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　２ 年　 ６ 月　 ４ 日現在

機関番号：１７１０２
研究種目：基盤研究(B)（一般）
研究期間：2016～2019
課題番号：１６Ｈ０２８３０

研究課題名（和文）LWE問題の解読計算量評価と格子準同型暗号の安全パラメータ設定法の確立

研究課題名（英文）Evaluation of the complexity of solving LWE problems and establishment of setting method of secure parameters for lattice-based homomorphic encryption

研究代表者

安田　雅哉（Yasuda, Masaya）

九州大学・マス・フォア・インダストリ研究所・准教授

研究者番号：３０５３６３１３

交付決定額（研究期間全体）：（直接経費）　　10,800,000円

研究成果の概要（和文）：格子暗号は量子計算機の解読にも耐性を持つと共に，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である．特に，近年提案されたLearning with Errors(LWE)問題ベースの格子暗号は処理性能に優れている．格子暗号の安全性は最短ベクトル問題などの計算量困難性に基づくが，これらの問題はNP困難であり漸近的な計算量しか知られていない．本研究では，最短ベクトル問題やLWE問題を効率的に解くアルゴリズムを開発すると共に，計算機上の求解実験による性能評価を行った．さらに，LWEベースの準同型暗号を実装し，秘匿行列乗算や秘匿統計処理などの応用先における性能を示した．

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合わせ格子暗号の安全性評価を行うと共に，安全なパラメータにおける格子準同型暗号の実装性能を示した．今回得られた格子暗号に対する解読技術や暗号解析法は数多くの著名な国際会議や海外雑誌で出版され暗号分野で非常に高い評価を得ると共に，格子暗号の安全パラメータの抽出が可能となった．また，抽出した安全パラメータを用いて，格子準同型暗号の秘匿行列乗算や秘匿統計処理の具体的な応用先における性能評価を行った．本研究の性能評価により，プライバシー保護利活用技術として格子準同型暗号が実社会で利用可能か判断できるため，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 cryptography that is resistant to quantum computers and is also applicable to construction of high-functional cryptography such as homomorphic encryption. In particular, LWE-based schemes have excellent processing performance. The security of lattice-based cryptography is based on the computational hardness of lattice problems such as the shortest vector problem, but these problems are NP-hard and only known as asymptotic complexity. In this research, we had developed new algorithms to efficiently solve lattice problems such as the shortest vector and the LWE problems, and also evaluated their performance by experiments. Furthermore, we had implemented LWE-based homomorphic encryption schemes and demonstrated the performance in concrete applications such as secure matrix multiplications and secure statistical processing.

