2021年度共同利用研究報告書

2022年05月06日

所属・職名 大阪大学大学院工学研究科・講師
王 イントウ

		整理番号	20210002	
1.研究計画題目	格子暗号の実用化に向けた研究			
2.新規・継続	新規			
3.種別	若手研究			
4.種目	短期共同研究			
5.研究代表者	氏名	王 イントウ		
	所属部局名	大阪大学大学院工学研究科	職名	講師
6.研究実施期間	2021年11月15日(月曜日)～2021年11月19日(金曜日)			
7.キーワード	量子暗号；耐量子暗号；暗号理論；数論アルゴリズム；情報セキュリティ			
8.参加者人数	94人			

9.本研究で得られた成果の概要

今回の共同研究では格子暗号を中心として、格子暗号プロトコルの設計、格子解読アルゴリズムの解析、安全性評価などの課題をめぐって公開型ワークショップを開催すると共に、非公開の内部討論会を実施した。

最先端の格子暗号技術と解読技術に関する研究成果を踏まえ、耐量子計算機暗号が実応用まで見据えたセキュアな高速実装、および解読アルゴリズムの改良において様々な新しい課題を発掘できた。例えば、大規模並列分散計算に対するベクトルの抽出方法をうまく理論化することができれば、最短ベクトル問題のヒューリスティックアルゴリズムはさらに進化できると思われる。これは今後の課題として展開していく。また、量子コンピュータで離散対数問題を解く際の出力を、格子の性質を用いて補正する方法、およびノイズ耐性のある格子アルゴリズムの開発について議論を行なったが、ビットの反転を反映した形で、距離空間を設計した上で格子アルゴリズムや、符号理論の誤り訂正を導入することでよりうまい補正方法を開発できる可能性があり、引き続き研究を続けていく予定である。さらに、格子暗号に対する安全性評価では、格子解読アルゴリズムの開発・改良・実装が重要な課題となるが、本共同研究では、既存研究の並び替え手法を考察し、最新式のG6K解読アルゴリズムにうまく適用できれば、G6Kの計算量を削減できる可能性を議論し、引き続き今後の課題として取り組んでいくこととなった。

以上、格子暗号の発展のために情報交換と共同作業を行い、非常に実りある共同研究となった。

2021 年九州大学マス・フォア・インダストリ研究所共同利用 若手研究-短期共同研究

“格子暗号の実用化に向けた研究”

(A study on the Application of Lattice-based Cryptography)

成果報告書

目次

1. 実施状況

本事業(若手研究-短期共同研究)は 2021 年 4 月に採択された。その後、6 月に組織委員で zoom オンラインミーティングを行い、共同研究の開催日程、開催形式、内部討論会の講演テーマなどを決定した。また、公開型ワークショップの開催形式、講演者候補の評定・招待、ワークショップの宣伝方法などについては、slack にて随時議論し 8 月末までに決定した。以下では、共同研究の情報、実施期間 2021 年 11 月 15 日(月)～11 月 19 日(金)において行なった内容について簡単に説明する。

組織委員

王　イントウ(代表者)	大阪大学・講師
池松　泰彦	九州大学マス・フォア・インダストリ研究所・助教
深作　亮也	九州大学大学院数理学研究院・助教
青野　良範	情報通信研究機構・テニュアトラック研究員
高安　敦	東京大学大学院情報理工学系研究科・講師
照屋　唯紀	産業技術総合研究所・主任研究員
梶田 海成	日本放送協会 放送技術研究所・研究員
相川　勇輔	三菱電機株式会社 情報技術総合研究所・研究員

アドバイザー

秋山 浩一郎	株式会社東芝 研究開発センター・技監

その他の参加者(内部討論会)

須賀 祐治	株式会社インターネットイニシアティブ・シニアエンジニア
岡田　怜士	東京大学・博士前期課程2年生

プロジェクト概要ウェブサイト:

https://joint.imi.kyushu-u.ac.jp/research-reports/year-2021/

研究実施期間:

2021 年 11 月 15 日(月)～11 月 19 日(金)

公開型ワークショップ参加者数:

計 94 名

公開型ワークショップのウェブサイト:

https://joint.imi.kyushu-u.ac.jp/post-1230/

公開型ワークショップのプログラム:

報告書の末尾に添付する。

1.1 スケジュール:

1 日目(非公開)

組織委員間で自己紹介を行い、本共同研究で焦点を当てる研究内容を確認した。また、公開型ワークショップの準備の進捗、経費使用状況、公開型ワークショップ登録者数について研究代表者より報告した。さらに、共同利用1週間のスケジュール、ワークショップオープンニング用スライド、座長の情報などを確認した。

2 日目(非公開+公開)

午前中は非公開として、青野より量子計算機を使用した Shor の量子解読アルゴリズムに関わる格子問題について解説があった。午後は公開型ワークショップ「新世代暗号の設計・評価」の前半を開催した。(プログラムは本報告書の末尾ページ参照。)

3 日目(非公開+公開)

午前中は非公開として、梶田より耐量子計算機暗号の候補の一つである(SIS 仮定に基づく)格子署名に関して紹介があり、議論を行った。午後は公開型ワークショップの後半を開催した。

