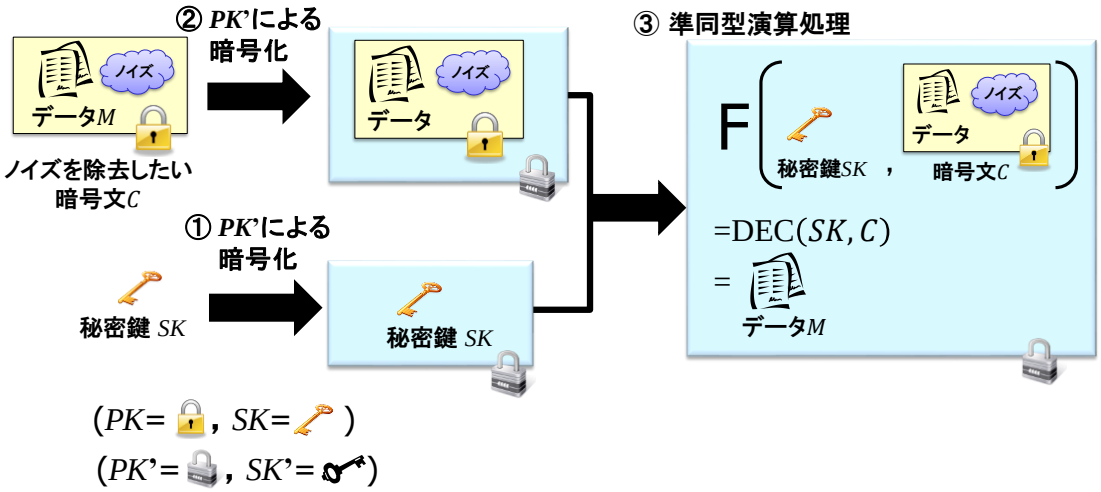
[16] 復号処理において、暗号文からノイズを除去できる仕組みについては、例えば、清藤・青野・四方［2015］等を参照されたい。

図表 6. 準同型演算処理 $M = F(M_1, M_2)$



（備考）F として加算$F(M_1, M_2) = M_1 + M_2$、乗算$F(M_1, M_2) = M_1 \times M_2$を行うことができる。

図表 7. ブートストラッピングのイメージ



型演算の回数を無制限にすることが可能になる。したがって、ブートストラッピングを何度も適用することにより、サムホワット型における準同型演算処理回数の制限を克服し、完全準同型暗号を構成できる。

しかしながら、上記の例では、1 つ目の鍵ペア(PK, SK) に加えて、上記のブートストラッピング処理を 1 回行うため、2 つ目の鍵ペア(PK', SK')を利用している。そのため、何度もブートストラッピングを行うためには複数の鍵ペアが必要になる。一般に、完全準同型暗号のモデルでは、 1 つの鍵ペア生成だけで何度も準同型演算を行うことができる機能を要求するため(図表 5 のモデル参照)、このままでは完全準同型暗号の実現には至らない。そこで、上記①～③において、$PK'=PK, SK'=SK$ としても安全性に問題がなければ、2 つ目の鍵ペア(PK', SK')を必要とせずに 1 つの鍵ペア(PK, SK)の生成だけでブートストラッピングを何度も行うことができるため、完全準同型暗号を実現できることになる。ただし、SK を PK で暗号化することになるため、暗号化するメッセージが鍵（この場合

は *SK*）に依存する場合にも安全性要件が満たされることが必要である[17]。

このように、ブートストラップを用いた完全準同型暗号の構成においては、準同型演算処理の回数が、利用するサムホワット型準同型暗号で設定されている上限を超えないようにすることや、攻撃者が *SK* の暗号文を得たとしても、安全性要件が満たされるように設計する必要がある。また、ブートストラッピングの処理には相応の時間を要することが課題として指摘されており、当該処理量を削減するための研究が行われている（Alperin-Sheriff and Peikert [2014]、Gentry, Sahai, and Waters [2013]等）。

