様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　２２　日現在

機関番号：　８７１０３
研究種目：　若手研究(B)
研究期間：　2012～2014
課題番号：　２４７４００７８

研究課題名（和文）非可換構造を用いた多変数多項式公開鍵暗号の設計と解析

研究課題名（英文）Design and analysis of multivariate public key cryptosystems using non-commutative structure

研究代表者

安田　貴徳（Yasuda, Takanori）

公益財団法人九州先端科学技術研究所・その他部局等・研究員

研究者番号：００４６４６０２

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：多変数多項式公開鍵暗号は量子コンピュータに耐性を持ち、暗号化や復号化の処理効率が良いという長所がある。一方で、膨大な鍵長を持つという課題点も持つ。そこで、これまで可換環や体を用いて設計していた多変数多項式公開鍵暗号に非可換環を応用して、鍵長を削減する方法を提案した。オリジナルの方式に比べて約80%の削減に成功した。その方式の安全性を解析し、適切なパラメータの選択方法を提示した。

研究成果の概要（英文）：Multivariate public key cryptosystems (MPKC) can resist attacks using quantum computer, and have efficient encryption and decryption. On the other hand, there is a problem that MPKC have huge key size. Therefore, I apply non-commutative rings to MPKC, which originally are designed using commutative rings and fields, and propose a method to reduce key size of MPKC. In comparison with the original scheme in MPKC, my scheme can reduce key size by about 80%. Moreover, I analyze its security and present how to select suitable parameters.

研究分野：　暗号理論

キーワード：　公開鍵暗号　ポスト量子暗号　多変数多項式公開鍵暗号

１．研究開始当初の背景

（１）1994 年に AT&T Bell 研究所の Peter W. Shor 氏が開発したアルゴリズムにより、量子コンピュータの普及が現実となれば、現代の公開鍵暗号基盤をなしている RSA 暗号と楕円曲線暗号は短時間で解読されることが証明された。

（２）上の理由で、量子コンピュータに耐性を持つ公開鍵暗号（耐量子暗号）の開発が急務となった。現在、暗号界では耐量子暗号は一大研究分野となっている。

（３）多変数多項式公開鍵暗号は耐量子コンピュータの候補であり、処理効率の高い公開鍵暗号として注目されていたが、RSA 暗号などと比べて鍵長が大きいという課題点があった。

２．研究の目的

研究の目的は、安全性を低下させることなく多変数多項式公開鍵暗号の鍵長を削減する方法を開発することである。基準は RSA 暗号であり、原型の多変数多項式公開鍵暗号は RSA 暗号の 200 倍近い鍵長を持っており、これを RSA 暗号に近い鍵長サイズまで軽減することが目的である。また、鍵長削減だけでなく、効率性の向上も同時に達成する方法が望ましい。

３．研究の方法

（１）非可換環を利用する。多変数多項式公開鍵暗号は位数の小さな有限体が基礎となるが、構成する際にさらに拡大体を利用する。これを非可換環にまで拡張し利用する。これにより、鍵長削減を達成する。

（２）非可換環を用いた方式で鍵長削減方式を開発した後、鍵長削減に寄与した部分を解析し、非可換環に拘らない鍵長削減方式に拡張する。

（３）従来方式とは構造が異なる多変数多項式公開鍵暗号の新しい方式を開発し、鍵長削減を達成する。

４．研究成果

（１）多変数多項式公開鍵暗号の方式の１つに Rainbow と呼ばれるものがある。これは高い安全性を持つことが期待されており、処理効率が高いことが長所である。しかし、他の多変数多項式公開鍵暗号の方式同様、鍵長が大きいことが課題であった。研究代表者は Rainbow に非可換環を利用し、鍵長削減方法を提案した。これにより約 80%の鍵長削減に成功した。

提案方式	方式1	方式2	方式3
安全性レベル	83bits	96bits	107bits
鍵サイズ	8.0kB	15.1kB	25.5kB
対応するオリジナル方式の鍵サイズ	33.6kB	70.7kB	128.2kB
削減率	76.1%	78.5%	79.9%

