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　６ 年　 ６ 月 １３ 日現在

機関番号：１７１０２
研究種目：若手研究
研究期間：2019～2023
課題番号：１９Ｋ２０２６６

研究課題名（和文）多変数連立方程式の求解困難性を基にした耐量子暗号の安全性評価

研究課題名（英文）Security analysis on post-quantum cryptography based on multivariate quadratic polynomial problem

研究代表者
池松　泰彦（Ikematsu, Yasuhiko）

九州大学・マス・フォア・インダストリ研究所・助教

研究者番号：４０８３３５７０

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：多変数連立方程式の求解困難性を基にした多変数多項式暗号(MPKC)における安全性解析を行った。特に、グレブナー基底攻撃・ランク攻撃の精密な評価を目指し、NIST PQC標準化計画に関連する方式を含めた様々な多変数多項式暗号の解析を行なった。その結果、いくつかの方式の脆弱性を発見したり、新たな攻撃手法に基づいた安全性評価を提案した。さらに、その過程で得られた結果を用いて、署名方式、ID方式などの提案を行なった。

研究成果の学術的意義や社会的意義
多変数多項式暗号は連立二次方程式の求解困難性を利用した耐量子計算機暗号の一つであり、量子コンピュータ時代における次世代暗号として必要不可欠な技術となっている。本研究課題で提案した方式や安全性解析手法により、安心・安全な耐量子計算機暗号の実用化に貢献できれば、量子コンピュータ時代の暗号基盤を支える重要な要素となり、社会に与えるインパクトは大きい。

研究成果の概要（英文）：We studied the security analysis on multivariate public key cryptography (MPKC) based on the hardness of solving multivariate quadratic equations over finite fields. In particular, we analysed various multivariate cryptosystems, including schemes submitted to the NIST PQC standardization project, aiming at a precise estimation of the Groebner basis attacks and rank attacks. As a result, we found vulnerabilities in some schemes and proposed security estimations based on new attack methods. Moreover, using the results obtained in this study, we proposed a signature scheme and ID scheme.

研究分野：暗号理論

キーワード：耐量子計算機暗号　多変数多項式暗号

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

Shor の量子アルゴリズムによって因数分解問題・離散対数問題は多項式時間で解かれるため、現在普及している RSA 暗号・楕円曲線暗号は大規模な量子コンピュータによって解読される可能性がある。そこでどのような古典・量子アルゴリズムでも破ることができない暗号として耐量子計算機暗号(PQC)の開発が活発に進められている。2016 年にはアメリカの政府機関 NIST が PQC の標準化計画を発表し、2017 年 11 月を締め切りとして 69 件もの暗号方式・鍵共有方式・署名方式が投稿され候補となった。その後、何度かの選考ラウンド(絞り込み)を経て最終的にいくつかの方式が標準化されることになっている。PQC の候補として格子暗号・符号暗号・同種写像暗号・多変数多項式暗号などがある。特に、多変数多項式暗号(MPKC)は有限体上の多変数連立二次方程式の求解問題(MQ 問題)の困難性に安全性の根拠を置く PQC の一つである。NIST PQC 標準化計画においてもいくつもの MPKC が投稿されたが、その中でも署名方式 UOV や HFE の改良方式(Rainbow, GeMSS など)は署名サイズが小さいという利点を有し、有力な候補となっていた。しかし、MPKC の安全性解析は十分成熟しているとは言い難く、各方式を特徴づける数学的構造を十分に利用できないまま安全性解析が行われていることもあり、MPKC の実用化・標準化のためにはより精密な安全性解析が求められている。

２．研究の目的

MPKC の安全性解析を精密化することが主な目的である。そのために、これまで提案されてきた方式に対して、その方式特有の数学的構造が安全性にどのように影響するのかを調べることが必要となる。例えば、グレブナー基底などの方程式求解アルゴリズムを使う際にその数学的構造を利用することで、アルゴリズムの効率化、計算量評価の精密化が可能かどうかを理論的・実験的に考察する必要がある。また、得られた考察によって MPKC の安全性を測る攻撃の固定パラメータに対する評価を行い、MPKC の実用的な安全性パラメータの導出を行う。