（２）完全準同型暗号の拡張方式

一般的に、完全準同型暗号は、多様な演算機能の実現可能性や汎用性を有する一方、以下のような応用上の課題が指摘されている。

1 つ目の課題として、これまで説明した完全準同型暗号では、同じ公開鍵で暗号化されたデータ同士の準同型演算処理のみが可能であり、異なる公開鍵で暗号化されたデータ同士では準同型演算処理ができないことである（課題 1）。例えば、複数の利用者が存在し、各利用者が個別の公開鍵（と秘密鍵）を利用している状況において、外部サーバが暗号化されたデータに対する統計処理等を行う場合には、課題 1 を解決する必要がある。この課題を解決する手法として、異なる公開鍵で暗号したデータ同士の演算を可能とする完全準同型暗号の拡張方式が提案されており、マルチ・キー（Multi-Key）完全準同型暗号と呼ばれる（López-Alt, Tromer, and Vaikuntanathan [2012]、Clear and AcGoldrick [2015]、Mukherjee and Wichs [2016]、Peikert and Shiehian [2016]等）。もっとも、これらの方式については、利用できる公開鍵の個数や演算処理の回数に一定の制約があるほか、暗号文等のサイズが公開鍵の個数（すなわち、利用者の人数）の 2 乗に比例して急激に増加することが知られている。最近では、実用性を高めるという観点から、上記の拡張方式における課題を解決するための研究が進められている（Brakerski and Perlman [2016]等）。

2 つ目の課題として、暗号化されたデータに対する準同型演算処理の結果から、準同型演算処理にかかる情報が漏えいすることである（課題 2）。外部サーバ（クラウド・サービス等）が、自社独自の統計解析手法を競合する他社に知られたくない状況を想定する場合には、課題 2 を解決する必要がある。その手法として、４節（１）に挙げる準同型暗号の安全性要件に加えて、攻撃者が、公開鍵、任意のデータに対応する暗号文、および暗号文同士の演算処理の結果を得たとしても、演算処理の内容を知ることができないという安全性要件を満たす方式

[17] 一般に、メッセージが鍵に依存する場合の暗号化の安全性は、KDM 安全性（key dependent message security）と呼ばれる（Black, Rogaway, and Shrimpton [2002]）。

が提案されている（Gentry, Halevi, and Vaikuntanathan [2010]、Ostrovsky, Paskin-Cherniavsky, and Paskin-Cherniavsky [2014]、Bourse *et al.* [2016]等）。こうした完全準同型暗号は、サーキット・プライベート（Circuit-Private）完全準同型暗号といわれている。

また、最近では、上記の課題 1 と 2 を同時に解決する手法も提案されている（Chongchitmate and Ostrovsky [2017]）。この手法は、マルチ・キー完全準同型暗号とサーキット・プライベート完全準同型暗号を安全に組み合わせるというものである。もっとも、データ（公開鍵、秘密鍵、暗号文）のサイズが大きいほか、暗号処理に要する時間も増加することから、データのサイズ削減や、暗号処理の効率化が、今後の課題として残されている。

５．準同型暗号の実装、応用、標準化

（１）準同型暗号の実装を巡る動向

準同型暗号については、これまでいくつかのソフトウェア・ライブラリが公開されており、クラウド・サービス等において準同型暗号を利用する際には、活用できるようになっている。現在主流のソフトウェア・ライブラリとしては、HElib（Homomorphic Encryption library、GitHub, inc. [2017c]）、SEAL（Simple Encrypted Arithmetic Library、Microsoft [2017]）が挙げられる[18]。本稿執筆時点におけるこれらの特徴は以下のとおりである。

イ．HElib

IBM 社が無償で公表している準同型暗号のソフトウェア・ライブラリである。現時点で入手可能なバージョンでは、サムホワット型の実現方式の 1 つである BGV 方式（Brakerski, Gentry, and Vaikuntanathan [2012]）に基づいた暗号処理が実装されている。このライブラリでは、暗号文のサイズ削減や演算処理の効率を向上させるための実装上の工夫（Smart and Vercauteren [2014]等）が施されている。また、ブートストラッピングを行う処理も実装されており、完全準同型暗号として利用することも可能である。

