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　 ５ 月 ２２ 日現在

機関番号：３２６８６
研究種目：基盤研究(B)（一般）
研究期間：2020～2023
課題番号：２０Ｈ０４１４２

研究課題名（和文）格子暗号の大規模解読実験と解読計算量評価

研究課題名（英文）Large-scale experiments for cryptanalysis of lattice-based cryptography and evaluation of the computational complexity

研究代表者

安田　雅哉（Yasuda, Masaya）

立教大学・理学部・教授

研究者番号：３０５３６３１３

交付決定額（研究期間全体）：（直接経費）　　13,500,000円

研究成果の概要（和文）：格子暗号は量子計算機による解読に耐性を持つと共に、完全準同型暗号などの高機能暗号の構成にも適用可能な次世代暗号技術である。本研究の目的は、格子暗号の安全性を支える最短ベクトル問題などの格子問題に対して、最良の解読アルゴリズムの設計・並列化と大規模な解読実験を行うと共に、その解読計算量を精密に評価することである。本研究では、格子問題の解読に必須の格子基底簡約に対し、世界で初めて分散型かつ非同期な大規模並列化システムの開発に成功した。また、その並列化システムを利用して、SVPチャレンジの解読実験を行い、その平均解読時間を見積もることに成功した。

研究成果の学術的意義や社会的意義
本研究では、耐量子性と高機能性の両方を併せ持つ格子暗号の安全性を支える数学問題に対して、実際の計算機上での解読実験を通して、その解読計算量を評価した。本研究で得られた格子暗号に対する解読技術や解析法は、高性能計算や暗号解析の分野における国際会議や学術雑誌で多数発表した。また、本研究の解読評価により、格子暗号の安全なパラメータ抽出が可能となるため、今後の格子暗号の標準化等の社会活動への貢献が期待できる。

研究成果の概要（英文）：Lattice-based cryptography is a next-generation cryptographic technology that is resistant to cryptanalysis by quantum computers and applicable to the construction of high-functional cryptography such as fully homomorphic encryption. The purpose of this research is to design and parallelize the best algorithms for solving lattice problems such as the shortest vector problem (SVP) that support the security of lattice-based cryptography. We also conduct large-scale solving experiments to estimate the time complexity precisely.In this research, we succeeded in developing the world's first distributed, asynchronous, and large-scale parallelization system for lattice basis reduction, which is essential for solving lattice problems. With the parallelization system, we conducted large-scale experiments for solving instances in the SVP challenge to estimate the average solving time.

研究分野：暗号数理

キーワード：格子問題　最短ベクトル問題　格子アルゴリズム　格子基底簡約　大規模並列化　列挙法　篩法

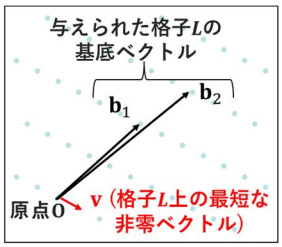
様　式　C－１９、F－１９－１（共通）

１．研究開始当初の背景

近年、量子計算機の実用化に向けた開発競争が世界中で加速している。一方、RSA 暗号や楕円曲線暗号などの現在広く普及している暗号技術の量子計算機による危殆化に備え、2016 年から米国標準技術研究所 NIST は量子計算機に耐性のある「耐量子計算機暗号」の標準化計画を進めている。耐量子計算機暗号の標準化計画に提案されたものとして、「格子暗号」・「符号暗号」・「多変数多項式暗号」・「同種写像暗号」の数学問題を利用した方式がある[NISTIR-8105]。特に、研究開始当初の 2019 年時点で Round2 に進んだ全 26 件の内 12 件が格子暗号に基づく方式で、格子暗号はポスト量子暗号を実現する有力候補と期待されている[NISTIR-8240]。（Round2 に進んだ 12 件の格子暗号方式の分類は右図を参照。）実際、格子暗号の安全性は NP 困難な問題に帰着することが証明されており、理論的に安全性が高いと考えられている。また、他の方式と比べて、公開鍵・秘密鍵・暗号文のサイズが小さく、暗号化・復号の処理も高速である。他方で、格子暗号は暗号化したまま加算や乗算を可能とする準同型暗号などの高機能暗号の構成にも有用である。このように，格子暗号は耐量子性と高機能性の両方を併せ持つ次世代暗号として期待されている。