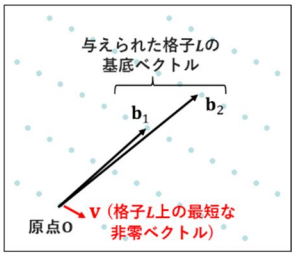
研究分野：数理暗号

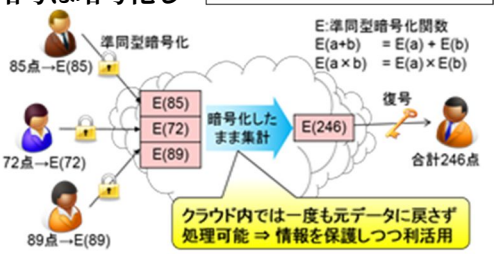
キーワード：格子暗号　最短ベクトル問題　LWE　準同型暗号　格子基底簡約

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

現在普及の RSA 暗号や楕円曲線暗号は，素因数分解や楕円曲線離散対数の問題を利用している．近年世界中で開発競争が加速している大規模な量子コンピュータが実現すると，これらの数学的問題は容易に解けることが[Shor@FOCS1994]によって示されている．一方，格子暗号は格子理論を利用した暗号技術で、その安全性は最短ベクトル問題（右図）などの計算量困難性に基づき，量子コンピュータでも容易に解読できないと期待されている．そのため，格子暗号は耐量子計算機暗号の有力候補として活発に研究されている．2016 年から米国標準技術研究所 NIST が耐量子計算機暗号の標準化を開始して以降，格子暗号が研究の中心になっている．また一方，準同型暗号[Gentry@STOC2009]や multilinear maps[Garg 等@EUROCRYPT2013]などの高機能暗号は格子暗号をベースに構成されている．特に，準同型暗号は暗号化したまま加算や乗算が可能な暗号で，クラウド上のデータを暗号化したまま集計や統計計算などが可能となる（右下図）．近年では，準同型暗号をプライバシー保護データマイニングへ応用する研究開発が産業界でも活発に行われている．（具体的には，IBM・富士通・日立から研究開発に関する報道発表がある．）



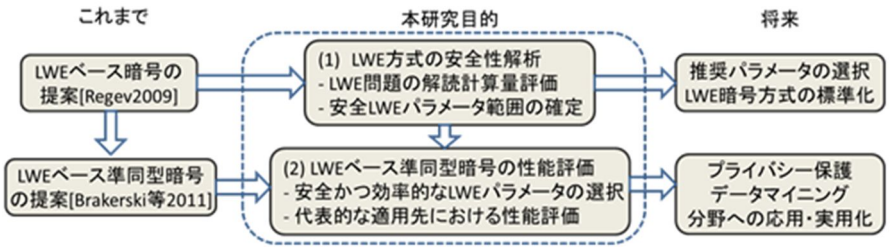


２．研究の目的

上記で紹介したように，格子暗号は耐量子性を持つと共に準同型暗号などの高機能暗号の構成に適用可能で欧米中心に研究が行われている．特に，近年提案された LWE（Learning With Errors）問題ベースの格子暗号は処理性能に優れ，公開鍵暗号の分野で活発に研究されている．格子暗号の安全性は最短ベクトル問題など格子問題の計算量困難性に基づくが，これらの問題は NP 困難であり漸近的な計算量しか知られていない．しかし，暗号を実用化する上では具体的な鍵長を設定し，その際の解読計算量を精密に評価する必要がある．LWE 格子暗号は，次元 n・素数 q・標準偏差 s の LWE パラメータ(n, q, s)から構成される．LWE 格子暗号の安全性は，LWE パラメータ(n, q, s)の各サイズとバランスに依存するため，解読計算量の評価は非常に困難である．そこで，本研究では以下の問題に取り組む．

(ア) 計算機による攻撃実験により，与えられた LWE パラメータに対する LWE 格子暗号の解読計算量を解析し，80-bit・128-bit などの安全性を持つ LWE パラメータ範囲を確定する．

(イ) 80-bit・128-bit 安全な LWE パラメータを用いて LWE 準同型暗号を実装し，準同型暗号の代表的な応用先である秘匿統計処理や秘匿検索に適用した場合の性能評価を行う．



３．研究の方法

本研究では，以下の 2 つの研究課題を解決することを目指す：

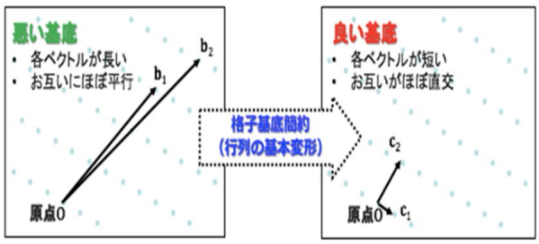
- 【課題 1】LWE 方式の安全性解析
  - LWE 問題に対して代表的な攻撃アルゴリズムを実装し，計算機による攻撃実験結果から，与えられた LWE パラメータ(n，q，s)に対する LWE 問題の解読計算量を評価する．
  - 下記の課題 2 で選択する LWE 準同型暗号方式に対する攻撃実験を行い，暗号方式を実用上安全に利用するために必要な LWE パラメータ範囲を確定する．
- 【課題 2】LWE ベース準同型暗号の試作実装・性能評価
  - 準同型暗号の代表的な応用先である秘匿統計処理や秘匿検索を実現可能とする LWE 準同型暗号方式を選択し，数学処理ソフトを用いたプロトタイプ実装を行う．
  - 上記で確定するパラメータ範囲の中から，処理性能が最速となる LWE パラメータを抽出し，LWE 準同型暗号方式の高速化と秘匿統計や秘匿検索における性能評価を行う．