ロ．SEAL

マイクロソフト社が無償で公表している準同型暗号のソフトウェア・ライブラリである。現時点で入手可能なバージョン 2.1 においては、サムホワット型の実現方式の 1 つである FV 方式（Fan and Vercauteren [2012]）に基づいた暗号処理が実装されている。このライブラリは外部のソフトウェア・ライブラリに依存することなく実行可能であり、また、安全に利用するためのパラメータの自動

[18] その他、FV-NFlib（GitHub, inc. [2017b]）や FHEW（GitHub, inc. [2017a]）等のソフトウェア・ライブラリも公開されている。

選択や暗号文に蓄積したノイズの程度を見積もるツール等も含まれている。

（２）準同型暗号の各分野への応用

近年、さまざまな分野において準同型暗号の応用に関する研究開発が活発化しているほか、既に一部のサービスにおいて実用化されている。以下では、主な応用事例について紹介する。

イ．線形回帰計算等の統計分析への応用

情報通信研究機構では、サムホワット型の準同型暗号を用いて、クラウドサーバ上での暗号化されたデータに対する統計処理を想定した実証実験を行い、100万件程度のデータに対する線形回帰計算を 30 分程度で処理できることを報告している（情報通信研究機構［2015］）。また、完全準同型暗号の応用として、データを暗号化した状態でロジスティック回帰分析を高速に行う手法を開発し、そのシミュレーションでは、サーバ上で 1 億件のデータを 30 分以内で分析可能と報告している（情報通信研究機構［2016］）[19]。さらに、Lu らは、完全準同型暗号を用いた線形回帰を含む統計分析手法を提案している（Lu, Kawasaki, and Sakuma [2017]）。その実証実験では、4,000 レコードについて 50 セルの分割表を 5 分で、また 6 次元 40,000 レコードの線形回帰計算を 15 分で計算可能と報告している。

ロ．化合物データベース検索技術への応用

産業技術総合研究所は、加算の準同型演算が可能な準同型暗号を用いて、化合物データベースにおいて類似した構造を有する化合物を実用的な速度で検索する技術を開発したと報告している（産業技術総合研究所［2011］）。この技術を利用した場合、登録者や利用者（創薬企業等）と外部サーバ（化合物データベースを提供する企業）は、互いに情報（創薬に用いられる化合物の情報）を開示することなく、情報共有が可能となるため、当該分野のイノベーションに資する技術と考えられる。

ハ．生体認証や検索技術への応用

富士通研究所は、サムホワット型準同型暗号を利用し、、生体情報（指紋や静脈データ等）を用いた生体認証やデータベース上のデータに対する検索処理への応用に関する報告を行っている。生体認証への応用事例においては、外部サーバに登録されている暗号化した静脈データ（2,048 ビットの特徴データ）と、利用者が認証時に提示した静脈データの照合処理を数ミリ秒で実行可能であるこ

[19] ロジスティック回帰分析とは、従属変数が 0 と 1 の間の値をとる場合に、定量的な関係としてロジスティック曲線を当てはめる回帰分析である。

とが実証されている（富士通研究所［2013］）。また、外部サーバ上に登録されている暗号化した文字列データ（16,000 文字程度）に対する検索処理を 1 秒以内で実行できることも実証されている（富士通研究所［2014］）。