安全性を支える格子問題		公開鍵暗号・鍵交換（9件）	電子署名（3件）
NTRU問題		NTRU, NTRU Prime	FALCON
LWE問題とその変種	標準LWE	Frodo-KEM	---
	Ring-LWE	NewHope	qTESLA
	Module-LWE	CRYSTALS-KYBER	CRYSTALS-DILITIUM
	LWR	Round5, SABER	---
	他の問題	LAC, Three Bears	---

格子暗号の実用化のためには、古典計算機と量子計算機の両方において現実時間では解読不可となる十分な安全性を持つ鍵長（鍵パラメータ）を選択する必要がある。現在普及している RSA 暗号や楕円曲線暗号の安全性は長期間かけて多角的に検証され十分な強度を持つ鍵長が選択されている。一方、格子暗号に対しては、最良の解読アルゴリズムの開発や大規模な解読実験などによる安全性解析が不十分で、今後の実用化に向けた最重要課題となっている。右上図に示したように、近年提案の格子暗号方式の安全性は NTRU や LWE（Learning With Errors）と呼ばれる数学問題の計算困難性に依存し、それらは最短ベクトル問題（Shortest Vector Problem, SVP）などの古典的な格子問題に帰着され安全性評価される。NTRU や LWE 方式の安全性は SVP の解読計算量から見積もるため、SVP は格子暗号の安全性解析で最も基本的かつ重要な問題である。右図に示すように SVP は次の問題である：「n次元の格子Lを生成する基底$\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$が与えられたとき、格子$L$の最短な非零なベクトル$\mathbf{v}$を見つけよ。」ランダムな格子において SVP は NP 困難で、高次元の問題に対しては古典計算機でも量子計算機でも効率的に解く方法が見つかっておらず、それが格子暗号の安全性の根拠となっている。しかし、格子暗号を実用化するには十分な強度を持つ格子次元などを具体的に選択し、その強度を精密に見積もる必要がある。そのためには、SVP などの格子問題に対する最良の解読アルゴリズムを明らかにし、その解読計算量を精密に評価することが不可欠な研究課題となっている。



２．研究の目的

本研究では、格子暗号の安全性を精密に評価し，十分な強度を持つ鍵パラメータの選択を可能とすることを目的とする。具体的には、次の 2 つの研究課題に取り組む：

① 格子暗号の安全性を支えるSVPなどの格子問題に対し最良の解読アルゴリズムの設計・並列化と大規模な解読実験を行い、想定される攻撃者の計算限界を実験的に見積もる。

② さらに上記で開発した解読アルゴリズムの解読計算量を理論的に解析し、理論と実験の両面から格子暗号の解読計算量を精密に評価する。

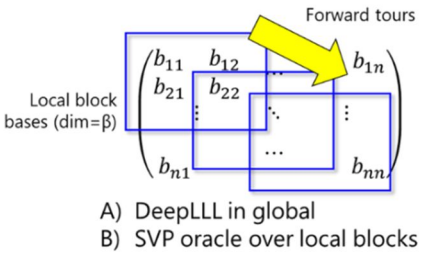
３．研究の方法

格子暗号の安全性を支える数学問題として SVP が最も基本的である。本研究では SVP に対する最良の解読アルゴリズムの開発を行う。SVP に対する既存の解法として、「厳密解法」と「近似解法」がある。厳密解法は全数探索で最短ベクトルを見つけるため、その計算量は格子次元に対して指数的である。一方、代表的な近似解法である LLL は多項式時間で高速だが、近似解しか見つけない。厳密解法と近似解法は互いに補完関係にあり、その最適な組み合わせが重要である。例えば、格子暗号解読の強力なツールである BKZ は厳密解法と近似解法を組み合わせたアルゴリズムで、ブロック化した射影格子で厳密解法を行いながら、全体の基底行列に LLL などの近似解法アルゴリズムを施す。特に、BKZ で SVP の近似解の探索が可能であると共に、厳密解法で最短ベクトルを見つけるのに適した「良い基底」を得ることができる。また、格子暗号の解読計算量の評価として，SVP の求解計算量をベースに算出する Core-SVP と呼ばれる手法が一般的である。具体的には、格子暗号を解読するために必要な SVP オラクルの次元βを評価し、β次元の SVP（SVP-β）の求解計算量を見積もる。Core-SVP を利用することで、SVP-βの計算量を統一基準とした、異なる暗号方式同士の解読計算量比較が可能となる。そこで本研究では、BKZ 型の基底簡約アルゴリズムの大規模並列化システムの開発を主に行う。