４．研究成果

【格子基底簡約の開発】

格子暗号の安全性を支える格子問題として最短ベクトル問題（Shortest Vector Problem，SVP）が最も基本的かつ重要である．SVP の解法として「厳密解法」と「近似解法」がある．最短ベクトルの数え上げなどの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 や BKZ などの格子基底簡約は高速だが，近似解しか見つけない．　ただし，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．より具体的には，与えられた格子の任意の基底から，格子基底簡約は各ベクトルが短くかつ互いのベクトルが直交に近い基底に変換する（右図）．

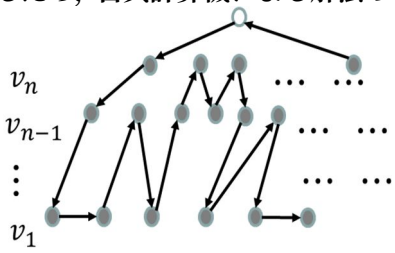


本研究の成果として，LLL の一般化である DeepLLL の高速化を行うと共に，BKZ の枠組みに組み込んだ新しいアルゴリズム DeepBKZ を提案した[1]．特に，Darmstadt 工科大学主催の SVP チャレンジにおける 102～127 の幅広い格子次元に対し，並列化なし汎用計算機上で数多くの記録更新に成功した（右下図）．127 次元の記録は当時の SVP チャレンジの世界ランキングで 14 位であり，並列化なしの計算機環境での結果としては現在も最上位に位置する．特に，既存の BKZ アルゴリズムと比較し，DeepBKZ では小さいブロックサイズで非常に短い格子ベクトルの探索が可能であることを実験的に示した．また，DeepLLL の output quality の解析や変種アルゴリズムの研究開発を行った[2,3,4,5]．また，研究分担者の青野と格子暗号解読に関するテキストを共同執筆した[6]．

Dimension n	Seed	New norm	Root Hermite factor $\gamma^{1/n}$
127	2	2932	1.00834
125	8	2907	1.00840
124	2	2854	1.00832
123	0	2883	1.00847
119	10	2863	1.00868
117	10	2840	1.00880
115	3	2699	1.00841
113	1	2681	1.00857
112	3	2653	1.00866
111	0	2684	1.00874
110	4	2621	1.00859
109	8	2613	1.00863
107	9	2566	1.00866
106	8	2551	1.00868
105	1	2604	1.00897
104	10	2546	1.00884
103	10	2520	1.00882
102	10	2512	1.00889

【最短ベクトルの数え上げ計算量の評価】

上述したように，SVP の厳密解法として最短ベクトルの数え上げアルゴリズムが有用である．最短ベクトルの数え上げでは，右下図のような最短ベクトルの探索木を構築し，そのノード間を効率よく探索する必要がある．主に研究分担者の青野が格子点探索アルゴリズムを用いた場合の計算量の下限を導き，暗号分野におけるトップ国際会議 CRYPTO2018 で発表した[7]．また，その結果を基に格子暗号のパラメータ設定法を開発し，青野が所属する NICT のチーム提案暗号 LOTUS[8]のパラメータを決めた．本方式は NIST が主催する耐量子計算機暗号コンテストへ提出済みである．また，実用的な量子計算機の発展に対応するため，古典計算機による解法のみならず量子計算機による LWE 問題の解法について研究を行った．格子暗号に対する古典計算機による数え上げの計算量を N としたときに，量子コンピュータを用いた場合にそれが共通鍵暗号の場合と同様に $\sqrt{N}$ に落ちるかどうかはパラメータ設定に関する重要な未解決問題であったが，Montanaro や Ambainis-Kokainis の量子木探索アルゴリズムを適用することで $\sqrt{N}$ にまで落ちることを証明した．この結果は暗号分野で著名な国際会議 Asiacrypt 2018 で発表した[9]．これらの結果は国内で非常に高く評価され，複数の招待講演を受けた[10, 11, 12]．