二．遺伝子（ゲノム）データ解析への応用

ゲノムデータには、犯罪の鑑定、疾患の早期診断、個別医薬、出生前検査等、さまざまな分野におけるユースケースが想定される。しかし、ゲノムデータは非常に機微に触れる個人情報であるため、当該データの検索処理や統計解析等を行うシステムやサービスは、長期間にわたりセキュリティ（特に、ゲノムデータの機密性）を確保することが必須である。準同型暗号はゲノムデータを暗号化したまま検索処理や統計解析等を実現できるため、ゲノムデータ解析への応用に向けた研究開発が国内外で盛んに行われている（Sumner [2014]、GeneWatch [2014]、Ishimaki *et al.* [2016]、Lu, Yamada, and Sakuma [2015]）。また、実装に関する研究開発においては、安全なゲノム解析の性能を競うコンペティション（Secure Genome Analysis Competition）が、2015 年から iDASH Privacy and Security Workshop において、米国立衛生研究所（National Institutes of Health：NIH）支援の下、実施されている。

（３）標準化に関する動向

準同型暗号に関する国際標準等は規定されていないものの、米国の政府機関、企業や研究者を中心に準同型暗号の標準化を推進する活動が進められている。2017 年 7 月にはマイクロソフト社において、ワークショップが開催され、その議論をもとに作成された準同型暗号に関するドキュメントが公開されている（Homomorphic Encryption Standardization [2017]）。当該ドキュメントの中では、主に、BGV 方式（Brakerski, Gentry, and Vaikuntanathan [2012]）、B/FV 方式（Brakerski [2012]、Fan and Vercauteren [2012]）が推奨されている。準同型暗号の応用や実装に関する研究開発や、標準化を推進する活動の活発化に伴い、今後は、準同型暗号（特に、完全準同型暗号やサムホワット型準同型暗号）の国際標準の策定に向けた動きが進展すると考えられる。

６．おわりに

米国連邦政府は、2022 年頃までに耐量子計算機暗号の政府調達基準を策定し、現在使用している公開鍵暗号を 2026 年頃までに耐量子計算機暗号へ移行する計画を示している（National Institute of Standards and Technology [2018]）。 また、欧州連合では、耐量子計算機暗号の標準化に向けたロードマップの検討を開始している（European Telecommunications Standards Institute [2017]）。わが国においても、CRYPTREC（Cryptography Research and Evaluation Committees）等において

研究動向の調査が開始されており（情報通信研究機構・情報処理推進機構［2017］）、今後、政府機関等を中心に量子コンピュータへの対策に関する検討が進められると考えられる。

上記のような耐量子計算機暗号への動きとともに、近年、クラウド計算、ビッグデータ分析、IoT 等、さまざまな情報処理におけるセキュリティ上の課題を解決しうる高機能な暗号技術へのニーズが高まっている。本稿では、このような高機能暗号の中でも、その演算機能の有用性と汎用性から、格子問題に基づく準同型暗号に焦点を当てて解説した。本稿では、格子問題に基づく準同型暗号の理論研究だけでなく、実装、応用、標準化の動向についても触れた。現在、完全準同型暗号やサムホワット型準同型暗号は、統計分析やゲノム解析をはじめととする諸分野において、実装・応用が進んでいる。金融分野においても、安全な金融サービスの提供の観点から広く利活用されることを期待したい。

以　上

参考文献

金融情報システムセンター、「金融機関等コンピュータ・システムの安全対策基準・解説書（第 8 版追補改訂）」、2015 年

國廣昇、「格子理論を用いた暗号解読の最近の研究動向」、『Fundamentals Review』、Vol.5(1)、電子情報通信学会、2011 年、42-55 頁

産業技術総合研究所、「秘密計算による化合物データベースの検索技術」、2011 年

情報通信研究機構、「暗号化したままデータを分類できるビッグデータ向け解析技術を開発」、2016 年

――――、「暗号化状態でセキュリティレベルの更新と演算の両方ができる準同型暗号方式を開発」、2015 年

――――・情報処理推進機構、「CRYPTREC シンポジウム 2017 配付資料」、2017 年

清藤武暢・青野良範・四方順司、「公開鍵暗号型の高機能暗号を巡る研究動向」、日本銀行金融研究所ディスカッション・ペーパー・シリーズ、No. 2017-J-8、日本銀行金融研究所、2017 年