４．研究成果

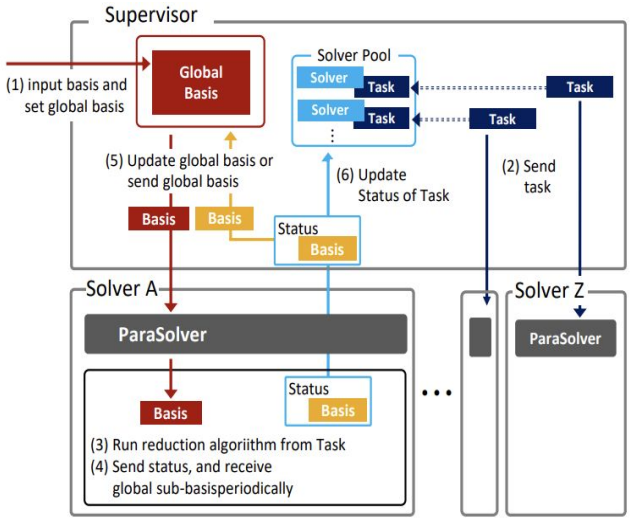
【新しい格子基底簡約アルゴリズムの開発と実装】

まず本研究の始めに、LLL の一般化である DeepLLL を BKZ の枠組みに組み込んだ DeepBKZ 基底簡約アルゴリズムの開発・実装を行った。具体的には、右図に示すように、従来の BKZ アルゴリズム同様にブロック化した射影格子上での最短ベクトルの探索・挿入を行う一方、DeepBKZ では全体の基底行列に対して DeepLLLL を施す。一般に LLL より DeepLLL は良い基底行列を見つけるため、DeepBKZ アルゴリズムは BKZ よりも短い格子ベクトルを見つけることが可能であることを理論的かつ実験的に検証した。また、自己双対型の Self-dual DeepBKZ などの DeepBKZ の亜種アルゴリズムの開発・実装も行い、SVP や LWE・NTRU 問題の求解に適用した。特に、代数構造を持つ Ring-LWE や NTRU の問題の求解については、Kannan の埋め込み法を改良した新しい SVP 帰着法を示した。

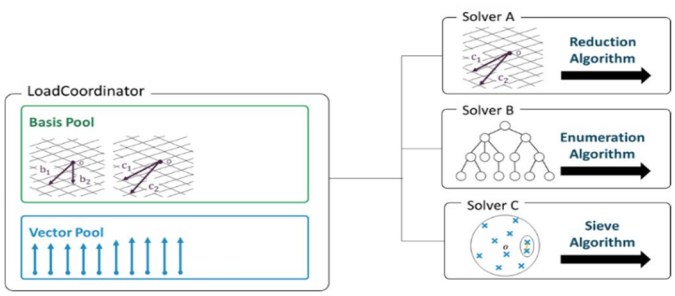


【格子アルゴリズムの大規模並列化システムの開発】

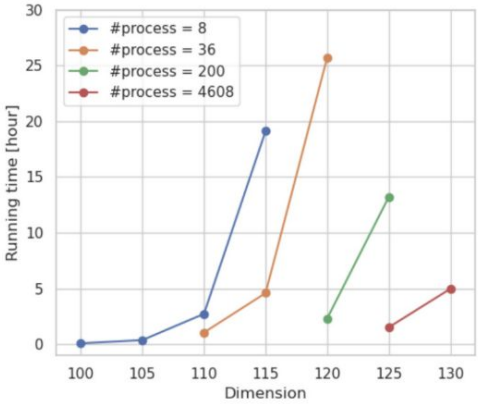
次に、上記で開発した DeepBKZ 基底簡約アルゴリズムの大規模並列化システムを開発した。具体的には、右下図のように、Supervisor-Solver 型の並列化システムで、入力した格子基底行列をランダム化し、ランダム化した同じ格子を生成する基底行列を Solver に分配する。各 Solver は、受け取った基底行列に対して DeepBKZ 基底簡約を行い、基底行列の上位部分（例えば、上位 16 個）の格子ベクトルが更新されるたびに、見つけた短い格子ベクトルを Supervisor に送信する。Supervisor は、各 Solver から受け取った短い格子ベクトルを元に global 基底行列を更新したのち、短い格子ベクトルをすべての Solver に送信する。一方、各 Solver は Supervisor から受け取った短い格子ベクトルを使って、Solver が持つ local 基底行列を DeepBKZ 基底簡約して短い格子ベクトルを探索していく。このように設計した並列化システムでは、各 Solver が独自に基底簡約を行う一方、並列化システム全体でより短い格子ベクトルを見つけるために、Supervisor と Sover の間で非同期に短い格子ベクトルの共有を行い、すべての Solver の基底簡約アルゴリズムの進捗を加速化することが可能である。このように設計した並列化処理の実現のために、分枝限定法に対する汎用的な並列化フレームワーク Ubiquity Generator (UG) を用いて、格子基底簡約の処理において世界で初めての分散型かつ非同期な大規模並列化システム MAP-SVP（Massively Parallel Solver for SVP）の開発に成功した。特に、各 Solver が行う DeepBKZ 基底簡約のサブルーチンとして省メモリ実装が可能な列挙法を採用し、最大 100,032 並列プロセスを持つ大規模計算機上で 130 次元程度の SVP の厳密解をおよそ 100 時間以内で探索可能であることを示した。これらの研究成果は、高性能計算の分野で最高峰の査読付き国際会議 SC’20（International Conference for High Performance Computing, Networking, Storage and Analysis）で発表した。