【整数計画法による最短ベクトル問題求解チャレンジ】

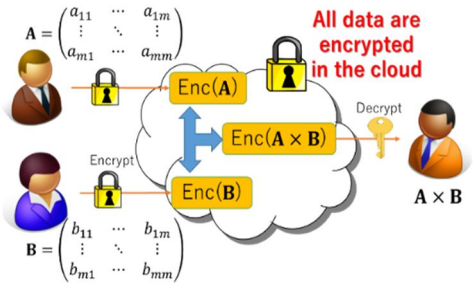
研究分担者の脇と協力して，SVP を整数二次計画問題（Mixed Integer Quadratic Problem, MIQP）に定式化して解読する方法にもチャレンジした．具体的には，格子ベクトルの 2 乗ノルムを目的関数とし，その目的関数を最小化する解を求める最適化問題に変換し，最適化の汎用エンジン CPLEX で解読した実験結果を報告した[13]．特に，ドイツの Darmstadt 大学が公開している SVP チャレンジに対して，CPLEX で解読できる格子次元の限界値を見積もると共に，seed が異なる SVP チャレンジ問題の最小解の散らばり方とその散らばり方による CPLEX の計算時間の違いについて議論した．

【LWE 問題への適用と求解チャレンジ】

LWE 求解用に格子基底に対する双対格子基底を DeepBKZ 基底簡約する双対 DeepBKZ 基底簡約を開発した[3]．特に，逆行列計算を必要とする双対格子基底を直接計算することなく，与えられた格子基底のユニモジュラ基底変換のみで，双対格子基底を DeepBKZ 基底簡約する方法を開発した．また，DeepBKZ 基底簡約と双対 DeepBKZ 基底簡約の有効性を検証するため，2016 年から公開されている LWE チャレンジ問題の解読に適用し，中規模のチャレンジ問題に対する解読時間を報告した（右下図）．また射影格子上の DeepBKZ 基底簡約を新たに開発すると共に，LWE チャレンジ問題に対する求解時間を報告した[14]．さらに，LWE における剰余パラメータを変更する Modulus Switching が LWE 求解として有効になるパラメータの条件を明らかにすると共に，求解に最適な剰余パラメータの選択法を与えた．これは LWR などの LWE 問題の亜種にも適用可能で，LWR 問題に対する求解実験を報告した[15]．

n	α	d	BKZ-20	DeepBKZ [20]	解読時間
40	0.005	120	7 秒	1 秒（$\beta = 20$）	8 秒
	0.010	130	9 秒	13 秒（$\beta = 23$）	22 秒
	0.015	140	15 秒	74 秒（$\beta = 25$）	89 秒
45	0.005	140	13 秒	4 秒（$\beta = 20$）	17 秒
	0.010	140	15 秒	838 秒（$\beta = 28$）	853 秒 $\approx$ 14.2 分
50	0.005	150	18 秒	13 秒（$\beta = 22$）	31 秒
55	0.005	160	19 秒	79 秒（$\beta = 25$）	98 秒
60	0.005	180	34 秒	2,152 秒（$\beta = 26$）	2,186 秒 $\approx$ 36.4 分