３．研究の方法

多項式系のグレブナー基底を求めるアルゴリズム F4 や F5 を使ったグレブナー基底攻撃や、行列のランクに着目したランク攻撃に関して、攻撃で現れる方程式系に付随する solving degree や degree of regularity などの不変量に関する既存研究を調査し、さらに特定の攻撃に現れる方程式系に対する不変量とその計算量との関係について理論的、実験的に考察する。また、これまで提案された方式の数学的構造を調べ、その構造を利用した攻撃の提案や、その構造が上記不変量にどのように影響するかを考察する。最終的に、安全性解析の精密化を行い、方式自体の解読または可能ならば改良を行う。

４．研究成果

以下の主な成果を得ることができた。

(1)数学的構造を利用した安全性解析：

① 20 年以上致命的な欠陥が発見されていない UOV 署名方式は MPKC における重要な方式となっているが、公開鍵の大きさが欠点とされている。そのため、UOV を効率化した改良方式がこれまでいくつも提案されてきた。その中で BAC-UOV 方式は、巡回行列の構造を使って安全性を損なわないよう UOV の公開鍵長を削減した改良方式である。本研究において、巡回行列が剰余環の構造を持ち、剰余環の分解に応じて巡回行列を二つのブロック行列に同時対角化することで、BAC-UOV を二つのサイズの小さい UOV に分解できることを示した。その二つの UOV をうまく組み合わせることで BAC-UOV への攻撃を提案し、例えば 147bit 安全性を持つ提案パラメータは 119bit の安全性しか持たないことが明らかになった。

② MQ-Sign 方式は韓国が行っている PQC 標準化プロジェクト KpqC に提案された方式で、UOV で扱われる行列構造を一部スパースにすることで効率化を図った改良方式である。先行研究として Aulbach らは、この方式のいくつかのバージョンに対して鍵復元攻撃を提案したが、それは秘密鍵 S が単純な形であることを仮定して行っている。これに対して我々の攻撃は一般的な秘密鍵 S に対応できる鍵復元攻撃を提案した。具体的には、正則行列 S、その逆行列、および中心写像 F の各成分を変数として，公開鍵から得られる連立二次方程式系を構成する。そして、この連立方程式を解くために、方程式系をいくつかの部分系に適切に分類し、変数のいくつかを総当たり法によって推測して連立線形方程式に帰着させる。最後に、連立線形方程式を解くことで秘密鍵 S を多項式時間で復元する。また、この攻撃に関する実験を行い、提案された安全性レベル 1, 3, 5 のパラメータを標準的なノートパソコンを用いて、30 分以内で破った。

③ SNOVA 方式は 2022 年に新たにスタートした NIST PQC 標準化追加公募において提案された方式で、有限体$\mathbb{F}_q$上の UOV に行列環$\mathbb{M}_l(\mathbb{F}_q)$の非可換性を利用することで効率化を図った改良方式である。この方式に対して、構成の別解釈を与えることで、従来の安全性解析を改良する手法を提案した。特に、UOV の既存攻撃である KS 攻撃、Reconciliation 攻撃、Intersection 攻撃を改良することができた。その結果、一部のパラメータが設定された安全性を満たしていないことを示した。以下の表はその計算量評価のまとめである。パラメータのv, oは UOV の oil 変数、vinegar 変数の個数である。kは方程式を解く際にk個の変数に適当な値を代入する Hybrid 手法のパラメータである。それぞれの攻撃の計算量の単位は gate である。また、I,III,V はそれぞれ$2^{143}, 2^{207}, 2^{272}$gate 安全性を満たすパラメータとして、SNOVA の提案者によって選定されたパラメータである。例えば、143gate 安全性が要求されるパラメータの一つ(一番上)は改良された Intersection 攻撃によって 87gate の安全性しか持たないことが明らかになった。

