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　４ 年　 ５ 月 ２４ 日現在

機関番号：１４４０１
研究種目：研究活動スタート支援
研究期間：2020～2021
課題番号：２０Ｋ２３３２２

研究課題名（和文）格子暗号の解読アルゴリズムの開発及び解読実験による安全性評価

研究課題名（英文）Study on developing lattice decoding algorithms and cryptanalysis to lattice-based cryptography

研究代表者

王　贇トウ（Wang, Yuntao）

大阪大学・工学研究科・講師

研究者番号：００８８０７９１

交付決定額（研究期間全体）：（直接経費）　　1,600,000円

研究成果の概要（和文）：本研究課題では，耐量子計算機暗号(PQC)の実用化に向けた安全性評価に関する研究を行った．特に，PQCの最有力候補である格子暗号の安全性根拠となる最短ベクトル問題(SVP)の近似版に対して解読アルゴリズムを開発・改良した．そこで，ドイツダルムシュタット工科大学が主催するSVP解読チャレンジにて158次元までの世界記録を達成した．また，格子探索アルゴリズムのENUMと篩法のTuple Sieveを改良し，それぞれの計算量とメモリコストを削減できた．更に，格子暗号のCRYSTALS-KYBERとSABERに対する乱数再利用攻撃の安全性を評価し，クエリ数が6以下で100%の攻撃成功率を得た．

研究成果の学術的意義や社会的意義
本研究課題では，次世代暗号の有力候補である格子暗号の解読アルゴリズムを改良し，スーパコンピュータで大規模解読実験を行い，世界記録を達成した．更に，格子暗号に対する攻撃法を考察することにより，実応用ではよく用いられる「乱数再利用」の安全性評価ができた．本研究課題により，耐量子計算機暗号への解読効率を向上させ，それに応じて頑丈な暗号パラメータの選出に参考できることと，乱数再利用の危機性を示したため学術的かつ実用的な貢献は大きいと考える．

研究成果の概要（英文）：In this research project, we focused on security evaluation for the practical use of post-quantum cryptography (PQC). In particular, we developed and improved several decoding algorithms for the approximation of shortest vector problem (SVP), which is the security evidence for lattice-based cryptography, one of the most promising candidates for PQC. We achieved a world record of 158 dimensions in the SVP decoding challenge organized by the Technical University of Darmstadt, Germany. Furthermore, we also improved ENUM (a lattice search algorithm) and Tuple Sieve (a sieve method) to reduce their computational and memory costs, respectively. In addition, we evaluated the security of random number reuse attacks against the lattice-based CRYSTALS-KYBER and SABER. As a result, we obtained a 100% success rate while the number of queries was less than 6.

研究分野：耐量子計算機暗号

キーワード：格子暗号　解読アルゴリズム　公開鍵暗号　安全性解析

様　式　C－１９、F－１９－１、Z－１９（共通）

1.　研究開始当初の背景

2016年に，アメリカ国立標準技術研究所(NIST)は次世代暗号(PQC)の標準化に向け活動を開始した．現在，数学の研究対象である格子理論を利用した格子暗号が注目され，格子暗号は次世代暗号の有力な候補になると期待されている．そこで，暗号方式の提案から社会展開まで繰り返し安全性解析を行う必要がある．即ち，暗号の安全性を代表的な困難問題に帰着し，この問題の効率的な解法が見つかれば，対象とする暗号方式は効率的に破れるため，より強度が高いパラメータを調整することが安全性評価の目標となる．格子暗号の安全性は，最短ベクトル問題(Shortest Vector Problem，SVP)の近似版などの数学問題の困難性を根拠としている．量子計算モデルにおいて，これらの問題は効率的な解読が不可能と予想されている．しかし，格子暗号は比較的新しく提案された暗号技術であるため，安全性解析が不十分であり，安全なパラメータが決定されておらず実用化には至っていない．格子暗号の安全性を評価するためには，SVPなどの格子問題を解く最適な格子アルゴリズムの開発とその計算量評価が必要である．

2.　研究の目的

本研究課題では，代表的な格子探索アルゴリズム(ENUM)と格子篩法(Sieve)の更なる改良を行い，実装の観点から格子暗号の安全性根拠となる近似SVP問題の計算量を正確に解析することを目指す．特に，ドイツのダルムシュタット工科大学が主催する格子暗号解読コンテストLattice Challengeシリーズの計算世界記録を上回ることで提案アルゴリズムの効率性を示す．

3.　研究の方法

本研究課題では，次世代公開鍵暗号方式として注目されている格子暗号に対する安全性の解析を行う．特に，近似SVPを解く現在最も効率的な簡約アルゴリズムに注目し，格子探索アルゴリズムENUMと格子篩法の改良について研究する．そして，改良したアルゴリズムを用いてクラスターサーバで大規模実験を行い，Lattice Challengeシリーズにおいて世界記録を更新することで、提案アルゴリズムの効率性を示す．また，格子暗号の乱数再利用パラダイムに対した攻撃法を考察し，プロトコルの実応用の観点から安全性を評価し，計算機実験で検証する．

