様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 ２３ 日現在

機関番号：３５３０２
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１９７

研究課題名（和文）耐量子暗号への非可換構造の応用と解析

研究課題名（英文）Application and analysis of non-commutative structure to post-quantum cryptography

研究代表者
安田　貴徳（Yasuda, Takanori）

岡山理科大学・工学部・准教授

研究者番号：００４６４６０２

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：量子コンピュータに耐性を持つ暗号を構成するための新しい数学問題として、制約付きMP問題を導入した。これまで頻繁に利用されてきた数学問題である通常のMP問題より、多変数多項式公開鍵暗号の暗号方式の構成が容易であり、実際に本研究課題で２つの暗号方式を開発した。制約付きMP問題を用いると非可換構造を持たせることができ、これらの方式は高い安全性を持つ。また、効率的な暗号化・復号化アルゴリズムを持つため、実用的な暗号方式となる。

研究成果の学術的意義や社会的意義
提案した暗号方式が、量子コンピュータに耐性を持つ公開鍵暗号の１つとして標準化され、未来の暗号基盤を支える重要な要素として通信などの安全性を守っていく可能性がある。

研究成果の概要（英文）：As a new mathematical problem which is resistant to quantum computer, I introduced the constrained MP problem. Compared with the mathematical problem, the usual MP problem which was often used, the constrained MP problem is easy to provide with encryption schemes on the multivariate public-key cryptosystems. In fact, I developed two encryption schemes using it. Such encryption scheme is possible to have non-commutative structure, therefore, it is highly secure. Moreover, since it has efficient encryption and decryption algorithm, it becomes practical.

研究分野：暗号理論

キーワード：耐量子暗号　多変数多項式公開鍵暗号　格子ベース暗号　公開鍵暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) 1994 年に発表された Shor のアルゴリズムにより、現在の公開鍵暗号基盤の柱となっている RSA 暗号と楕円曲線暗号が量子コンピュータの性能を仮定すると理論上多項式時間で解読可能であることが証明された。この発表を機に徐々に量子コンピュータに耐性を持つ公開鍵暗号（耐量子暗号）の研究が盛んになり始めた。

(2) アメリカの NIST（米国標準技術研究所）が 2016 年に耐量子暗号の国際会議 PQCrypto2016 において耐量子暗号の標準暗号を公募すると発表した。実際に公募が始まり、応募された暗号の選定作業が行われており、現在 Round 2 まで進んでいる。

２．研究の目的

(1) 耐量子暗号にはいくつか候補があるが、安全性の解析が不十分であり、また、暗号の種類（暗号方式、署名方式、鍵配送）によっては設計自体が難しいものも存在する。暗号設計では多項式環のような可換な代数構造が良く利用される。それ自身が脆弱な暗号であっても、可換構造を非可換構造に変えた場合、安全性の強度が増し、量子コンピュータを用いた攻撃に耐性を持つ暗号に生まれ変わる可能性がある。本研究では、数学的非可換構造を用いた耐量子暗号の設計の可能性について調べることを目的とした。

(2) 耐量子暗号には鍵長問題などいくつかの課題が指摘されている。一方、非可換構造の多くは、少ない情報で複雑な構造を表せるという特性を持っている。それを利用し、耐量子暗号の持つ従来課題の解決の可能性について調べることを目的とした。

３．研究の方法

(1) まずは，様々な非可換環を調べ、その実現方法を明らかにする。その後、多項式環など可換代数構造が用いられている暗号に対し、その可換構造部分を非可換環に置き換えて暗号として成り立つかどうかを検証する。暗号として成り立つものに対し、適切な調整を行うことで暗号設計を確定させ、新方式とする。その後、理論的、実験的に安全性解析を行う。

(2) 非可換環の実現方法を調べることで、必要なサイズの非可換環を実現するための情報量を知ることができる。これを耐量子暗号共通の課題である鍵長問題の解決に利用する。少ない情報で複雑な構造を表せる非可換環ほど、鍵長問題を解決しやすくなる。また、非可換環を用いて暗号方式、署名方式、鍵配送や様々な機能を持つ暗号の開発を行う。