上記で開発した格子基底簡約アルゴリズムの大規模並列化システム MAP-SVP をベースに、右下図のように、SVP を含む格子問題に対する効率的な求解法である「格子基底簡約(Lattice basis reduction)」・「列挙法（Enumeration)」・「篩法（Sieve)」の異なる 3 種類の格子アルゴリズムを大規模計算機上で同時に動作可能とする並列化フレームワーク CMAP-LAP（Configurable Massively Parallel Solver for Lattice Problems）の開発に成功した。CMAP-LAP の設計・開発・SVP 求解実験結果については、高性能計算分野のトップ査読付き国際会議の 1 つである HiPC2021（High Performance Computing）で発表した。



【大規模並列化システムを利用した SVP チャレンジの求解実験】



上記で開発した格子アルゴリズムの大規模並列化システムを利用して、ドイツ・Darmstadt 公開大学が開催・運営している SVP チャレンジの求解実験を行った。具体的には、並列プロセス数が 8，36，200，4608 の異なる計算機を用いて、SVP チャレンジ求解の平均時間を測定した。特に、各プロセスのメモリ容量が少ない計算機を利用したため、並列化システム内の格子アルゴリズムとして列挙法を採用した。右図にまとめたように、並列プロセス数が 4608 の計算機上では、130 次元（横軸）の SVP チャレンジの近似解の探索に平均 5 時間（縦軸）程度であることを示した。また図から、同じ格子次元に対しては、プロセス数が増大するごとに、SVP の求解時間が短縮されることが分かる。より具体的には、並列プロセス数の比率に応じて、SVP の求解時間が短縮されることから、本研究で開発した並列化システムの並列化効果を実証することに成功した。さらに、同じプロセス数を利用した場合、格子次元が 5 増えるごとに、SVP の求解時間がおよそ 4〜5 倍程度増大することが図から読み取れるので、本実験結果をベースに他の格子次元における SVP の求解時間を見積もることが可能となった。

