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　３ 年　 ６ 月　 １ 日現在

機関番号：１２６０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2020
課題番号：１７Ｋ００１８５

研究課題名（和文）ポスト量子暗号の標準化に向けた安全な暗号パラメータの導出

研究課題名（英文）Security Analysis of Post-Quantum Cryptography

研究代表者
高木　剛（Tsuyoshi, Takagi）

東京大学・大学院情報理工学系研究科・教授

研究者番号：６０４０４８０２

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究課題では、ポスト量子暗号(PQC)の標準化に向けた安全な暗号パラメータの導出に関する研究を行なった。特に、格子暗号の安全性の根拠となるLearning With Errors (LWE)問題に対する困難性を評価し、ダルムシュタット工科大が主催する解読チャレンジにおいて、70次元のLWE問題を32.7CPU時間で解読する世界記録を達成した。また、ring-LWE問題の困難性に基づいた効率的な2者間鍵交換方式を構成し、NIST PQC標準化プロジェクトの安全性レベルを達成する暗号パラメータを提案した。更に、格子暗号に対する様々な攻撃法（法切替攻撃、鍵再利用攻撃など）の安全性を評価した。

研究成果の学術的意義や社会的意義
本研究課題では、格子暗号に対して堅牢な計算量評価と実計算環境による大規模解読実験を行い、攻撃法の現実的なfeasibilityを評価することにより、128ビット安全性を有する具体的な暗号パラメータの導出を行った。本研究課題により、ポスト量子暗号の安全性検証法を深化させ、その安全な暗号パラメータの選定に貢献できるため学術的かつ実用的な波及効果は大きい。

研究成果の概要（英文）：In this research project, we conducted research on the derivation of secure cryptographic parameters for the standardization of post-quantum cryptography (PQC). In particular, we evaluated the difficulty of the Learning with Errors (LWE) problem, which is the basis of the security of lattice-based cryptography, and we achieved a world record for solving the 70-dimensional LWE problem in 32.7 CPU hours in the LWE challenge hosted by Darmstadt University of Technology. We also constructed an efficient key exchange scheme based on the difficulty of the ring-LWE problem and proposed cryptographic parameters to achieve the security level of the NIST PQC standardization project. Furthermore, the security of various attack methods against lattice-based cryptography (modulus switching attack, key reuse attack, etc.) was evaluated.

研究分野：暗号理論

キーワード：暗号・認証等　公開鍵暗号　ポスト量子暗号　格子暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

米国標準技術研究所 NIST は、国際会議 PQCrypto2016 においてポスト量子暗号の標準化計画を発表した。暗号方式の標準化において最も重要な研究課題は安全性評価である。鍵長を無限大にした場合の漸近的な安全性証明法はあるが、128 ビット安全性などの固定長の暗号パラメータに対する安全性の厳密評価は重要な未解決問題となっていた。

２．研究の目的

本研究課題では、進展している最新の攻撃手法を踏まえながら想定される攻撃者の解読能力を評価することを目標とし、以下の問題に取り組む。

(1)ポスト量子暗号に対する最新の攻撃手法と攻撃が有効となる範囲を包括的に考察する。
(2)標準化候補に有効な攻撃手法に対して、改良可能性の考察と理論的な限界値を解明する。
(3)計算機解読実験の大量データを外挿することにより安全な暗号パラメータを選定する。

３．研究の方法

格子暗号の安全性評価において必要となる攻撃手法は、次の 5 種類に大別することができる。
1.SVP を用いた SIS 攻撃、2．CVP を用いた BDD 攻撃、3．組合せ論的な BKW 攻撃、
4．多変数多項式による Arora-Ge 攻撃、5．特別なパラメータに対する弱鍵攻撃
本研究課題では、各攻撃が有効となる暗号パラメータ(n,m,q,σ)の適応範囲を考察する。また、各攻撃が持つ数理特性を解析することにより、想定される攻撃限界の境界条件を理論的に求める。更には、各攻撃が有効となる範囲を汎用計算機により実装し、十分な解読実験データの収集と外挿評価により 128 ビット安全性(標準鍵長)を有する格子暗号のパラメータを構築する。

