多変数多項式システムを用いた安全な暗号技術の研究（131310002）

Research of secure cryptographic technology using polynomial system

研究代表者

安田 貴徳　九州先端科学技術研究所

Takanori Yasuda　Institute of Systems, Information Technologies and Nanotechnologies

研究分担者

櫻井 幸一 †　高木 剛 †　ダハン・グザヴィエ †　ホアン・ユンジュ †

Kouichi Sakurai†　Tsuyoshi Takagi†　Xavier Dahan†　Yun-Ju Huang†

†九州先端科学技術研究所

†Institute of Systems, Information Technologies and Nanotechnologies

研究期間　平成 25 年度～平成 27 年度

概要

多変数多項式公開鍵暗号の厳密な安全性評価基準の設計と、暗号パラメータサイズの削減などの従来からの課題の克服のため以下の 3 点に取り組む。1. 計算機実験とコンテストによる多変数多項式公開鍵暗号の安全性の厳密評価、2. 代数構造を使った多変数多項式公開鍵暗号の暗号パラメータサイズの削減、3. 耐量子暗号のワークショップの開催と耐量子暗号の研究拠点の形成。

１．まえがき

現在既に広く普及している暗号技術（RSA暗号と楕円曲線暗号）の安全性は、大規模な量子コンピュータの出現により崩壊することが知られている。そのため、量子コンピュータに耐性を持つ次世代暗号技術（耐量子暗号）の開発が世界的な急務となっている。実際、暗号業界では、PQCRYPTOという耐量子暗号を主のテーマとした国際会議が定期的に開催されるなど、活発に研究が進んでいる。さらに、本課題の研究代表者らが運営し、平成28年2月に開催されたPQCrypto 2016では、米国標準技術研究所（NIST）が、耐量子暗号の標準化暗号の公募を開始するとのアナウンスを行った。また、欧州電気通信標準化機構ETSIも耐量子暗号のワークショップを定期的に開催している。産業界においても、耐量子暗号の実用化に向けた研究開発活動が見られる。

２．研究開発内容及び成果

本研究開発では耐量子暗号の候補の中でも処理効率が高いという特長を持つ多変数多項式公開鍵暗号を研究開発の対象としている。但し、多変数多項式公開鍵暗号は安全性の厳密解析、鍵長の削減問題、新しい暗号方式の開発といった研究課題を持つことがすでに知られている。多変数多項式公開鍵暗号が今後標準化、実用化されるためには、これらの課題を克服することが必須である。以上の状況を踏まえ、本研究開発では全体（３年）を通して以下の３つを目標として掲げた。

① 計算機実験とコンテストによる多変数多項式公開鍵暗号の**安全性の厳密評価**

② 代数構造を使った多変数多項式公開鍵暗号の**暗号パラメータサイズの削減**

③ 耐量子暗号のワークショップの開催と耐量子暗号の**研究拠点の形成**

目標①に対する成果

平成27年4月1日から解読コンテストMQチャレンジを開催した。早速、F5攻撃アルゴリズムの提案者J.-C. Faugère氏が回答を寄せるなど、その後も順調に回答が寄せられており、１年間で約30問が解読された。リースした計算機サーバを用いて、寄せられた回答の正誤を確認し、正解の場合はホームページで回答の情報を掲載するなどの管理を行った。また、MQチャレンジの開催案内、中間報告の発表（５件）も行った。６タイプの問題を用意したが、タイプ毎に異なる解読方法が用いられており、安全性の傾向を得ることができた。今後、暗号の主流が耐量子暗号に移行していくことが確実で、多変数多項式公開鍵暗号もその担い手の一つと目されている中、多変数多項式暗号の安全性を正確に見積もるための評価基準としてこのMQチャレンジが中心的な役割を果たして行くことになる。こういったことから目標①は計画通りの成果を上げた。

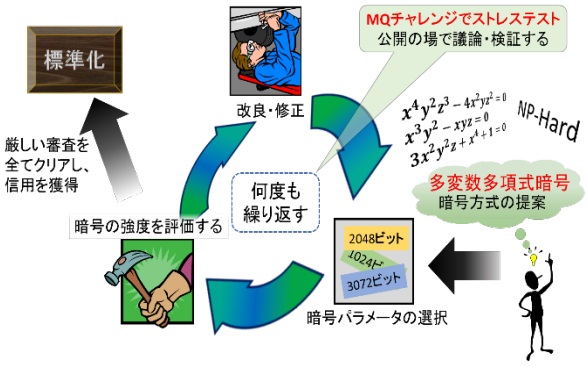

図１　安全性の厳密評価方法

目標②に対する成果

多変数多項式公開鍵暗号の安全な暗号方式の開発を行い、１つの方式を提案し、特許出願を行った。これは鍵長の削減と安全な暗号方式の開発という２つの課題を克服している。また、格子ベース暗号を応用し、部分復号技術を実現する高機能技術を提案し、特許出願を行った。これは従来の部分復号技術の持つ鍵管理の複雑さの問題を解決している。これに関してさらに報道発表を行いネット配信応用というより具体的な実用方法を提案した。さらに多変数多項式公開鍵暗号の鍵長削減問題を克服した方式を３種類開発した。暗号開発に関する論文を７件発表し、全