	(q, v, o, l)	KS attack	Reconciliation attack	Intersection attack
I	$(16, 28, 17, 2)$	**93**	**132** $(k = 2)$	**87** $(k = 0)$
	$(16, 25, 8, 3)$	209	209 $(k = 15)$	221 $(k = 0)$
	$(16, 24, 5, 4)$	309	270 $(k = 30)$	349 $(k = 0)$
III	$(16, 43, 25, 2)$	**149**	**193** $(k = 6)$	**120** $(k = 0)$
	$(16, 49, 11, 3)$	461	438 $(k = 66)$	529 $(k = 0)$
	$(16, 37, 8, 4)$	469	388 $(k = 45)$	507 $(k = 0)$
V	$(16, 61, 33, 2)$	**229**	277 $(k = 17)$	**167** $(k = 1)$
	$(16, 66, 15, 3)$	617	575 $(k = 87)$	690 $(k = 0)$
	$(16, 60, 10, 4)$	805	695 $(k = 112)$	922 $(k = 0)$

④ 多項式系同型問題(IP 問題)の変種である CDH-BIPC 問題に基づいた暗号方式の安全性解析を行った。IP 問題とは、有限体$\mathbb{F}$上の二つの二次多項式写像$F: \mathbb{F}^n \to \mathbb{F}^m$と$G: \mathbb{F}^n \to \mathbb{F}^m$に対して、$G = T \circ F \circ S$を満たす正則な線形変換の組$S, T$を求める問題であり、CDH-BIPC 問題は IP 問題を巡回行列を用いて線型化した Diffe-Hellmann 型の計算問題となる。この暗号方式に対して、線型化に着目することによって同値鍵を多項式時間で構成するアルゴリズムを提案した。この攻撃によって、提案された 128bit 安全性パラメータのいくつかを標準的な PC を用いて 10 時間以内で破ることに成功した。

(2)安全性解析の改良：

① Rainbow は NIST PQC 標準化計画のファイナリストになった多変数署名方式である。その安全性解析に現れる bilinear 多項式に付随する 2 変数 Hilbert 級数を考察し、degree of regularity などの不変量を見積もることで、RBS 攻撃の計算量のより精密な評価を行った。

②MPKC の安全性解析に現れる MinRank 問題は MQ 問題とも深く関係する。そして MinRank 問題は特定の MQ 問題に帰着させることでグレブナー基底アルゴリズムなどを使って求解される。本研究において、MinRank 問題の求解方法の一つである Kipnis-Shamir 法に対する Verbel らの解析が Rainbow 署名方式にどのように影響を与えるかについて考察を行った。特に、Verbel らの解析で構成される syzygy が、ランダム MinRank 問題の場合と Rainbow の場合とで違いがないかを検証した。本研究においては Rainbow にのみ現れる syzygy を構成できなかったため、Verbel らの解析は Rainbow の安全性解析には影響がなかった。今後の課題として、実験などを利用して Rainbow にのみ現れる syzygy の有無について調べることが挙げられる。

③ Beullens によって Rainbow に対する Rectangular MinRank 攻撃が提案された。この攻撃は Rainbow の公開鍵である行列を変形し、現れた MinRank 問題を support minor モデリングを用いて解くことで秘密鍵の復元を行う。本研究によって、この攻撃手法が公開鍵多項式の数が通常の UOV よりも多いような UOV 改良方式に対しても適用できることを示した。その結果、MAYO, QR-UOV などの NIST PQC 標準化追加公募の候補にも Rectangular MinRank 攻撃が適用でき、この攻撃に基づいた安全性解析を行なった結果、提案パラメータが安全であることを確認した。この攻撃が他の方式にも適用できないかが今後の課題となる。

(3)新方式の提案：

① BAC-UOV の手法を一般化して QR-UOV 署名方式を提案した。具体的には、BAC-UOV の解析で現れた特定の剰余環を任意の剰余環に一般化し、さらに、構成の際に必要とされる剰余環の行列表示と転置操作のずれをなくすための補正行列の存在・構成を示すことで BAC-UOV を一般化した署名方式 QR-UOV を構成した。また、BAC-UOV で提案した(1)①の攻撃を回避す