4.　研究成果

本研究課題において主に以下の4つの研究成果がある．

(1)　最短ベクトル問題(SVP)の代表的な求解アルゴリズムとなる格子点探索アルゴリズム(ENUM)が知られている．本研究ではENUMへの入力基底の順序を変更する射影格子と双対格子それぞれの性質を利用したPPRとDPR手法を提案し，ENUMの計算量を削減できた．特に，DPRは45次元格子で探索ノード総数を平均32.8%削減されることが実験から示された(図1)．本研究結果について国内学会SCIS2021で発表を行い，国際会議ICISC2021に採録され，ベストペーパー賞を受賞した．

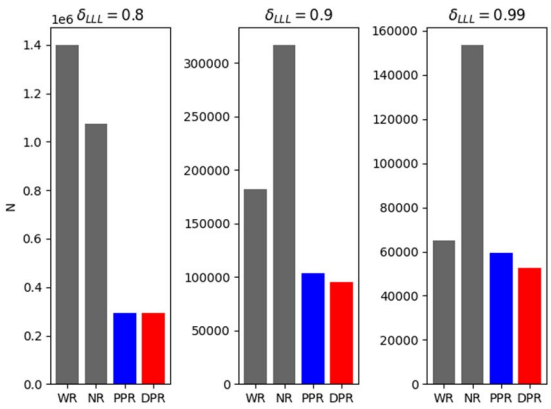
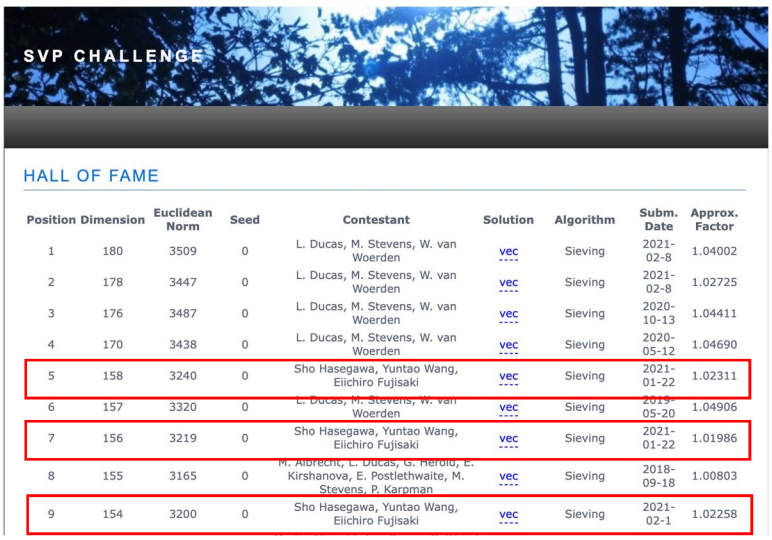


図 1 30 次元において提案手法(PPR, DPR)と従来研究結果(WR, NR)の
探索ノード数の比較

(2) 2019年にAlbrecht等が提案したG6Kアルゴリズムは，SVP Challengeにて180次元の近似最短ベクトルを見つけている．使用時間の制限がある大規模計算機でG6Kを使用する場合，近似最短ベクトルが見つかる前にプログラムが停止し，それまでに計算した解読データが消えてしまうことがある．本研究では，G6Kに保存機能の追加とパラメータの最適値の調整を行った．その結果，SVP Challengeで未解読次元であった154，156，158次元の近似最短ベクトルを見つけた(図2)．本研究結果について第92回CSEC研究会で発表を行った．



Position	Dimension	Euclidean Norm	Seed	Contestant	Solution	Algorithm	Subm. Date	Approx. Factor
1	180	3509	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2021-02-8	1.04002
2	178	3447	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2021-02-8	1.02725
3	176	3487	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2020-10-13	1.04411
4	170	3438	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2020-05-12	1.04690
5	158	3240	0	Sho Hasegawa, Yuntao Wang, Eiichiro Fujisaki	vec	Sieving	2021-01-22	1.02311
6	157	3320	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2019-05-20	1.04906
7	156	3219	0	Sho Hasegawa, Yuntao Wang, Eiichiro Fujisaki	vec	Sieving	2021-01-22	1.01986
8	155	3165	0	M. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. Postlethwaite, M. Stevens, P. Karpman	vec	Sieving	2018-09-18	1.00803
9	154	3200	0	Sho Hasegawa, Yuntao Wang, Eiichiro Fujisaki	vec	Sieving	2021-02-1	1.02258