【LWE 準同型暗号の開発と応用】



Brakerski-Vaikuntanathan 提案の Ring-LWE 準同型暗号方式を開発する共に，秘匿生体認証[16]・秘匿行列乗算[17]・秘匿統計処理[18]などの応用先に対する高速化と性能評価を行った．（右図は準同型暗号による秘匿行列乗算イメージ．）Ring-LWE の平文空間を定める環 $F_q[x]/(x^n + 1)$上の暗号文を効率的に変換する手法として，SIMD 操作を可能とする CRT 方式[Smart 等@PKC2010], 多倍長データ一括化方式[Lauter 等@CCSW2011]やその拡張である一括内積計算など数多く提案されており，これらの最適な組み合わせにより秘匿計算の高速化を図った．一方，上記の LWE 問題に対する解読実験と解読計算量評価から，80-bit や 128-bit などの異なる安全性レベルを持つ LWE パラメータを抽出し，十分な安全性を持った Ring-LWE 準同型暗号の秘匿生体認証や秘匿統計処理に対する実装性能の結果を示した．

主な論文成果（出版・発表済み情報のみ）

[1] J. Yamaguchi and M. Yasuda, “Explicit formula for Gram-Schmidt vectors in LLL with deep insertions and its applications,” NuTMiC 2017, Springer LNCS 10737, pp. 142—160 , 2017.

[2] M. Yasuda, J. Yamaguchi, “A new polynomial-time variant of LLL with deep insertions for decreasing the squared-sum of Gram-Schmidt lengths,” Designs, Codes and Cryptography, Vol 87, pp. 2489—2505, 2019.

[3] M. Yasuda, J. Yamaguchi, M. Ooka, S. Nakamura, “Development of a dual version of DeepBKZ and its application to solving the LWE challenge,” AFRICACRYPT 2018, Springer LNCS 10831, pp. 162—182, 2018.

[4] M. Yasuda, “Self-dual DeepBKZ for finding short lattice vectors,” MathCrypt 2018. (to appear in a MathCrypt special issue of Journal of Mathematical Cryptology)

[5] M. Yasuda, K. Yokoyama, T. Shimoyama, J. Kogure, and T. Koshiba, “Analysis of decreasing squared-sum of Gram-Schmidt lengths for short lattice vectors,” Journal of Mathematical Cryptology, Vol. 11, pp. 1—24, 2017.

[6] **青野良範，安田雅哉，「格子暗号解読のための数学的基礎：格子基底簡約アルゴリズム入門」，IMI シリーズ：進化する産業数学（第 3 巻），近代科学社，2019 年 9 月出版.**

[7] Y. Aono, P. Q. Nguyen, T. Seito, J. Shikata, “Lower bounds on lattice enumeration with extreme pruning,” CRYPTO 2018, Springer LNCS 10992, pp. 608—637, 2018.

[8] L. T. Phong, T. Hayashi, Y. Aono, S. Moriai, “LOTUS: Learning with errOrs based encryption with chosen ciphertexT secUrity for poSt quantum era,” available at https://www2.nict.go.jp/security/lotus/index.html

[9] Y. Aono, P. Q. Nguyen, Y. Shen, “Quantum lattice enumeration and tweaking discrete pruning,” Asiacrypt 2018, Springer LNCS, 11272, pp. 405—434, 2018.

[10] **青野良範**, Phong Q. Nguyen, **清藤武暢**, **四方順司**, 「Extreme pruning **を用いた格子点探索アルゴリズムにおける計算量の下限について** (from Crypto 2018)」ISEC 2018.**（招待講演）**

[11] **青野良範,「格子ベクトル数え上げアルゴリズムにおける計算量の下限について」**, FIT 2019 **（トップコンファレンスセッション，招待講演）**

[12] Y. Aono. P. Q. Nguyen, Y. Shen, “Quantum lattice enumeration and tweaking discrete pruning (from ASIACRYPT 2018),” WCIS 2019. **（招待講演）**

[13] K. Kimura, H. Waki and M. Yasuda, “Application of mixed integer quadratic program to shortest vector problems”, JSIAM Letters, Vol. 9, pp. 65—68, 2017.