るための必要十分条件が剰余環を構成する法多項式の既約性であることを示した。さらに QR-UOV の基礎体を持ち上げることで異なるパラメータの UOV に変形できることを示し、様々な観点から安全性解析も行なった。これらの結果、UOV 方式と比べて 2〜3 倍公開鍵長の小さい方式として QR-UOV を提案した。この QR-UOV は NIST PQC 標準化追加公募に 2023 年 6 月投稿し、書類選考を経て、第一回評価ラウンドの候補となっている。

② MinRank 問題に基づいた ID 方式の提案を行なった。MinRank 問題とは、与えられた行列の組に対して、非自明な線形和でランクが低いものを求める問題で、耐量子計算機暗号のベースとなり得る計算問題である。MinRank 問題の利点として、Rainbow などの多変数多項式暗号の安全性と関係することから、計算量評価などについては詳しく調べられてきた。そのため、安全性評価が盤石な MinRank 問題ベースの方式が提案できる可能性があるが、Asiacrypt 2001 で Courtois による対話型 ID 方式や、Fiat-Shamir(FS)変換による署名方式が提案されて以降、MinRank 問題をベースとした方式の開発はほとんど進展がなく、未開拓の計算問題であった。そこで Courtois の研究に着目し、2022 年に Courtois の方式を改良し、各ラウンドの cheating probability が 2/3 から 1/2 になる効率的な ID 方式を提案した。

