京都大学	博士（情報学）	氏名	Sun Chao
論文題目	Constructive and Destructive Aspects of Euclidean Lattices in Cryptography （暗号におけるユークリッド格子の構成および解析に関する研究）		

（論文内容の要旨）

暗号学の研究は、構成（構築的な側面）と解読（解析的な側面）という二つのテーマに大きく分類できる。構成は、効率的で安全な通信方式を確立することを目的としている。一方、暗号解読の目標は、提案されている方式の欠陥を見つけ出し、機密情報を漏洩しうる技術を除外することである。

現在広く使用されている公開鍵暗号技術（RSA、DSA、ECDSA など）は、素因数分解問題または離散対数問題の困難性に基づいている。しかし、これらの問題は Shor アルゴリズムを用いて量子コンピュータで効率的に解くことが可能である。Shor アルゴリズムを実行し実際の暗号技術が破れるほど性能の良い量子コンピュータ未だに実現されていないにもかかわらず、量子計算技術が早く進歩しており、RSA や ECDSA が破られるのは時間の問題に過ぎないとの見解もある。そのため、暗号学者は量子コンピュータの潜在的な脅威に備えて、新しい暗号方式（いわゆる耐量子暗号）の設計に着手している。耐量子暗号の安全性の根拠は、効率的な量子アルゴリズムが知られていない様々な計算問題の困難性を基にしている。そのうち、ユークリッド格子に関する問題に基づく「格子ベース暗号」が特に注目されている。複数のメリットが挙げられる。アルゴリズム的な観点からは、格子ベース暗号はベクトルや行列に対する線形演算からなるので、シンプルで実装しやすい。セキュリティ面では、格子問題を対象に「最悪時から平均時計算への帰着」などが示されており、確固とした安全性の基盤となる。さらに、格子暗号は、完全準同型暗号をはじめとする、従来暗号技術や他の耐量子暗号では実現できない斬新的な新暗号技術を可能とする。

本論文では、格子暗号を巡り、構成と解読との両側面に関する研究を紹介している。バイナリエラーLWE の安全性、ECDSA に対する格子攻撃、および安全で効率的な格子ベース電子署名の構成という、三つの課題における研究結果について述べたものである。

本論文は全五章で構成されている。

第一章では、暗号学の歴史および 20 年ほどにわたる格子暗号の構成・解読の両側面の発展について述べられている。また、三つの研究成果と、これらの社会情報学への貢献を順次に概説している。

第二章では「バイナリエラーLWE」という計算問題の安全性について分析されている。格子暗号の代表的な計算問題である LWE 問題に於いては、エラーベクトルというものがあるが、さまざまな場面ではそれぞれのエラーベクトルの分布が使われている。とりわけ、０か１かの成分のバイナリーエラーベクトルの重要な特集例が検討されており、対応するバイナリエラーLWE 問題が IoT デバイス用の暗号方式の安全性根拠等として注目されている。この問題を対象に、準指数関数時間の求解アルゴリズム（グレブナー基底計算を簡約し特化したアルゴリズム）を

提案し、サンプル数により計算量を如何に変動するか評価する。これを基に、バイナリエラーLWE 問題の困難性を厳密に評価することができ、IoT デバイス用の暗号方式のパラメター設定を再検討できる。さらに、分析を非一様ランダムなバイナリーエラーベクトルにも拡張し、安全性を証明できるパラメター範囲と、効率的に破れるパラメター範囲を明らかにする。従って、本章で述べられている結果は、暗号分野の構成と解読の両側面にまで及ぶ。

第三章では、解読側面に焦点を当てて、(EC)DSA という幅広く使用されている電子署名方式を対象に、既存研究で知られている格子攻撃を改良する。ユークリッド格子が暗号分野においてはじめて導入されたのは公開鍵暗号の解読アルゴリズムを提案するであり、歴代の著名な攻撃の多くが、格子簡約アルゴリズムに基づいている。その一つは Howgrave-Graham と Smart の乱数の偏った (EC)DSA への攻撃である。(EC)DSA 署名生成において使われている乱数の一部のビットがゼロなどの偏りが生じる場合、秘密鍵を回復する格子簡約アルゴリズムに基づいた重要な攻撃のことである。この攻撃が考案されたのは 2001 年であったが、その時は実際の鍵回復を達成するために必要な偏りビット数が高く、やや理論的な脅威に過ぎなかった。しかし、それ以来さまざまな改良が提案されてきて、必要なビット数がどんどん少なくなってきた。本章で述べられている研究は、このビット数をさらに少なくする新たな手法であり、Howgrave-Graham と Smart 攻撃の最先端の改良となる。この進歩の背後にある基本的なアイデアは、回復しようとしている秘密鍵に対する数ビット分の全数検索である。このような検索を行うと、格子攻撃により回復しないといけない秘密情報のサイズがその分少なくなり、格子簡約の計算時間が減るわけである。なお、とあるパラメター範囲においては、格子簡約の高速化は数ビットの全数検索のコストを上回るので、トータルで攻撃の大幅な改良が得られると示されている。