[14] S. Nakamura, N. Tateiwa, K. Kinjo, Y. Ikematsu, M. Yasuda and K. Fujisawa, “Solving the search-LWE problem by lattice reduction over projected bases,” to be presented at ICMC 2020.

[15] L. Q. Huy, M. K. Pradeep, S. Nakamura, K. Kinjo, D. H. Duong and M. Yasuda, “Impact of the modulus switching technique on some attacks against learning problems,” IET Information Security, Vol. 14, No. 3, pp. 286—303, 2020.

[16] M. Yasuda, “Secure Hamming distance computation for biometrics using ideal-lattice and ring-LWE homomorphic encryption,” Information Security Journal: A Global Perspective, Vol. 26, No. 2, pp. 85—103, 2017.

[17] M. K. Pradeep, D. H. Duong and M. Yasuda, “Enhancement for secure multiple matrix multiplications over ring-LWE homomorphic encryption,” ISPEC 2017, Springer LNCS 10701, pp. 320—330, 2017.

[18] R. Deevashwer, M. K. Pradeep and M. Yasuda, “Faster PCA and Linear Regression through Hypercubes in HElib,” ACM WPES 2018, pp. 42—53, 2018.

５．主な発表論文等

〔雑誌論文〕　計15件（うち査読付論文　15件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Yasuda Masaya、Yamaguchi Junpei、Ooka Michiko、Nakamura Satoshi	４．巻 10831
２．論文標題 Development of a Dual Version of DeepBKZ and Its Application to?Solving the LWE Challenge	５．発行年 2018年
３．雑誌名 Springer Lecture Notes in Computer Science	６．最初と最後の頁 162～182
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-89339-6_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 Okumura Shinya、Sugiyama Shingo、Yasuda Masaya、Takagi Tsuyoshi	４．巻 35
２．論文標題 Security analysis of cryptosystems using short generators over ideal lattices	５．発行年 2018年
３．雑誌名 Japan Journal of Industrial and Applied Mathematics	６．最初と最後の頁 739～771
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/s13160-018-0306-z	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、Duong Dung Hoang、Yasuda Masaya	４．巻 11124
２．論文標題 Solving LWR via BDD Strategy: Modulus Switching Approach	５．発行年 2018年
３．雑誌名 Springer Lecture Notes in Computer Science	６．最初と最後の頁 357～376
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-00434-7_18	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 Rathee Deevashwer、Mishra Pradeep Kumar、Yasuda Masaya	４．巻 2018
２．論文標題 Faster PCA and Linear Regression through Hypercubes in HElib	５．発行年 2018年
３．雑誌名 Proceedings of the 2018 Workshop on Privacy in the Electronic Society	６．最初と最後の頁 42～53
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3267323.3268952	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 該当する