表1：非可換環を用いた鍵長削減

（２）まだらな鍵を用いる方法その１．非可換環を用いた鍵長削減方式は鍵長削減率が非常に高いが、安全性解析が難しく、安全性に対する影響が見積もりにくい構造が存在する。そこで既存の攻撃方法の攻撃計算量を解析し、それらに耐性を持つ最小限のパラメータ削減箇所を見極め、さらに署名生成の効率性を向上させる方式を提案した。署名方式 Rainbow を基にしており、その oil 部分と呼ばれる部分を削減した。

	鍵長	署名生成	実験
オリジナル方式	90226 bytes	98636 M	694 μsec
提案方式	56674 bytes	58938 M	455 μsec
削減率	37.2%	39.8%	34.4%

表2：オイル部分の鍵長削減

（３）まだらな鍵を用いる方法その２．（２）の研究の続きとして、Rainbow の鍵の Vinegar 部分とよばれる部分を削減し、さらに署名生成が効率的となる方式を提案した。

	鍵長	署名生成	実験
オリジナル方式	89776 bytes	98112 M	695 μsec
提案方式	52709 bytes	60966 M	475 μsec
削減率	41.3%	37.9%	31.7%

表3：ビネガー部分の鍵長削減

（４）上記の（２）と（３）は併用することができた。削減効果も効率性向上も重ね合わせることができた。これにより、約 80%の鍵長削減と約 60%の署名生成効率性の向上を達成することができた。

（５）2 次形式を用いた多変数多項式公開鍵暗号の署名方式を提案した。これは従来の全射多変数多項式写像を用いる署名方式の構造とはことなり、2 つの全射でない多項式写像を用いる新しい方式である。さらに安全性においても従来の攻撃の多くが適用できない数学的に特殊な構造を持っている。この方式は従来方式の鍵長の削減および、効率性向上も達成する。

（６）通常よりやや大きめの基礎体 GF(2^16)や GF(2^32)などを用いる場合の多変数多項式公開鍵暗号の効率性向上のための基礎体の選択方法と GPU を用いた効率的計算方法をいくつか考案し、それらを比較した。基礎体を GF(2^8)などの乗積表が使用できる小さい体の拡大体として見て、定義多項式を用いる代わりに生成元による指数表示で元を表示する方法が効率的であることが分かった。

Method	XOR	AND	MOD	LOOKUP	Memory
Polynomial basis	961	1,024	1	0	4B
Normal basis	16,864	16,400	0	0	63B
Zech's method	1 ADD	0	1	3	32GB
Lookup table	0	0	0	1	64EB

表4：GF(2^32)の算術演算速度比較

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計８件）

（１） Takanori Yasuda, Jintai Ding, Tsuyoshi Takagi, Kouichi Sakurai, “A variant of rainbow with shorter secret key and faster signature generation”, ACM Asia Public-Key Cryptography Workshop (AsiaPKC2013), pp.57-62, 2013, 査読あり, DOI:10.1145/2484389.2484401.

（２） Motoki Kitahara, Takanori Yasuda, Takashi Nishide, Kouichi Sakurai, “Upper bound of the length of information embedd in RSA public key efficiently”, ACM Asia Public-Key Cryptography Workshop (AsiaPKC2013), pp.33-38, 2013, 査読あり, DOI: 10.1145/2484389.2484394.

（３） Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai, “Security of multivariate signature scheme using non-commutative rings”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E97-A, No.1, pp.245-252, 2014, 査読あり, DOI: 10.1587/transfun. E97.A.245.

（４） Takanori Yasuda, Tsuyoshi Takagi, Kouichi Sakurai, “Efficient variant of Rainbow without triangular matrix representation”, The 2015 Asian Conference on Availability, Reliability and Security (AsiaARES2014), Springer LNCS, Vol.8407, pp.532-541, 2014, 査読あり,Doi:10.1007/978-3-642-55032-4_55.