――――・――――・――――、「量子コンピュータの解読に耐えうる暗号アルゴリズム『格子暗号』の最新動向」、『金融研究』、第 34 巻第 4 号、日本銀行金融研究所、2015 年、135～170 頁

――――・四方順司、「公開鍵暗号を巡る新しい動き: RSA から楕円曲線暗号へ」、『金融研究』、第 32 巻第 3 号、日本銀行金融研究所、2013 年、17～50 頁

――――・――――、「高機能暗号を活用した情報漏えい対策『暗号化状態処理技術』の最新動向」、『金融研究』、第 33 巻第 4 号、日本銀行金融研究所、2014 年、97～132 頁

――――・――――、「量子コンピュータが共通鍵暗号の安全性に与える影響」、日本銀行金融研究所ディスカッション・ペーパー・シリーズ、No. 2018-J-2、日本銀行金融研究所、2018 年

――――・中野倫太郎・四方順司、「ID ベース暗号による代理人再暗号化方式の一般的構成法」、『2014 年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2014 年

富士通研究所、「世界初！暗号化したまま統計計算や生体認証などを可能にする準同型暗号の高速化技術を開発」、2013 年

――――、「暗号化したまま検索が可能な秘匿検索技術を開発」、2014 年

Albrecht, Martin R., “On Dual Lattice Attacks against Small-secret LWE and Parameter Choices in HElib and SEAL,” *Proceedings of EUROCRYPT 2017*, LNCS 10211, Springer-Verlag, 2017, pp.103-129.

American National Standards Institute, “X9.62: Public Key Cryptography forthe Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),” 2005.

Alperin-Scheriff, Jacob, and Chris Peikert, “Faster Bootstrapping with Polynomial Error,” *Proceedings of CRYPTO 2014*, Vol.1, LNCS 8616, Springer-Verlag, 2014, pp.297-314.

Bennett, Charles H., and Gilles Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, 1984, pp.175-179.

Bethencourt, John, Amit Sahai, and Brent Waters, “Ciphertext-Policy Attribute-Based Encryption,” *Proceedings of IEEE Symposium on Security and Privacy (SP)*, 2007, pp. 321-334.

Black, John, Phillip Rogaway, and Thomas Shrimpton, “Encryption-Scheme Security in the Presence of Key-Dependent Messages,” *Proceedings of Selected Areas in Cryptography (SAC) 2002*, LNCS 2595, Springer-Verlag, 2002, pp.62-75.

Blaze, Matt, Gerrit Bleumer, and Martin Strauss, “Divertible Protocol and Atomic Proxy Cryptography,” *Proceedings of EUROCRYPT 1998*, LNCS 1403, Springer-Verlag, 1998, pp.127-144.

Boneh, Dan, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano, “Public Key Encryption with Keyword Search,” *Proceedings of EUROCRYPT 2004*, LNCS 3027, Springer-Verlag, 2004, pp.506-522.

———, Eu-Jin Goh, and Kobbi Nissim, “Evaluating 2-DNF Formulas on Ciphertexts,” *Proceedings of Theory of Cryptography Conference (TCC) 2005*, LNCS 3378, Springer-Verlag, 2005, pp.535-554.

Bourse, Florian, Fafaël Del Pino, Michele Minelli, and Hoeteck Wee, “FHE Circuit Privacy Almost for Free,” *Proceedings of CRYPTO 2016*, LNCS 7414, Springer-Verlag, 2012, pp.868-886.

Brakerski, Zvika, “Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP,” *Proceedings of CRYPTO 2012*, LNCS 7417, Springer-Verlag, 2012, pp.868-886.

————, Craig Gentry, and Vinod Vaikuntanathan, “(Leveled) Fully Homomorphic Encryption without Bootstrapping,” *Proceedings of Innovations in Theoretical Computer Science Conference (ITCS) 2012*, Association for Computing Machinery, 2012, pp. 309-325.