５．主な発表論文等

〔雑誌論文〕　計18件（うち査読付論文　14件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Yasuhiko Ikematsu, Rika Akiyama	４．巻 -
２．論文標題 Revisiting the security analysis of SNOVA	５．発行年 2024年
３．雑誌名 APKC2024	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yasuhiko Ikematsu	４．巻 -
２．論文標題 A survey on small public key signature schemes derived from UOV signature scheme	５．発行年 2024年
３．雑誌名 Mathematical Foundations for Post-Quantum Cryptography, Mathematics for Industry, Springer	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Hiroki Furue, Yasuhiko Ikematsu	４．巻 LNCS 14128
２．論文標題 A New Security Analysis Against MAYO and QR-UOV Using Rectangular MinRank Attack	５．発行年 2023年
３．雑誌名 Proceedings of IWSEC 2023	６．最初と最後の頁 101-116
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 池松 泰彦, Hyungrok Jo, 安田 貴徳	４．巻 Vol.123, No.129, ISEC2023-31
２．論文標題 韓国PQC標準化計画(KpqC)で提案されたMQ-Signの安全性解析	５．発行年 2023年
３．雑誌名 電子情報通信学会技術研究報告	６．最初と最後の頁 113-118
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 Yasuhiko Ikematsu, Hyungrok Jo, Takanori Yasuda	4．巻 LNCS 14402
2．論文標題 A security analysis on MQ-Sign	5．発行年 2023年
3．雑誌名 Proceedings of the 24th World Conference on Information Security Applications	6．最初と最後の頁 40-51
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yasuhiko Ikematsu, Rika Akiyama	4．巻 -
2．論文標題 Revisiting the security analysis of SNOVA	5．発行年 2024年
3．雑誌名 2024 Symposium on Cryptography and Information Security	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 Shuhei Nakamura, Yasuhiko Ikematsu, Yacheng Wang	4．巻 E106-A No.3
2．論文標題 A New Analysis of the Kipnis-Shamir Method Solving the MinRank Problem	5．発行年 2023年
3．雑誌名 IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences (Special Section on Cryptography and Information Security)	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yasuhiko Ikematsu, Shuhei Nakamura, Tsuyoshi Takagi	4．巻 Vol.17, Issue 2
2．論文標題 Recent progress in the security evaluation of multivariate public-key cryptography	5．発行年 2023年
3．雑誌名 IET Information Security	6．最初と最後の頁 210-226
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yuntao Wang, Yasuhiko Ikematsu, Takanori Yasuda	4．巻 LNCS13600
2．論文標題 Lattice-Based Public Key Cryptosystems Invoking Linear Mapping Mask	5．発行年 2022年
3．雑誌名 Proceedings of ProvSec 2022	6．最初と最後の頁 88-104
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yasuhiko Ikematsu, Shuhei Nakamura, Bagus Santoso, Takanori Yasuda	4．巻 13007
2．論文標題 Security Analysis on an ElGamal-like Multivariate Encryption Scheme Based on Isomorphism of Polynomials	5．発行年 2021年
3．雑誌名 Lecture Notes in Computer Science	6．最初と最後の頁 235-250
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Shuhei Nakamura, Yasuhiko Ikematsu, Yacheng Wang, Tsuyoshi Takagi	4．巻 896
2．論文標題 New complexity estimation on the Rainbow-Band-Separation attack	5．発行年 2021年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 1-18
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Hiroki Furue, Yasuhiko Ikematsu, Yutaro Kiyomura, Tsuyoshi Takagi	4．巻 13093
2．論文標題 A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV	5．発行年 2021年
3．雑誌名 Lecture Notes in Computer Science	6．最初と最後の頁 187-217
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yacheng Wang, Yasuhiko Ikematsu, Shuhei Nakamura, Tsuyoshi Takagi	4．巻 12583
2．論文標題 Revisiting the Minrank Problem on Multivariate Cryptography	5．発行年 2020年
3．雑誌名 Lecture Notes in Computer Science	6．最初と最後の頁 291-307
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yasuhiko Ikematsu, Ryoya Fukasaku, Momonari Kudo, Masaya Yasuda, Katsuyuki Takashima, Kazuhiro Yokoyama	4．巻 -
2．論文標題 Hybrid Meet-in-the-Middle Attacks for the Isogeny Path-Finding Problem	5．発行年 2020年
3．雑誌名 Proceedings of the 7th ACM Workshop on ASIA Public-Key Cryptography	6．最初と最後の頁 36-44
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yuntao Wang, Yasuhiko Ikematsu, Koichi Akiyama, Tsuyoshi Takagi	4．巻 -
2．論文標題 Cryptanalysis of Giophantus(TM) Schemes against Hybrid Attack	5．発行年 2020年
3．雑誌名 Proceedings of the 7th ACM Workshop on ASIA Public-Key Cryptography	6．最初と最後の頁 28-35
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Hiroki Furue, Koha Kinjo, Yasuhiko Ikematsu, Yacheng Wang, Tsuyoshi Takagi	4．巻 12100
2．論文標題 A Structual Attack on Bloch-Anti-Circulant UOV at SAC 2019	5．発行年 2020年
3．雑誌名 Lecture Notes in Computer Science	6．最初と最後の頁 323-339
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yasuhiko Ikematsu,Shuhei Nakamura, Bagus Santoso, Takanori Yasuda	４．巻 -
２．論文標題 Security analysis on an El-Gamal-like multivariate encryption scheme based on a generalization of IP2S problem	５．発行年 2021年
３．雑誌名 Symposium on Cryptography and Information Security (SCIS2021)	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 Yuntao Wang, Yasuhiko Ikematsu, Takanori Yasuda	４．巻 -
２．論文標題 Public Key Cryptosystems Combining Lattice and Multivariate Polynomial	５．発行年 2021年
３．雑誌名 Symposium on Cryptography and Information Security (SCIS2021)	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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17件（うち招待講演　1件／うち国際学会　3件）

１．発表者名 池松泰彦
２．発表標題 Revisiting the security analysis against 2F method
３．学会等名 第 19 回日本応用数理学会研 究部会連合発表会
４．発表年 2023年

１．発表者名 Bagus Santoso, Yasuhiko Ikematsu, Shuhei Nakamura, Takanori Yasuda
２．発表標題 Three-Pass Identification Scheme Based on MinRank Problem with Half Cheating Probability
３．学会等名 ISITA 2022
４．発表年 2022年