（５） Takanori Yasuda, Tsuyoshi Takagi, Kouichi Sakurai, “Multivariate signature scheme using quadratic forms”, Fifth International Conference on Post-Quantum Cryptography (PQCrypto2013), Springer LNCS, vol.7932, pp.243-258, 2013,査読あり,DOI: 10.1007/978-3-642-38616-9_17.

（６） Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai, “Efficient variant of Rainbow using sparse secret keys”, Innovative Information Science & Technology Research Group, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.5, No.3, pp.3-13, 2014,査読あり,DOI:なし.

（７） Satoshi Tanaka, Takanori Yasuda, Kouichi Sakurai, “Fast evaluation of multivariate quadratic polynomials over GF(2^32) using grahpics processing units”, Innovative Information Science & Technology Research Group, Journal of Internet Services and Information Security (JISIS), Vol.4, No.3, pp.1-20, 2014,査読あり,DOI:なし.

（８） Satoshi Tanaka, Chen-Mou Cheng, Takanori Yasuda, Kouichi Sakurai, “Parallelization of QUAD stream cipher using linear recurring sequences on graphics processing units”, The Second IEEE International Symposium on Computing and Networking (CANDAR2014), pp.543-548, 2014,査読あり,DOI:10.1109/CANDOR.2014.85.

〔学会発表〕（計９件）

（１）安田貴徳, 高木剛, 櫻井幸一, “三角行列表示を用いない Rainbow 型電子署名方式”, 情報セキュリティ研究会(ISEC2010), 北海道工業大学, 2012 年 7 月.

（２）安田貴徳, 高木剛, 櫻井幸一, “非可換環を用いた多変数多項式署名方式に対するランク攻撃に対する考察”, コンピュータセキュリティシンポジウム 2012(CSS2012), 松江市, 2012 年 11 月.

（３）安田貴徳, 高木剛, 櫻井幸一, “2 次形式の分類定理を用いた多変数多項式デジタル署名”, 2013 年暗号と情報セキュリティシンポジウム(SCIS2013), 京都市, 2013 年 1 月.

（４）安田貴徳, “多変数多項式暗号の動向”, 2013 年ソサイエティ大会, 九州工業大学, 2013 年 9 月.

（５）安田貴徳, 高木剛, 櫻井幸一, “固定された係数を持つペアリングフレンドリ曲線”, 2014 年暗号と情報セキュリティシンポジウム(SCIS2014), 鹿児島市城山観光ホテル, 2014 年 1 月.

（６）安田貴徳, 高木剛, 櫻井幸一, “楕円曲線の効率的モデルの Ate 系ペアリングへの応用”, 情報セキュリティ研究会(ISEC2013), 札幌コンベンションセンター, 2013 年 7 月.

（７）Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, Kouichi Sakurai, “Multivariate Quadratic Challenge”, ETSI Quantum Safe Workshop, カナダオタワ, 2014 年 10 月.

（８） Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, Kouichi Sakurai, “MQ チャレンジ ～多変数多項式暗号の安全性評価～”, 応用数理学会 2015 年研究部会連合発表会, 中央大学, 2015 年 3 月.

（９）安田貴徳, “PQCrypto 2014 参加報告”, 第 32 回情報とセキュリティシンポジウム(SCIS2015), 北九州市, 2015 年 1 月.

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

○取得状況（計０件）

〔その他〕
ホームページ等
http://www.isit.or.jp/lab2/member/takanoriyasuda_japanese/

６．研究組織
(1)研究代表者
安田貴徳（YASUDA Takanori）
（公財）九州先端科学技術研究所・研究員
研究者番号：00464602

(2)研究分担者　なし

(3)連携研究者
高木剛（TAKAGI Tsuyoshi）
九州大学マスフォアインダストリ研究所・教授
研究者番号：60404802

櫻井幸一（SAKURAI Kouichi）
九州大学システム情報科学研究院・教授
研究者番号：60264066