４．研究成果

(1) 多変数公開鍵暗号の新しい数学問題の導入

多変数公開鍵暗号は多変数多項式系を秘密鍵や公開鍵として利用しており、多くの場合、その主な安全性は多変数多項式方程式の求解の困難性に基づいている。これは MP 問題と呼ばれている。本研究課題において、この MP 問題を一般化（ある意味では制限化）し、制約付き MP 問題という新しい数学問題を導入した．制約付き MP 問題では、通常の MP 問題の定義域を制限し、その定義域内にある解の求解問題を考える。制限定義域を全体とすれば通常の MP 問題が得られることから一般化であるといえる。この制約付き MP 問題の求解の困難性を暗号方式の開発に利用した。この制約付き MP 問題を導入した大きな理由は、多変数公開鍵暗号の従来課題の一つである「暗号方式の開発」である。多変数公開鍵暗号は署名方式には強く、Rainbow や HFEv-といった優れた署名方式が既に提案されている。一方で、多変数公開鍵暗号の暗号方式はこれまでにたくさん提案されてきたもののほとんどが解読されている。理由は、単射でかつ秘密鍵保持者だけが知ることのできる抜け穴（トラップドア）を持つ多変数多項式写像（かつ、MP 問題の解読が困難なもの）を構成することが難しいからである。これまで暗号方式の構成に主に利用されてきたのは巨大な有限体上の１変数多項式に Weil 制限を施すことで多変数多項式に見せるという方法であった。ところが、この方法は１変数多項式が持つ可換性を利用することにより解読される。本研究課題が非可換性にこだわっている理由の一つがこれである。こういったことから、通常の MP 問題を利用した暗号方式の開発は停滞状態にあり、安全性保証に用いる新しい数学問題が必要であった。そこで新しい数学問題として制約付き MP 問題を考案した。制約付き MP 問題の場合、1 変数多項式を利用しない暗号方式の開発が可能になる。実際に、制約付き MP 問題を安全性仮定とする暗号方式を 2 種類開発することに成功した。それらは非可換性を構造として持ち、少なくとも 1 変数多項式を用いて構成した場合のように可換性を利用して簡単に解読されるということはない。

(2) 多変数公開鍵暗号の新暗号方式の提案（その１）

制約付き MP 問題の解読困難性を仮定して暗号方式を開発した。これは多変数公開鍵暗号の従来の（すでに解読されたものも含めた）暗号方式を強化して利用する方法でもある。これを *pq* 法と名付けた。簡単に説明すると従来の暗号方式にノイズとなるような多変数多項式を加えることで安全性を強化している。通常の MP 問題の解読困難性を仮定する場合、この方法では解の場所が変わることになり、復号がうまくいかない。そこで制約付き MP 問題が必要となる。定義

域を制限することにより、その定義域内ではノイズの追加が解の場所に影響を与えないようにすることができる。その性質を利用して暗号方式を構成した。従来方式は今のところ、どれを用いても安全にすることができる。実際に実装まで行ったのは、松本-今井方式（C^*方式)、三角写像を用いた方式(echelon 型方式)、Square 方式の３つの従来方式に対してである。それぞれ、*pq*-C^*，*pq*-TM，*pq*-Square と名付けた。いずれも効率的な暗号化、復号化アルゴリズムを持つことが実験的にも確認できた。この提案方式は論文化し、査読付き国際会議 ProvSec2018 に投稿して採択された。

(3) 多変数公開鍵暗号の新暗号方式の提案（その２）

もう一つ制約付き MP 問題の解読困難性を仮定して暗号方式を開発した。これを PERN（Polynomial Equations over Real Numbers）と名付けた。これは(2)の *pq* 法による構成で作られる暗号の方式（の公開鍵を）を完全に含む一般的な方法である。さらに安全性を強化することが可能である。ただし、復号方法は *pq* 法とは異なる。*pq* 法の復号方法はノイズを除去した後、そこで利用している従来方式の復号アルゴリズムを使っている。例えば、*pq*-TM であれば、echelon 型の多変数多項式方程式を解くため、変数を 1 つずつ代数計算で解くことが可能であり、効率的な復号が可能である。一方、PERN はノイズを除去した後、多変数多項式を実数体上の方程式と見ることにより最適化手法を用いた方程式求解を利用する。様々な求解手法が知られているが、本研究課題においては Newton 法のような直線探索法に絞って復号に利用した。実数体上で計算することや収束点列を利用することなどから実用時間内に復号化可能かどうか検証が必要であったので、実際に（4 アルゴリズムを）実装し、復号効率性を見積もった。*pq* 法に比べると効率性は劣るものの十分実用的な実行時間（2 秒以内）で復号できることを確認した。本方式が *pq* 法より優れている点は、公開鍵の一般性である。それは安全性仮定が *pq* 法よりも少なくて済むことを言っており、安全性が高い。今後、理論的安全性証明（証明可能安全性）をつけることが目標である。この提案方式は論文化し、査読付き国際会議 PQcrypto2020 に投稿して採択された。