1．著者名 Aono Yoshinori、Nguyen Phong Q.、Shen Yixin	4．巻 11272
2．論文標題 Quantum Lattice Enumeration and Tweaking Discrete Pruning	5．発行年 2018年
3．雑誌名 Sprigner Lecture Notes in Computer Science	6．最初と最後の頁 405～434
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-03326-2_14	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 Aono Yoshinori、Nguyen Phong Q.、Seito Takenobu、Shikata Junji	4．巻 10992
2．論文標題 Lower Bounds on Lattice Enumeration with?Extreme Pruning	5．発行年 2018年
3．雑誌名 Springer Lecture Notes in Computer Science	6．最初と最後の頁 608～637
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-96881-0_21	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, Duong Dung Hoang, Yasuda Masaya	4．巻 10701
2．論文標題 Enhancement for Secure Multiple Matrix Multiplications over Ring-LWE Homomorphic Encryption	5．発行年 2017年
3．雑誌名 Information Security Practice and Experience. ISPEC 2017. Lecture Notes in Computer Science, Springer	6．最初と最後の頁 320～330
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-72359-4_18	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 Duong Dung Hoang, Yasuda Masaya, Takagi Tsuyoshi	4．巻 10599
2．論文標題 Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU	5．発行年 2017年
3．雑誌名 Information Security. ISC 2017. Lecture Notes in Computer Science, Springer	6．最初と最後の頁 79～91
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-69659-1_5	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 Yamaguchi Junpei, Yasuda Masaya	4．巻 10737
2．論文標題 Explicit Formula for Gram-Schmidt Vectors in LLL with Deep Insertions and Its Applications	5．発行年 2018年
3．雑誌名 Number-Theoretic Methods in Cryptology. NuTMiC 2017. Lecture Notes in Computer Science, Springer	6．最初と最後の頁 142～160
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-76620-1_9	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 Kimura Keiji、Waki Hayato、Yasuda Masaya	4．巻 9
2．論文標題 Application of mixed integer quadratic program to shortest vector problems	5．発行年 2017年
3．雑誌名 JSIAM Letters	6．最初と最後の頁 65～68
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.14495/jsiaml.9.65	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 29
2．論文標題 Simple Analysis of Key Recovery Attack Against LWE	5．発行年 2017年
3．雑誌名 Mathematical Modelling for Next-Generation Cryptography, Springer	6．最初と最後の頁 221～238
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-10-5065-7_12	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 26
2．論文標題 Secure Hamming distance computation for biometrics using ideal-lattice and ring-LWE homomorphic encryption	5．発行年 2017年
3．雑誌名 Information Security Journal: A Global Perspective	6．最初と最後の頁 85～103
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1080/19393555.2017.1293199	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 Aono Yoshinori, Nguyen Phong Q.	４．巻 10211
２．論文標題 Random Sampling Revisited: Lattice Enumeration with Discrete Pruning	５．発行年 2017年
３．雑誌名 Advances in Cryptology, EUROCRYPT 2017, Lecture Notes in Computer Science, Springer	６．最初と最後の頁 65～102
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-56614-6_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 M. Yasuda, K. Yokoyama, T. Shimoyama, J. Kogure, and T. Koshiba	４．巻 11
２．論文標題 Analysis of decreasing squared-sum of Gram-Schmidt lengths for short lattice vectors	５．発行年 2017年
３．雑誌名 Journal of Mathematical Cryptology	６．最初と最後の頁 1--24
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1515/jmc-2016-0008	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 3.Dung Hoang Duong, Pradeep Kumar Mishra, and Masaya Yasuda	４．巻 67
２．論文標題 Efficient secure matrix multiplication over LWE-based homomorphic encryption	５．発行年 2016年
３．雑誌名 Tatra Mountains Mathematical Publications	６．最初と最後の頁 69--83
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1515/tmmp-2016-0031	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 －

〔学会発表〕　計20件（うち招待講演　2件／うち国際学会　3件）

１．発表者名 Masaya Yasuda
２．発表標題 Self-dual DeepBKZ for finding short lattice vectors
３．学会等名 MathCrypt 2018（国際学会）
４．発表年 2018年