４．研究成果

2017 年度は，格子暗号の安全性の根拠となっている Learning With Errors (LWE)問題に対する困難性を考察した。LWE 問題に対する攻撃として Bounded distance decoding (BDD)攻撃が知られており、CT-RSA 2013 において、Liu-Nguyen は基底をランダム化し Gamma-Nguyen-Regev の extreme pruning を適応した高速化を提案している。2017 年度は、unimodular 行列を用いたランダム化および enumeration の並列アルゴリズムによる高速化、BKZ アルゴリズムのブロックサイズと枝刈り係数の最適化などを考察した。提案並列アルゴリズムは、ACNS2016 の Kirshanova-May-Wiemer の方法と比較して高速化を実現している。

表 1 LWE 問題(次元 n,エラー率α,サンプル数m)の解読実験結果

(n, α)	δ	m	Average pBKZ cost ($\log_2$(secs))	Minimum pBKZ cost ($\log_2$(secs))
(45, 0.005)	1.025	118	5.99	4.28
(50, 0.005)	1.019	144	7.51	6.49
(55, 0.005)	1.017	162	9.03	8.08
(60, 0.005)	1.013	195	13.13	10.62
(65, 0.005)	1.012	213	16.04	14.65

一方、BDD 攻撃を Kannan's embedding により高い次元の格子の unique-SVP に帰着する方法を考察した。Kannan's embedding 攻撃が高速となる、埋め込み係数の大きさ、LWE 問題のサンプル数の大きさ、BKZ アルゴリズムのブロックサイズを考察した（表 1)。これにより、ダルムシュタット工科大が主催する LWE Challenge において、70 次元の LWE 問題を 32.73 シングルコア時間(CPU E5-2697)で解読する世界記録を達成した。最後に、NIST によるポスト量子暗号の標準化計画の動向や多変数多項式暗号および格子暗号の安全性評価方法に関するサーベイ論文を、電子情報通信学会英文論文誌で発表した。

2018 年度は、格子の最短ベクトル問題 SVP に対する高速な解法として、BKZ アルゴリズムの改良を行なった。LLL 簡約基底をノルムの大きさの順序で並び替えることにより、BKZ アルゴリズムで用いる基底列挙法の高速化を検討した。100 次から 120 次元の格子に対して、NTL ライブラリによりブロックサイズβが 15 から 30 の BKZ 簡約基底を求めたところ、提案手法では 40%から 46%程度の確率で短い基底を求めることができた。

また、格子を用いた完全準同型暗号の構成で利用される General Approximate Common Divisors(GACD)問題の困難性を評価した。2014 年に Ding と Tao により提案されたアルゴリズムを改良して、必要されるサンプル数に関する新たな条件式を求めて、計算機実験により有効性を

確認した。更に、格子暗号の IoT ディバスなどの組込み機器での効率性能を評価するために、JavaScript による高速実装を行なった。格子暗号としては Lizard, Kyber, Frodo, および NewHope を選択して、Web browsers, Tessel2, Android の計算環境で高速実装による効率性のデータを得た。

最後に、昨年度に国際会議で発表した、Learning With Errors(LWE)問題の困難性に関する論文をジャーナル論文化した。この論文では、LWE 問題を Kannan's embedding により格子の unique-SVP に帰着する方法に対して、埋め込み係数の大きさ、LWE 問題のサンプル数の大きさ、BKZ アルゴリズムのブロックサイズを考察した。

2019 年度は、ring-LWE 問題の困難性に基づいた効率的な 2 者間鍵交換方式を構成した。2 者間鍵交換方式では秘密鍵を再利用しない ephemeral 乱数が用いられるが、この場合は ring-LWE 問題の解読に必要なサンプル数が 1 個だけとなり、複数のサンプルを用いる通常の ring-LWE 問題より困難な計算問題となる。本研究では、NIST PQC 標準化プロジェクトの安全性レベルを達成する ring-LWE 問題ベースの鍵交換方式に対する暗号パラメータを提案した(表 2)。