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　0件／うちオープンアクセス　4件）

１．著者名 Satoshi Nakamura, Nariaki Tateiwa, Masaya Yasuda, Katsuki Fujisawa	４．巻 accepted
２．論文標題 Parallel DeepBKZ 2.0: Development of parallel DeepBKZ reduction with large blocksizes	５．発行年 2024年
３．雑誌名 Mathematical Foundations for Post-Quantum Cryptography	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 オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Satoshi Nakamura, Masaya Yasuda	４．巻 accepted
２．論文標題 Expanded lattices for solving ring-based LWE and NTRU problems	５．発行年 2024年
３．雑誌名 Mathematical Foundations for Post-Quantum Cryptography	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 オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 安田雅哉	４．巻 106
２．論文標題 NIST標準化の格子暗号方式の紹介	５．発行年 2023年
３．雑誌名 電子情報通信学会誌11月号（特集「耐量子計算機暗号の最新動向」における記事）	６．最初と最後の頁 982--987
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 Nariaki Tateiwa, Yuji Shinano, Masaya Yasuda, Shizuo Kaji, Keiichiro Ymamura, Katsuki Fujiwara	４．巻 41
２．論文標題 Development and analysis of massive parallelization of a lattice basis reduction algorithm	５．発行年 2024年
３．雑誌名 Japan Journal of Industrial and Applied Mathematics (JJIAM)	６．最初と最後の頁 13～56
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s13160-023-00580-z	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 Tateiwa Nariaki, Shinano Yuji, Yamamura Keiichiro, Yoshida Akihiro, Kaji Shizuo, Yasuda Masaya, Fujisawa Katsuki	4．巻 －
2．論文標題 CMAP-LAP: Configurable Massively Parallel Solver for Lattice Problems	5．発行年 2021年
3．雑誌名 IEEE, International Conference of High Performance Computing, Data and Analytics (HiPC2021)	6．最初と最後の頁 42～52
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/hipc53243.2021.00018	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 Nakamura Satoshi, Yasuda Masaya	4．巻 304
2．論文標題 Dynamic self-dual DeepBKZ lattice reduction with free dimensions and its implementation	5．発行年 2021年
3．雑誌名 Discrete Applied Mathematics	6．最初と最後の頁 220～229
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.dam.2021.07.035	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 Ikematsu Yasuhiko, Nakamura Satoshi, Yasuda Masaya	4．巻 12835
2．論文標題 A Trace Map Attack Against Special Ring-LWE Samples	5．発行年 2021年
3．雑誌名 International Workshop on Security (IWSEC2021), Springer LNCS	6．最初と最後の頁 3～22
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-85987-9_1	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 Nakamura Satoshi, Yasuda Masaya	4．巻 13129
2．論文標題 An Extension of Kannan's Embedding for Solving Ring-Based LWE Problems	5．発行年 2021年
3．雑誌名 IMA International Conference on Cryptography and Coding (IMACC2021), Springer LNCS	6．最初と最後の頁 201～219
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92641-0_10	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 Yasuda Masaya	4．巻 33
2．論文標題 A Survey of Solving SVP Algorithms and Recent Strategies for Solving the SVP Challenge	5．発行年 2020年
3．雑誌名 Proceedings of MQC 2019 (International Symposium on Mathematics, Quantum Theory, and Cryptography)	6．最初と最後の頁 189～207
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-15-5191-8_15	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 Tateiwa Nariaki、Shinano Yuji、Nakamura Satoshi、Yoshida Akihiro、Kaji Shizuo、Yasuda Masaya、Fujisawa Katsuki	4．巻 -
2．論文標題 Massive Parallelization for Finding Shortest Lattice Vectors Based on Ubiquity Generator Framework	5．発行年 2020年
3．雑誌名 International Conference for High Performance Computing, Networking, Storage, and Analysis (SC20)	6．最初と最後の頁 1～15
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/SC41405.2020.00064	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 Mishra Pradeep Kumar、Rathee Deevashwer、Duong Dung Hoang、Yasuda Masaya	4．巻 30
2．論文標題 Fast secure matrix multiplications over ring-based homomorphic encryption	5．発行年 2021年
3．雑誌名 Information Security Journal: A Global Perspective	6．最初と最後の頁 219～234
掲載論文のDOI（デジタルオブジェクト識別子） 10.1080/19393555.2020.1836288	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 Nakamura Satoshi、Ikematsu Yasuhiko、Yasuda Masaya	4．巻 1262
2．論文標題 Dynamic Self-dual DeepBKZ Lattice Reduction with Free Dimensions	5．発行年 2020年
3．雑誌名 Proceedings of the Sixth International Conference on Mathematics and Computing (ICMC 2020)	6．最初と最後の頁 377～391
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-15-8061-1_30	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 Nakamura Satoshi、Tateiwa Nariaki、Kinjo Koha、Ikematsu Yasuhiko、Yasuda Masaya、Fujisawa Katsuki	４．巻 1262
２．論文標題 Solving the Search-LWE Problem by Lattice Reduction over Projected Bases	５．発行年 2020年
３．雑誌名 Proceedings of the Sixth International Conference on Mathematics and Computing (ICMC 2020)	６．最初と最後の頁 29～42
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-15-8061-1_3	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 Yasuda Masaya、Nakamura Satoshi、Yamaguchi Junpei	４．巻 88
２．論文標題 Analysis of DeepBKZ reduction for finding short lattice vectors	５．発行年 2020年
３．雑誌名 Designs, Codes and Cryptography	６．最初と最後の頁 2077～2100
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-020-00765-4	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 Yasuda Masaya	４．巻 14
２．論文標題 Self-dual DeepBKZ for finding short lattice vectors	５．発行年 2020年
３．雑誌名 Journal of Mathematical Cryptology	６．最初と最後の頁 84～94
掲載論文のDOI（デジタルオブジェクト識別子） 10.1515/jmc-2015-0053	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17件（うち招待講演　7件／うち国際学会　1件）