１．発表者名
安田雅哉

２．発表標題
格子暗号の紹介とプライバシー保護利活用技術への応用について

３．学会等名
数学連携ワークショップSociety5.0と数学3～数学と情報セキュリティ研究とのかかわり～（招待講演）

４．発表年
2019年

１．発表者名
中邑聡史，安田雅哉

２．発表標題
DeepBKZ基底簡約アルゴリズムの改良と解析

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
Le Quoc Huy，中邑聡史，金城皓羽，安田雅哉

２．発表標題
Modulus Switchingによる探索LWE/LWR問題の解析とその影響評価

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
安田雅哉

２．発表標題
Deep insertions を用いた格子基底簡約の紹介

３．学会等名
RIMS共同研究（公開型）Computer Algebra--Theory and its Applications 2018

４．発表年
2018年

１．発表者名
中邑聡史，安田雅哉

２．発表標題
DeepLLLの改良とBKZへの組み込みの提案

３．学会等名
日本応用数理学会2018年度年会

４．発表年
2018年

１．発表者名
Pradeep Kumar Mishra, Dung Hoang Duong, Masaya Yasuda

２．発表標題
Secure multiple matrix multiplications via homomorphic encryption

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
山口純平，安田雅哉

２．発表標題
DeepLLL簡約基底の解析とDeepBKZの高速計算方の提案

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
安田雅哉，山口純平，大岡美智子，中邑聡史

２．発表標題
双対版DeepBKZ基底簡約の開発とLWEチャレンジ解読への応用

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
王立華，Pradeep Kumar Mishra，青野良範，Le Trieu Phong，安田雅哉

２．発表標題
Ring-LWEを用いたセキュアな行列乗算のためのパッキング方法

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
山口純平，安田雅哉

２．発表標題
DeepLLLを用いたSVP解読報告

３．学会等名
情報セキュリティ研究会（ISEC），信学技法，vol. 117，no. 125，ISEC2017-23

４．発表年
2017年

１．発表者名
Yoshinori Aono， Phong Q. Nguyen

２．発表標題
Random Sampling Revisited: Lattice Enumeration with Discrete Pruning（from Eurocrypt 2017）

３．学会等名
情報セキュリティ研究会(ISEC)（招待講演）

４．発表年
2017年

１．発表者名
M. Kudo，J. Yamaguchi，Y. Guo and M. Yasuda

２．発表標題
Practical analysis of key recovery attack against search-LWE problem

３．学会等名
International Workshop on Security（IWSEC2016）（国際学会）

４．発表年
2016年

１．発表者名
23.Dung Hoang Duong, Pradeep Kumar Mishra, and Masaya Yasuda

２．発表標題
Efficient secure matrix multiplications using RLWE-based homomorphic encryption

３．学会等名
Central European Conference on Cryptology (CECC2016)（国際学会）

４．発表年
2016年

１．発表者名
山口純平，安田雅哉

２．発表標題
DeepLLLにおけるグラムシュミットベクトル更新の高速化

３．学会等名
2017年暗号と情報セキュリティシンポジウム(SCIS2017)

４．発表年
2017年

１．発表者名
安田雅哉，山口純平

２．発表標題
New Variants of DeepLLL for Decreasing Squared-Sum of Gram-Schmidt Lengths

３．学会等名
2017年暗号と情報セキュリティシンポジウム(SCIS2017)

４．発表年
2017年

１．発表者名
青野良範，清藤武暢，四方順司

２．発表標題
SIS問題の計算量評価

３．学会等名
2017年暗号と情報セキュリティシンポジウム(SCIS2017)

４．発表年
2017年

１．発表者名
Yuntao Wang, Yoshinori Aono, Tsuyoshi Takagi

２．発表標題
Experimental analysis of LWE problem

３．学会等名
2017年暗号と情報セキュリティシンポジウム(SCIS2017)

４．発表年
2017年

１．発表者名
安田 雅哉, 脇 隼人

２．発表標題
整数計画法による格子最短ベクトル探索問題の解読報告

３．学会等名
日本応用数理学会2016年度年会

４．発表年
2016年

１．発表者名
安田雅哉, 横山和弘

２．発表標題
Analysis of Decreasing Squared-Sum of Gram-Schmidt Lengths for Finding Short Lattice Vectors

３．学会等名
信学技法, IEICE Technical Report, ISEC 2016-7

４．発表年
2016年

〔図書〕　計1件

１．著者名	４．発行年
青野 良範、安田 雅哉	2019年
２．出版社	５．総ページ数
近代科学社	216
３．書名	
格子暗号解読のための数学的基礎	

〔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	脇　隼人 (Waki Hayato) (00567597)	九州大学・マス・フォア・インダストリ研究所・准教授 (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セキュリティ基盤研究室・主任研究員 (82636)	