１．発表者名
池松泰彦

２．発表標題
多変数多項式暗号の最近の進展について

３．学会等名
金沢暗号理論勉強会（招待講演）

４．発表年
2021年

１．発表者名
Yasuhiko Ikematsu

２．発表標題
Security Analysis on an ElGamal-like Multivariate Encryption Scheme Based on Isomorphism of Polynomials

３．学会等名
Inscrypt2021（国際学会）

４．発表年
2021年

１．発表者名
池松泰彦

２．発表標題
A study of the Kipnis-Shamir approach against the Rainbow signature scheme

３．学会等名
Symposium on Cryptography and Information Security (SCIS2022)

４．発表年
2022年

１．発表者名
池松泰彦

２．発表標題
Rainbow署名方式に付随するMinRank問題について

３．学会等名
日本応用数理学会第18回研究部会連合発表会

４．発表年
2022年

１．発表者名
Yasuhiko Ikematsu

２．発表標題
A study on randomness used in signature generation of UOV

３．学会等名
The 7th International Conference on Mathematics and Computing (ICMC2021)（国際学会）

４．発表年
2021年

１．発表者名
池松 泰彦

２．発表標題
Security analysis on an El-Gamal-like multivariate encryption scheme based on a generalization of IP2S problem

３．学会等名
Symposium on Cryptography and Information Security (SCIS2021)

４．発表年
2021年

１．発表者名
池松 泰彦

２．発表標題
耐量子計算機暗号におけるグレブナー基底攻撃の計算量評価について

３．学会等名
日本数式処理学会第29回大会

４．発表年
2020年

１．発表者名
池松 泰彦

２．発表標題
A Vulnerability on an Efficient Signature Generation Using Precomputation for UOV

３．学会等名
コンピュータセキュリティシンポジウム2020

４．発表年
2020年

１．発表者名
Yasuhiko Ikematsu

２．発表標題
Hybrid meet-in-the-middle attacks for the isogeny path-finding problem

３．学会等名
The 7th ACM ASIA Public-Key Cryptography Workshop (APKC 2020)（国際学会）

４．発表年
2020年

１．発表者名
池松泰彦

２．発表標題
同種写像パス探索問題に対する中間一致攻撃のハイブリッド手法

３．学会等名
Symposium on Cryptography and Information Security (SCIS2020)

４．発表年
2020年

１．発表者名
Yasuhiko Ikematsu

２．発表標題
Hybrid meet-in-the-middle attacks for the isogeny path-finding problem

３．学会等名
The 12th Workshop among Asian Information Security Labs (WAIS 2020)

４．発表年
2020年

１．発表者名
中村周平、池松泰彦、王亜成

２．発表標題
On the First Fall Degrees of Small Field Type MPKCs

３．学会等名
Symposium on Cryptography and Information Security (SCIS2020)

４．発表年
2020年

１．発表者名
Yuntao Wang、Yasuhiko Ikematsu、Koichiro Akiyama、Tsuyoshi Takagi

２．発表標題
Cryptanalysis of Giophantus(TM) Schemes against Hybrid Attack

３．学会等名
Symposium on Cryptography and Information Security (SCIS2020)

４．発表年
2020年

１．発表者名
Hiroki Furue、Koha Kinjo、Yasuhiko Ikematsu、Yacheng Wang、Tsuyoshi Takagi

２．発表標題
A Structural Attack on Block-Anti-Circulant UOV at SAC 2019

３．学会等名
Symposium on Cryptography and Information Security (SCIS2020)

４．発表年
2020年

１．発表者名
Yacheng Wang, Yasuhiko Ikematsu, Shunhei Nakamura, Tsuyoshi Takagi

２．発表標題
A Hybrid Method for Solving the Minrank Problem

３．学会等名
コンピュータセキュリティシンポジウム2019 （CSS2019）

４．発表年
2019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

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関