体の論文数、発表数も当初の計画よりも多かった。目標②は計画以上の成果を上げた。

図２　提案方式の応用

目標③に対する成果

ワークショップを２回、国際会議を１回開催した。開催した国際会議である「PQCrypto」は耐量子暗号の注目度が高まっていくにつれ、参加者数も増える傾向にはあったものの、PQCrypto 2016は前回のPQCryptoの参加者数(125名)を大きく超え、約240名の参加者が集まる特に注目度の高い会議となった。Winter Schoolの講演者および招待講演者の10名の研究者は耐量子暗号の専門家であり、本課題の研究活動に対して様々な評価・助言を提供して頂いた。それにより多変数多項式公開鍵暗号が今後、公開鍵暗号として実用化に向かっていく道筋が見られたことは本会議を開催した意義の一つである。また、多変数多項式公開鍵暗号と比較検討の対象となる格子ベース暗号、符号ベース暗号などについても最新動向を把握することができ、それぞれの得意、不得意分野が存在し、特に多変数多項式公開鍵暗号は署名や認証などの得意分野を活かした実用方法を目指すことが重要であることを認識できた。耐量子暗号の権威者たちからも本会議および本研究開発に対して高い評価を得ることができた。また、今回の国際会議により、福岡の地を日本の耐量子暗号の研究拠点として広くアピールすることができたと考えている。目標③は計画以上の成果を上げた。

３．今後の研究開発成果の展開及び波及効果創出への取り組み

（イ）　解読コンテスト「MQ チャレンジ」継続

MQ チャレンジの web ページは九州大学のサーバで管理されているため、今後も継続することが可能である。MQ チャレンジは開始からまだ１年しか経っておらず、多変数多項式公開鍵暗号の安全性を厳密評価するためにはまだデータ量が不十分である。そのため、今後も５年以上は MQ チャレンジを継続することを予定している。これにより得られたデータは web 上で公開し、安全性の評価基準として利用されることを目的としている。特に NIST による耐量子暗号の標準化プロジェクトの安全性評価指標として MQ チャレンジの結果が用いられることが今後の大きな目標となる。また、MQ チャレンジで扱う問題の追加を検討している。より実用化に即した安全性評価基準を提供することを目指す。

（ロ）提案した方式の標準化

提案した暗号方式の標準化を目指す予定である。本研究課題の活動の一環として運営した PQCrypto 2016 では NIST による耐量子暗号の標準化暗号の公募がアナウンスされた。今後、数年から十数年の間に新しい標準化暗号が決定される。この標準化暗号として本研究課題の提案方式を申請することを検討している。 [誌上発表リスト 1]は多変数多項式公開鍵暗号における暗号方式である。多変数多項式公開鍵暗号では、署名方式は比較的構成しやすいが、暗号方式は安全な方式の候補自体が少ないため、実用的な方式の開発が難しいとされてきた。そのため、[誌上発表リスト 1]が標準化されれば多変数多項式公開鍵暗号が署名方式、暗号方式の両方で標準化暗号を持つ可能性が高くなる。NIST は暗号標準化において世界で最も影響力が大きい機関であり、NIST で標準化された暗号は暗号基盤として世界中に普及する可能性が極めて高い。そういったことから提案方式の標準化は多変数多項式公開鍵暗号の次世代暗号としての普及につながる。

４．むすび

多変数多項式公開鍵暗号の厳密な安全性評価や実用的方式の開発など、計画した３つの目標に対して予想した以上の成果を上げることができた。但し、現在も実行中の解読コンテスト「MQ チャレンジ」は長い時間をかけて慎重に調査するべき性格のものであり、今後もデータ収集を継続する予定である。

【誌上発表リスト】

[1]Takanori Yasuda, Kouichi Sakurai, "A multivariate encryption scheme with Rainbow", ICICS2015 Springer LNCS vol. 9543 pp222-236 2015 年 12 月 10 日

[2]Takanori Yasuda, Tsuyoshi Takagi, Kouichi Sakurai、“Efficient variant of Rainbow using sparse secret key”, Journal of Wireless Mobile Networks Ubiquitous Computing, and Dependable Applications (JoWUA) Vol. 5 No. 3 2014

[3]Takanori Yasuda, Tsuyoshi Takagi, Kouichi Sakurai, “Security of Multivariate Signature Scheme using Non-commutative Rings”, IEICE TRANS. FUNDAMENTALS Vol. E97-A No.1 2014

【申請特許リスト】

[1]安田貴徳、穴田啓晃、櫻井幸一、“復号方法”、 特許出願番号：特願2015-160207、日本、2015年8月14日

[2]安田貴徳、穴田啓晃、櫻井幸一、“暗号装置及び復号装置”，特許出願番号：特願2015-160207、日本、2015年8月14日

【受賞リスト】

[1]田中哲士、情報 処理 学会 九州支部奨励賞、“線形回帰数列を用いた GF 上の QUAD ストリーム暗号の並列実装”、平成 26 年度（第 67 回）電気・情報関係学会九州支部連合大会、2015 年 1 月 5 日

[2]Satoshi Tanaka, Chen-Mou Cheng, Takanori Yasuda, Kouichi Sakurai、WICS Best Paper“Parallelization of QUAD Stream Cipher using Linear Recurring Sequences on Graphics Processing Units”, The Second International Symposium on Computing and Networking (CANDAR'14), 2014 年 10 月 29 日

[3]IWSEC2013 Best Student Paper Award: Yun-Ju Huang、Christophe Petit, Naoyuki Shinohara and Tsuyoshi Takagi, "Improvement of Faugère et al.'s method to solve ECDLP", 2013 年 11 月 20 日

【本研究開発課題を掲載したホームページ】

http://www.isit.or.jp/lab2/member/takanoriyasuda_japanese/