(4) 128 ビット安全性に対するパラメータの見積もり

(2)や(3)の提案方式に対し、現在、安全性の基準となっている 128 ビット（および、192 ビット、256 ビット）安全性を持つパラメータを見積もった。まずは多変数公開鍵暗号に対する攻撃を実験的、理論的に解析した。グレブナー基底攻撃が最も驚異となる攻撃となるが、まず方式依存の脆弱性を持たないかどうかを実験的に検証した。一般的な制約付き MP 問題と同等と見なしてよいかという検証である。そのあと、グレブナー基底の計算量の理論的見積もりを用いて 128 ビット安全性を持つパラメータを見積もった。それ以外にも格子ベース暗号で用いる攻撃や総当たり攻撃に対する計算量の見積もりに対してもパラメータの見積もりを行い、いずれの攻撃に対しても 128 ビット安全性を持つパラメータが決定できた。また、量子コンピュータが利用できるようになった場合の攻撃計算量も見積もった。探索に関するグローバーのアルゴリズムが利用可能である場合の攻撃計算量を計算し、128 ビット安全性を持つパラメータを見積もった。この結果はそれぞれの提案方式の採択論文に掲載されている。以下の表は、PERN の 128 ビット、192 ビット、256 ビットのパラメータとそれに対する体の標数の大きさ、鍵生成の時間、暗号化の時間、復号化の時間、秘密鍵長、公開鍵長を並べたものである。

(n, L, L_G)	level	$\|q\|_2$	key gen.(ms)	enc.(ms)	dec.(ms)	SK(kB)	PK(kB)
$(80, 15, 11)$	128	39.99	477.53	0.71	185.18	298	1,328
$(122, 15, 9)$	192	41.79	1499.66	1.87	828.81	1,009	4,884
$(166, 15, 9)$	256	43.55	4369.40	6.47	2526.77	2,481	12,807

表 1　提案方式 PERN のパラメータとその性能

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　1件／うちオープンアクセス　0件）

１．著者名 Takanori Yasuda	４．巻 11192
２．論文標題 Multivariate Encryption Schemes Based on the Constrained MQ Problem	５．発行年 2018年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 129～146
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-01446-9_8	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hiroaki Anada, Takanori Yasuda, Junpei Kawamoto, Jian Weng, Kouichi SAKURAI	４．巻 45
２．論文標題 RSA Public Keys with Inside Structure: Proofs of Key Generation and Identities for Web-of-Trust	５．発行年 2019年
３．雑誌名 Journal of Information Security and Applications	６．最初と最後の頁 10-19
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1016/j.jisa.2018.12.006	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Takanori Yasuda, Yacheng Wang, Tsuyoshi Takagi	４．巻 12100
２．論文標題 Multivariate Encryption Schemes Based on Polynomial Equations over Real Numbers	５．発行年 2020年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 402-421
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-44223-1_22	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 安田貴徳
２．発表標題 ペアリング高速計算に適した楕円曲線からその適切な部分群への効率的な写像
３．学会等名 Symposium on Cryptography and Information Security (SCIS2018)
４．発表年 2018年

１．発表者名 安田貴徳，照屋唯紀
２．発表標題 制約付きMP問題に基づいた多変数公開鍵暗号方式
３．学会等名 Symposium on Cryptography and Information Security (SCIS2019)
４．発表年 2019年

１．発表者名 安田貴徳
２．発表標題 ノイズを利用した多変数公開鍵暗号
３．学会等名 Symposium on Cryptography and Information Security (SCIS2020)
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	高木　剛 (Takagi Tsuyoshi)		