図2 改良アルゴリズムを用いたSVP Challengeで158次元まで記録を達成した．
(https://latticechallenge.org/svp-challenge/)

(3) さらに，本研究ではSVPの求解アルゴリズムの一つであるTuple Sieve(TS)を並列化したアルゴリズムの提案及び実装を行った．結果としては，42次元において16コアを用いて従来のアルゴリズムであるTSと比べ48倍の高速化を達成したとともにTSの1/2のメモリ空間，並列Gauss Sieveの3/4のメモリ空間を削減することに成功した(図3，図4)．本研究結果は国内学会SCIS2022で発表した．

次元	非並列		並列	
	Gauss Sieve	Tuple Sieve	Gauss Sieve	Tuple Sieve
40	21.4	2393.2	10.2	123.0
42	54.7	12120.1	29.0	278.3

次元	非並列		並列	
	Gauss Sieve	Tuple Sieve	Gauss Sieve	Tuple Sieve
40	21.5	2392.6	29.5	2190.1
42	54.4	12037.4	105.729	5123.8

図3 アルゴリズムの実測時間(左)とCPU時間(右)

次元	非並列		並列	
	Gauss Sieve	Tuple Sieve	Gauss Sieve	Tuple Sieve
40	383.7	291.4	475.1	207.4
42	562.1	501.5	876.7	287.6

図4 アルゴリズムの最大リストサイズ(ベクトルの平均個数)

(4) ProvSec2020でWangらよりmeta-PKEモデルに当てはまる格子暗号に対する乱数再利用攻撃が提案された．この攻撃によって，暗号化を行うBobの秘匿されるべき乱数が再利用された際に，その乱数を復元できることが確認された．本研究では，格子暗号方式のCRYSTALS-KYBERとSABERがmeta-PKEに当てはまることを確認し，それぞれのプロトコルに対してBobの乱数を完全に復元する新たな攻撃手法を提案した．提案の攻撃に必要なクエリ数は6以下となり，成功率は全て100%となった(図5)．本研究成果は国内学会SCIS2021にて発表し，国際会議ProvSec2021で発表した．

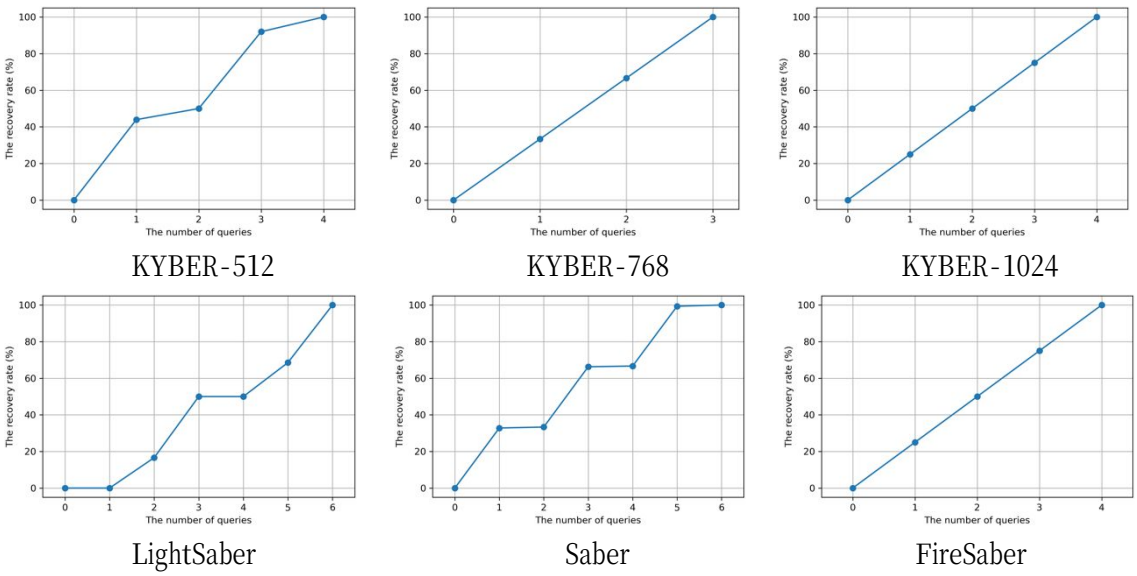


図 5 CRYSTALS-KYBER と SABER 方式に乱数再利用攻撃を適用し、クエリ数が 6 以内に復号率が 100%に達することを示す．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　1件／うちオープンアクセス　0件）

１．著者名 YU Xiaoling、WANG Yuntao、XU Chungen、TAKAGI Tsuyoshi	４．巻 E105.A
２．論文標題 Revisiting the Orthogonal Lattice Algorithm in Solving General Approximate Common Divisor Problem	５．発行年 2022年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 195～202
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021CIP0021	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

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　2件）

〔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			
中国	南京理工大学	太原理工大学		