表 2：ring-LWE 問題ベースの提案鍵交換方式と他の方式の比較

Name	Type	n	q	Claimed security	Public key (Bytes)	Total (Bytes)
This work	DH	512	120833	AES-128 145-bit	832	1744
	DH	1024	120833	AES-192/256 282-bit	1664	3472
BCNS	DH	1024	$2^{32}-1$	128-bit	4096	8320
NewHope	DH	1024	12289	281-bit	1792	3872
NewHope-Simple	KEM	1024	12289	281-bit	1792	4000
HILA5	KEM	1024	12289	255-bit	1792	3836

更に、低次元の LLL アルゴリズムが最短ベクトルを出力しない条件を考察し、LLL アルゴリズムの出力に対して後処理を行うことにより最短ベクトルに変換できる方法を提案した。また、代表者の高木は、ポスト量子暗号を専門に議論する国際会議 PQCrypto 2019 において招待講演 "Computational Challenge Problems in Post-Quantum Cryptography"を行い、更にはポスト量子暗号の一般向けの入門書「暗号と量子コンピュータ」をオーム社から出版した。

次に、分担者の安田は以下の研究を行った。ポスト量子暗号と期待されている格子暗号の安全性を支える格子問題を解く新しい格子基底簡約アルゴリズムとして、格子基底ベクトルのグラムシュミット長の 2 乗和を効率よく削減する多項式時間計算量の DeepLLL の変種を開発すると共に、その効果を実験的に示した。また、NIST に提案された数多くの格子暗号方式の安全性を支える LWE 問題に対して、LWE の剰余パラメータを変化させる modulus switching を暗号解読に適用した際の影響を理論的かつ実験的に解析した。

2020 年度は、米国標準技術研究所 NIST が進める PQC 標準化プロジェクト第 3 ラウンドの候補暗号となる格子暗号 SABER に関する研究を進めた。SABER は、格子暗号を構成する標準的な LWE 問題の変種となる Learning with Rounding (LWR) 問題の困難性を基にした暗号方式となる。2020 年度は、LWE 問題の解法として知られる Bai-Galbraith 埋込法を LWR 問題に適用した際に構成される格子において、LWE 問題の場合とは異なる最短ベクトルが存在することを示した。また、SABER に対する鍵再利用攻撃を考察して、秘密鍵の各係数を確定的に復元できるクエリの組み合わせを 50 万程度の候補の中から割り出すことで、平均 3103 クエリ程度で秘密鍵を復元できることを示した。これらの結果は、2021 年暗号と情報セキュリティシンポジウム(SCIS 2021)において発表した。

一方、格子暗号 NewHope に対する鍵不一致攻撃を考察して、攻撃者がサーバに送信するクエリの停止条件や秘密鍵となる多項式の係数の判定条件を改良することにより、既存研究よりサーバへのクエリ数を約 52 万と約 42%の削減に成功した。本結果は国際会議 ACSP 2020 において発表した。また、前年度までに研究を進めていた格子簡約アルゴリズムの論文を、ジャーナル論文誌 International Journal of Information Security において発表した。更に、代表者の高木は、NICT サイバーセキュリティシンポジウム 2021 において、招待講演 "耐量子計算機暗号の最新動向" を行った。