１．発表者名 高橋康，西田直央，海上勇二，豊永三朗，池松泰彦，縫田光司，安田雅哉
２．発表標題 ハイブリッドStreaming法によるCRYSTALS-Dilithiumのリソース最適化
３．学会等名 暗号と情報セキュリティシンポジウム（SCIS2024）
４．発表年 2024年

１．発表者名
片山瑛，中邑聡史，上野真奈，安田雅哉

２．発表標題
FALCON におけるマスキング実装の提案

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2024）

４．発表年
2024年

１．発表者名
佐藤新，Auzemery Aurelien，片山瑛，安田雅哉

２．発表標題
近似最近ベクトル探索と埋め込み法を用いた格子による素因数分解法の実装報告

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2024）

４．発表年
2024年

１．発表者名
安田雅哉

２．発表標題
格子ベース準同型暗号の応用と格子基底簡約

３．学会等名
研究集会「暗号と量子計算」（東京工業大学）（招待講演）

４．発表年
2023年

１．発表者名
安田雅哉

２．発表標題
格子問題の求解アルゴリズムとその応用

３．学会等名
2023年度東大数理・情報数学セミナー（招待講演）

４．発表年
2023年

１．発表者名
中邑聡史、片山瑛、安田雅哉

２．発表標題
探索Module-LWE問題に対する格子攻撃の実験報告

３．学会等名
2023年暗号と情報セキュリティシンポジウム（SCIS2023）

４．発表年
2023年

１．発表者名
Masaya Yasuda

２．発表標題
Lattice Basis Reduction and Its Application to Cryptanalysis

３．学会等名
Mathematics for Industry in the Asia Pacific Area at SIAM Conference on Computational Science and Engineering (CSE23)（国際学会）

４．発表年
2023年

１．発表者名
安田雅哉

２．発表標題
格子基底簡約とLWE/NTRU問題に対する格子攻撃

３．学会等名
九大IMI共同利用「耐量子計算機暗号と量子情報の数理」（招待講演）

４．発表年
2022年

１．発表者名
安田雅哉

２．発表標題
格子暗号の安全性を支える格子問題の解読法

３．学会等名
東大数理・情報数学セミナー

４．発表年
2022年

１．発表者名
中邑聡史，安田雅哉

２．発表標題
NTRU格子の拡張と格子攻撃

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

４．発表年
2022年

１．発表者名
中邑聡史，安田雅哉

２．発表標題
探索Ring-LWE問題に対するKannanの埋め込み法の拡張

３．学会等名
日本応用数理学会2021年度年会「数論アルゴリズムとその応用」（JANT）セッション

４．発表年
2021年

１．発表者名
安田雅哉

２．発表標題
最短ベクトル問題を解くための格子基底簡約とその大規模並列化

３．学会等名
研究集会「量子暗号理論と耐量子暗号」（早稲田大学・Zoomによるオンライン開催）（招待講演）

４．発表年
2022年

１．発表者名
安田雅哉

２．発表標題
現代の暗号技術を支える数学

３．学会等名
KISTEC教育講座「情報セキュリティ理解のための先端暗号技術入門」（招待講演）

４．発表年
2021年

１．発表者名
安田雅哉

２．発表標題
格子基底簡約とその大規模並列化の紹介

３．学会等名
九大IMI共同利用研究集会「新世代暗号の設計・評価」（招待講演）

４．発表年
2021年

１．発表者名
安田雅哉

２．発表標題
最短ベクトル問題求解に向けた格子基底簡約入門

３．学会等名
RIMS共同研究「準周期的秩序の数理とその周辺」（招待講演）

４．発表年
2021年

１．発表者名
立岩斉明，品野勇治，吉田明広，鍛冶静雄，安田雅哉，藤澤克樹

２．発表標題
最短格子ベクトル問題求解におけるUbiquity Generator Frameworkを用いた大規模MPI並列化

３．学会等名
第176回ハイパフォーマンスコンピューティング研究発表会

４．発表年
2020年

１．発表者名
中邑聡史，安田雅哉

２．発表標題
代数構造を持つ格子上の最短ベクトル探索アルゴリズムの開発

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2021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
研究分担者	鍛冶　静雄 (Kaji Shizuo) (00509656)	九州大学・マス・フォア・インダストリ研究所・教授 (17102)	
研究分担者	藤澤　克樹 (Fujisawa Katsuki) (40303854)	九州大学・マス・フォア・インダストリ研究所・教授 (17102)	
研究分担者	青野　良範 (Aono Yoshinori) (50611125)	国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所・主任研究員 (82636)	

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