第四章では、構成側面に着目して、格子ベースハッシュ＆サイン署名の設計に関する研究を紹介する。米 NIST が策定した標準化プロセスにおいて、三つの署名方式が選定されたが、そのうち最も性能が高く最もコンパクトな候補方式は格子ベースハッシュ＆サイン署名 Falcon のことである。しかし、Falcon の署名生成アルゴリズムが非常に複雑で、正確で安全に実装するのは困難であり、物理攻撃などから保護するのは難しい。そのため、比較的にシンプルな後継方式 Mitaka が提案されてきて、Falcon と同じぐらいのスピードと鍵・署名サイズを達成しながら著しく実装しやすい。しかし、Falcon に比べて安全性水準は 20 ビットほど低いため、同程度のパラメターにしてしまうと、NIST が定める水準には及ばない。本章では、Mitaka の鍵生成アルゴリズムの中核となる「NTRU 落とし戸生成」のために全く新しい手法を提案することにより、Mitaka のすべての長所を維持しながら Falcon と同程度の安全性水準を達成する方法を紹介する。なお、新しい鍵生成アルゴリズムは Mitaka よりもシンプルで遥かに高速である。結果として、Falcon と Mitaka のそれぞれの利点をすべて兼ね備えた新署名方式を構成することができ、多くの場面で利用されうると考えられる。

第五章は、上記三つの課題に対する結果をまとめて、それぞれの貢献を振り返る。

（続紙 ２ ）

（論文審査の結果の要旨）

本論文の主題である暗号技術は情報化社会において安全なデータ流通を可能にする基盤技術であり、銀行取引・通信販売・インスタントメッセージ・マイナンバーカードなど様々な情報システムの安全性を保証している。しかし、現在それらのシステムにおいて使われている公開鍵暗号や電子署名は「素因数分解」もしくは「離散対数問題」という数学的問題の困難性に基づいており、大型量子計算機が実現されてしまえばShorアルゴリズムにより効率的に破られてしまうことが知られている。なお、ここ数年は大幅な量子計算の進展があったため、その脅威はますます差し迫っている。そのため、量子計算機に対しても安全な暗号技術である「耐量子暗号」の開発が情報化社会の維持発展に不可欠である。それに向けて幾つかの有力なアプローチが提案されているが、そのうち一番注目されているのはユークリッド格子に関する計算問題の困難性に基づく「格子ベース暗号」であり、本論文の研究対象となる。NIST（米国立標準技術研究所）が進める耐量子暗号標準化プロセスにおいて、四つの方式が選定されてきて将来的に幅広く使われるようになる見込みであるが、そのうち三つも格子ベース方式となっている。従って、格子ベース暗号の安全性評価や効率性向上などが社会的に意義のある研究課題であると言える。さらに、ユークリッド格子は現在普及している従来暗号技術に対する攻撃においても使われており、格子問題の研究は現時点での情報通信の安全性にも直結している。本論文第一章では格子ベース暗号の重要性が社会的・技術的観点で述べられており、研究動機が明確に示されている。

本論文では、暗号学におけるユークリッド格子に関する三つの課題に取り組んでいる。まず第二章では、一部の格子ベース暗号方式（とりわけIoTデバイスなど、実社会でますます広まってきている組込みシステムのための軽量耐量子暗号方式）の安全性根拠となる「バイナリエラーLWE問題」の困難性について述べている。既存のArora-Ge攻撃を一般化した、任意のサンプル数に対する準指数関数時間の求解アルゴリズムを紹介し、その計算コストが評価している。それを基に、軽量耐量子暗号方式のパラメター設定を再検討している。さらに、分析を非一様ランダムなバイナリーエラーLWEにも拡張し、安全性を証明できるパラメター範囲と、効率的に破れるパラメター範囲を解明している。実世界用の次世代暗号方式に対して新たな知見を与える結果である。

第三章では、従来暗号技術の(EC)DSA署名を対象としたユークリッド格子を用いる乱数偏り攻撃について論じている。(EC)DSA署名生成における乱数の一部のビットが漏洩してしまうと、格子簡約アルゴリズムを用いて多くの署名から秘密鍵を回復するが可能であるという脆弱性が20年以上前に指摘された。しかし、当時の必要な漏洩ビット数が高く、サイドチャネル分析などにより実際のほとんどの場面に生じうる漏洩を上回っていた。それ以来、さまざまな改良が提案されてきたが、本章では秘密鍵に対する数ビット分の全数検索という新たな手法を導入し、これまでの最小の漏洩ビット数に対する格子簡約攻撃を達成している。その漏洩ビット数が実際の暗号ライブラリーに確認されたこともあるため、サイドチャネル対策などの重要性を強調する結果であると認められる。

第四章では、ハッシュ＆サイン型格子ベース署名方式の安全性と効率性を検討している。NIST標準化プロセスにおいて一番高性能でコンパクトな選定署名方式はハッシュ＆サイン型格子ベース署名の一例であるFalconとなるが、署名生成アルゴリズムが複雑で非常に実装しにくいとされている。一方、Falconの簡素化として提案された後継方式Mitakaはシンプルな署名生成アルゴリズムを持っており、同程度の性能を持つが、安全性の面では劣っている。本章ではMitakaのための全く新しい鍵

生成アルゴリズムを提案し、安全性の高い署名鍵を生成する手法を導入し、Mitakaの実装しやすい署名生成アルゴリズムを維持しながらFalconと同じ安全性水準を達成している。この結果はより多くの場面で使用されうる高性能耐量子署名方式の設計を可能とし、理論と実用の両面で意義のある結果である。

以上、本研究の結果は格子ベース暗号の具体的な安全性・効率性向上から格子を用いた従来暗号方式の安全性評価概念まで広範囲の課題に対する研究を進展させ、格子ベース暗号の実現に貢献するものであると言える。

以上により、本論文は博士（情報学）の学位論文として価値あるものと認める。また、令和５年２月１７日に実施した論文内容とそれに関連した口頭試問の結果、合格と認めた。なお、本論文の令和６年３月２３日以降のインターネットでの全文公表についても支障がないことを確認した。

要旨公開可能日：　2023　年　4 月　1 日以降