５．主な発表論文等

〔雑誌論文〕　計15件（うち査読付論文　14件／うち国際共著　5件／うちオープンアクセス　15件）

１．著者名 Rui Xu, Yeo Sze Ling, Kazuhide Fukushima, Tsuyoshi Takagi, Seo Hwajung, Shinsaku Kiyomoto, Henricksen Matt	４．巻 LNCS 10355
２．論文標題 An Experimental Study of the BDD Approach for the Search LWE Problem	５．発行年 2017年
３．雑誌名 The 15th International Conference on Applied Cryptography and Network Security, ACNS 2017	６．最初と最後の頁 253-272
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-61204-1_13	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Saed Alsayigh, Jintai Ding, Tsuyoshi Takagi, Yuntao Wang	４．巻 LNCS 10418
２．論文標題 The Beauty and the Beasts - The Hard Cases in LLL Reduction	５．発行年 2017年
３．雑誌名 12th International Workshop on Security, IWSEC 2017	６．最初と最後の頁 19-35
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-64200-0_2	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Tsuyoshi Takagi	４．巻 Vol.E101-A, No.1
２．論文標題 Recent Developments in Post-Quantum Cryptography	５．発行年 2018年
３．雑誌名 IEICE Transaction	６．最初と最後の頁 3-11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.3	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Yuntao Wang, Yoshinori Aono and Tsuyoshi Takagi	４．巻 LNCS 10631
２．論文標題 An Experimental Study of Kannan's Embedding Technique for the Search LWE Problem	５．発行年 2018年
３．雑誌名 19th International Conference on Information and Communications Security, ICICS 2017	６．最初と最後の頁 541-553
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-89500-0_47	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名	4．巻
Wang Yuntao, Takagi Tsuyoshi	LNCS 10946
2．論文標題	5．発行年
Improving the BKZ Reduction Algorithm by Quick Reordering Technique	2018年
3．雑誌名	6．最初と最後の頁
23rd Australasian Conference on Information Security and Privacy	787-795
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1007/978-3-319-93638-3_47	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	－

1．著者名	4．巻
Xiaoling Yu, Yuntao Wang, Chungen, Tsuyoshi Takagi	ICISCE 2018
2．論文標題	5．発行年
Studying the Bounds on Required Samples Numbers for Solving the General Approximate Common Divisors Problem	2018年
3．雑誌名	6．最初と最後の頁
5th International Conference on Information Science and Control Engineering	533-537
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1109/ICISCE.2018.00117	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	該当する

1．著者名	4．巻
Yuan Ye, Xiao Junting, Fukushima Kazuhide, Kiyomoto Shinsaku, Takagi Tsuyoshi	Vol. 2018
2．論文標題	5．発行年
Portable Implementation of Postquantum Encryption Schemes and Key Exchange Protocols on JavaScript-Enabled Platforms	2018年
3．雑誌名	6．最初と最後の頁
Security and Communication Networks	1-14
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1155/2018/9846168	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	－

1．著者名	4．巻
Yuntao Wang, Yoshinori Aono, Tsuyoshi Takagi	E101.A
2．論文標題	5．発行年
Hardness Evaluation for Search LWE Problem Using Progressive BKZ Simulator	2018年
3．雑誌名	6．最初と最後の頁
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	2162-2170
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1587/transfun.E101.A.2162	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	－

1．著者名 Yasuda Masaya, Yamaguchi Junpei	4．巻 Vol.87
2．論文標題 A new polynomial-time variant of LLL with deep insertions for decreasing the squared-sum of Gram-Schmidt lengths	5．発行年 2019年
3．雑誌名 Designs, Codes and Cryptography	6．最初と最後の頁 2489-2505
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-019-00634-9	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Jintai Ding, Xinwei Gao, Tsuyoshi Takagi, Yuntao Wang	4．巻 LNCS 11464
2．論文標題 One Sample Ring-LWE with Rounding and its Application to Key Exchange	5．発行年 2019年
3．雑誌名 17th International Conference on Applied Cryptography and Network Security	6．最初と最後の頁 323-343
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-21568-2_16	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Kotaro Matsuda, Atsushi Takayasu, Tsuyoshi Takagi	4．巻 Vol.E102-A
2．論文標題 Explicit Relation between Low-dimensional LLL-reduced Bases and Shortest Vectors	5．発行年 2019年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1091-1100
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1091	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Le Huy Quoc, Mishra Pradeep Kumar, Nakamura Satoshi, Kinjo Koha, Duong Dung Hoang, Yasuda Masaya	4．巻 Vol.14
2．論文標題 Impact of the modulus switching technique on some attacks against learning problems	5．発行年 2020年
3．雑誌名 IET Information Security	6．最初と最後の頁 286-303
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/iet-ifs.2019.0220	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Yuntao Wang, Tsuyoshi Takagi	４．巻 Vol. 20
２．論文標題 Studying lattice reduction algorithms improved by quick reordering technique	５．発行年 2021年
３．雑誌名 International Journal of Information Security	６．最初と最後の頁 257-268
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-020-00501-y	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計11件（うち招待講演　3件／うち国際学会　2件）