————, and Renen Perlman, “Lattice-Based Fully Dynamic Multi-key FHE with

Short Ciphertexts," *Proceedings of CRYPTO 2016*, Vol. 1, LNCS 9814, Springer-Verlag, 2016, pp.190-213.

Canetti, Ran, Shai Halevi, and Jonathan Katz, "A Forward-secure Public-key Encryption Scheme," *Journal of Cryptology*, 20 (3), 2007, pp. 265-294.

Chongchitmate, Wutichai, and Rafail Ostrovsky, "Circuit-Private Multi-key FHE," *Proceedings of International Conference on Practice and Theory in Public-Key Cryptography (PKC) 2017*, Vol. 2, LNCS 10174, Springer-Verlag, 2017, pp.241-270.

Clear, Michael, and Ciarán McGoldrick, "Multi-Identity and Multi-Key Leveled FHE from Learning with Errors," *Proceedings of CRYPTO 2015*, Vol.2, LNCS 9216, Springer-Verlag, 2015, pp.630-656.

Desmedt, Yvo, "Threshold Cryptography," *Transactions on Emerging Telecommunications Technologies*, Vol. 5(4), 1994, pp. 449–458.

Dierks, Tim, and Eric Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," Request for Comments, no.5246, 2008.

Dodis, Yevgeniy, Jonathan Katz, Shouhuai Xu, and Moti Yung, "Key-Insulated Public Key Cryptosystems," *Proceedings of EUROCRYPT 2002*, LNCS 2332, Springer-Verlag, 2002, pp. 65-82,.

ElGamal, Taher, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, Vol.31, no.4, 1985, pp.469–472.

European Telecommunications Standards Institute, "ETSI TC Cyber Working Group for Quantum Safe Cryptography," *ETSI IQC Quantum Safe Workshop*, 2017.

Fan, Junfeng, and Frederik Vercauteren, "Somewhat Practical Fully Homomorphic Encryption," *IACR ePrint Archive,* 2012/144, 2012.

GeneWatch, "A Cipher for Your Genome," *Council for Responsible Genetics (CRG)*, 2014.

Gentry, Craig, "Fully Homomorphic Encryption Using Ideal Lattices," *Proceedings of Annual ACM Symposium on Theory of Computing* (*STOC) 2009*, Association for Computing Machinery, 2009, pp.169-178

————, Shai Halevi, and Vinod Vaikuntanathan, "i-Hop Homomorphic Encryption and Rerandomizable Yao Circuits," *Proceedings of CRYPTO 2010*, LNCS 6223, Springer-Verlag, 2010, pp.155-172.

————, Amit Sahai, and Brent Waters, "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based," *Proceedings of CRYPTO 2013*, Vol. 1, LNCS 8043, Springer-Verlag, 2013, pp.75-92.

GitHub, inc., “FHEW,” 2017a.

————, “FV-NFLlib,” 2017b.

————, “HElib,” 2017c.

Goldwasser, Shafi, and Silvio Micali, “Probabilistic Encryption,” *Journal of Computer and System Sciences*, 28 (2), 1984, pp.270–299.

Homomorphic Encryption Standardization, “Security of Homomorphic Encryption, ” White Paper, 2017.

International Organization for Standardization, “ISO 11568-4: Banking-Key Management (Retail) –Part 4: Key Management Techniques using Public Key Cryptography,” 2007.

Ishimaki, Yu, Kana Shimizu, Koji Nuida, and Hayato Yamana, “Privacy-Preserving String Search for Genome Sequences Using Fully Homomorphic Encryption,” *Proceedings of IEEE Symposium on Security and Privacy (SP)*, 2016.

Knight, Will, “IBM Raises the Bar with a 50-Qubit Quantum Computer,” *MIT Technology Review*, 2017.

Koblitz, Neal, “Elliptic Curve Cryptosystems,” *Mathematics of Computation*, Vol.48, 1987, pp.203-209.