１．発表者名 Junting Xiao, Ye Yuan, Kazuhide Fukushima, Shinsaku Kiyomoto, Tsuyoshi Takagi
２．発表標題 Efficient Implementation of discrete Gaussian sampling for Lattice-based Cryptography using JavaScript
３．学会等名 コンピュータセキュリティシンポジウム（CSS2017）
４．発表年 2017年

１．発表者名 井上晶登，齋藤恆和，金城皓羽，高木剛
２．発表標題 モンゴメリリダクションの改良によるNTTの高速化
３．学会等名 2018年暗号と情報セキュリティシンポジウム（SCIS2018）
４．発表年 2018年

１．発表者名 Ye Yuan, Junting Xiao, Kazuhide Fukushima, Shinsaku Kiyomoto, Tsuyoshi Takagi
２．発表標題 Portable implementation of post-quantum encryption schemes and key exchange protocols on JavaScript-enabled platforms
３．学会等名 2018年暗号と情報セキュリティシンポジウム（SCIS2018）
４．発表年 2018年

１．発表者名
Tsuyoshi Takagi

２．発表標題
Recent Developments in Post-Quantum Cryptography

３．学会等名
22nd Workshop on Elliptic Curve Cryptography (ECC 2018)（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
井上晶登，王イントウ，高安敦，高木剛

２．発表標題
少ないサンプル数のLWE問題に対するkannanの埋め込み法の挙動評価

３．学会等名
2019年暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
Junting Xiao, Ye Yuan, Tsuyoshi Takagi

２．発表標題
Parallel Implementation and Comparison of Lattice-based Digital Signature Schemes using JavaScript

３．学会等名
2019年暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
青木大地，福島和英，清本晋作，高木剛

２．発表標題
SubSieveを用いた最短ベクトル問題の求解実験

３．学会等名
2019年暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
高木剛

２．発表標題
量子コンピュータの時代に安全な次世代暗号の標準化動向

３．学会等名
Security Days Spring 2019 Tokyo（招待講演）

４．発表年
2019年

１．発表者名
Tsuyoshi Takagi

２．発表標題
Computational Challenge Problems in Post-Quantum Cryptography

３．学会等名
The Tenth International Conference on Post-Quantum Cryptography　Chongqing University（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
岡田怜士，王イントウ，高木剛

２．発表標題
格子暗号NewHopeに対する鍵不一致攻撃の改良

３．学会等名
2020年暗号と情報セキュリティシンポジウム（SCIS2020）

４．発表年
2020年

１．発表者名
青木大地，福島和英，清本晋作，高木剛

２．発表標題
ユニモジュラ行列による格子基底のランダム化について

３．学会等名
2020年暗号と情報セキュリティシンポジウム（SCIS2020）

４．発表年
2020年

〔図書〕　計1件

１．著者名 高木 剛	４．発行年 2019年
２．出版社 オーム社	５．総ページ数 232
３．書名 暗号と量子コンピュータ ―耐量子計算機暗号入門―	

〔産業財産権〕

〔その他〕

東京大学大学院情報理工学系研究科数理情報学専攻数理情報第1研究室
http://crypto.mist.i.u-tokyo.ac.jp/

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
研究分担者	安田　雅哉 (Yasuda Masaya) (30536313)	立教大学・理学部・准教授 (32686)	

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			
中国	Beijing Jiaotong University	China University of Geosciences	Nanjing University Science Technology	
USA	University of Cincinnati			
Singapore	Institute for Infocomm Research			