López-Alt, Adriana, Eran Tromer, and Vinod Vaikuntanathan, “On-the-fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption,” *Proceedings of Annual ACM Symposium on Theory of Computing (STOC) 2012*, Association for Computing Machinery, 2012, pp.1219-1234.

Lu, Wen-jie, Shoei Kawasaki, and Jun Sakuma, “Using Fully Homomorphic Encryption for Statistical Analysis of Categorical, Ordinal and Numerical Data,” *Network and Distributed System Security Symposium (NDSS) 2017*, online proceedings.

————————, Yoshiji Yamada, and Jun Sakuma, “Privacy-Preserving Genome-Wide Association Studies on Cloud Environment Using Fully Homomorphic Encryption,” *BMC Medical Informatics and Decision Making*, Vol. 15, No.s5, 2015.

Microsoft, “Simple Encrypted Arithmetic Library,” 2017.

Miller, Victor S., “Use of Elliptic Curves in Cryptography,” *Proceedings of CRYPTO 1985*, LNCS 218, Springer-Varlag, 1985, pp.417-426.

Mukherjee, Pratyay, and Daniel Wichs, “Two Round Multiparty Computation via Multi-key FHE,” *Proceedings of EUROCRYPT 2016*, vol. 2, LNCS 9666, Springer-Verlag, 2016, pp.735-763.

Naor, Moni, and Gil Segev, “Public-Key Cryptosystems Resilient to Key Leakage,” *Proceedings of CRYPTO 2009*, LNCS 5677, Springer-Verlag, 2009, pp.18-35.

National Institute of Standards and Technology, “Post-Quantum Cryptography,” 2018.

Ostrovsky, Rafail, Anat Paskin-Cherniavsky, and Beni Paskin-Cherniavsky, “Maliciously Circuit-Private FHE,” *Proceedings of CRYPTO 2014*, vol. 1, LNCS 8616, Springer-Verlag, 2014, pp.536-553.

Paillier, Pascal, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” *Proceedings of EUROCRYPT 1999*, Springer-Verlag, 1999, pp.223-238.

Peikert, Chris, and Sina Shiehian, “Multi-Key FHE from LWE, Revisited,” *Proceedings of International Conference on Theory of Cryptography (TCC) 2016*, Vol.2, LNCS 9986, Springer-Verlag, 2016, pp.217-238.

Rivest, Ronald, Adi Shamir, and Leonard Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” *Communications of the ACM*, 21(2), 1978, pp.120-126.

Sahai, Amit, and Brent Waters, “Fuzzy Identity-Based Encryption,” *Proceedings of EUROCRYPT 2005*, LNCS 3494, Springer-Varlag, 2005, pp 457-473.

Sumner, Thomas, “How to Hide Your Genome,” *Science*, American Association for the Advancement of Science (AAAS), 2014.

Shannon, Claude, “Communication Theory of Secrecy Systems,” *Bell System Technical Journal*, 28(4), 1949, pp.656-715.

Shikata, Junji, “Trends and Development of Information-Theoretic Cryptography,” *IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E98-A, No.1, The Institute of Electronics, Information and Communication Engineers, 2015, pp. 16-25.

Shor, Peter, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” *Proceedings of Foundations of Computer Science (FOCS) 1994*, 1994, pp.124-134.

———, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing*, 26(5), 1997, pp.1484-1509.

Smart, Nigel P., and Frederik Vercauteren, “Fully Homomorphic SIMD Operations,” *Designs, Codes and Cryptography*, Vol.71, No.1, 2014, pp.57-81.

Vernam, Gilbert S., “Cipher Printing Telegraph Systems for Secret Wire and Radion Telegraphic Communications,” *Journal of American Institute of Electrical Engineers*, Vol.45, 1926, pp.295-301.

Yasuda, Masaya, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, and Takeshi Koshiba, “Secure Pattern Matching Using Somewhat Homomorphic Encryption,”

Proceedings of ACM workshop on Cloud computing security workshop (CCSW) 2013, 2013, pp.65-76.