4 日目(非公開+公開)

午前は公開型ワークショップの講演スライドを元に出てきた疑問や課題について議論を行った。午後は梶田より Ring-SIS ベース格子署名の構成に関する最新の研究成果の報告があり、議論を行った。また、照屋より格子解読アルゴリズム G6K の GPU 版の実行実験についての現状の解説があった。

5 日目(非公開+公開)

これまでの非公開討論会の議論や公開型ワークショップの内容をまとめた。そして最後に、本共同研究で得た内容を今後どのように公表していくかについて話し合った。

2. 研究背景

ここでは、本共同研究で得た成果を述べるために必要な研究背景について簡単に解説する。

現在の情報社会では、RSA や ECC などの標準暗号方式を使うことで個人情報や通信情報が守られている。RSA と ECC ではそれぞれ素因数分解問題と楕円曲線離散対数問題という数学問題の計算困難性に安全性の根拠が置かれる。しかしながら、Shor の量子解読アルゴリズム[1]により、これらの数学問題は多項式時間で解読されてしまうことが数学的に証明されている。さらに近年、量子計算機が急速に発展していることもあり、量子計算に耐性を持つ次世代計算機暗号の研

究開発は喫緊な課題となっている。実際、2016 年にアメリカ国立標準技術研究所(NIST)は耐量子計算機暗号(PQC)の標準化に向けたプロジェクトを開始した。2020 年の夏に発表された第 3 ラウンドの提案方式 7 件の内、格子理論に関連する計算問題をベースとした格子暗号は 5 件となっている。そのことからもわかるように、格子暗号は耐量子計算機暗号の最有力候補と期待されており、国内外で幅広く研究されている。

2.1 格子の定義

格子はm次元の規則的な網目の交点の集合であり、図 1 のように記述できる幾何的な対象であり、n個線形独立なベクトル$\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$の整数係数の線形結合全体の集合

$L = L(\mathbf{b}_1, \dots, \mathbf{b}_n) := \{\sum_{i=1}^{n} v_i \mathbf{b}_i \in \mathbb{R}^m \mid v_i \in \mathbb{Z}^n\}$

として定義される。格子Lを生成する線形独立なn個のベクトルの組$\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$を基底と呼び、整数$n$を階数、$m$を次元と呼ぶ。特に$m = n$のとき、格子は完全階数であると言う。

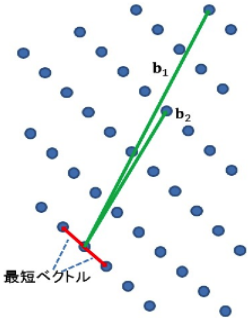


図 1. 2 次元格子の例と最短ベクトル問題

2.2 格子問題

格子を使った基本的な計算問題は、下(2.2.1)で述べる最短ベクトル問題(SVP)であり、これは NP 困難であることが知られ、近似最短ベクトル問題は格子暗号の安全性の根拠として利用されている。暗号の構成において SVP は基本となる数学的問題であるが、さらにそれに関連する問題として Learning with Errors (LWE)問題やその多項式環バーションの Ring-LWE 問題[2]、Ring-SIS 問題[3]などがあり、さまざまな暗号プロトコルで扱われている。

2.2.1 最短ベクトル問題(SVP)

n次元格子$L \subseteq \mathbb{Z}^n$ の基底$\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$が与えられた時、最も短い非零ベクトル$\mathbf{v} \in L$を見つける問題が最短ベクトル問題である(図 1)。

2.2.2 Ring Learning With Errors (Ring-LWE) 問題 [2]

近年、格子理論においては Ring Learning with Errors (Ring-LWE)問題が注目されている。その理由として、Ring-LWE 問題をベースとする暗号は高い効率性と強い安全性を備えており、実用的な耐量子計算機暗号として有望視されているからである。Ring-LWE 問題を説明する。まず、qを素数、$\mathbb{Z}_q$をqを法とする整数の剰余環、多項式$f(x) = x^n + 1$の対する剰余環を$R_q = \mathbb{Z}_q[x]/(f(x))$とする。また、$D_{\mathbb{Z},\sigma}$を$\mathbb{Z}$上の標準偏差$\sigma$の(離散)確率分布とし、$D_{\mathbb{Z}^n,\sigma}$は係数を$D_{\mathbb{Z},\sigma}$から一様ランダムにサンプルされる$R_q$上の多項式の分布とする。このとき、一様ランダムにサンプル

される多項式$\mathbf{a} \in R_q$と$\mathbf{s} \in R_q$と、$D_{\mathbb{Z}^n,\sigma}$からランダムにサンプルされるエラー多項式$\mathbf{e} \in R_q$によって組$(\mathbf{a}, \mathbf{b} := \mathbf{as} + \mathbf{e}) \in R_q \times R_q$が与えられたとき、秘密多項式$\mathbf{s} \in R_q$を求める問題をRLWE 問題と呼ぶ。図 2 では Ring-LWE 問題に基づく暗号方式の例を挙げる。

公開鍵	$(a, b = a \cdot s + e) \in R_q \times R_q$, $R_q = \mathbb{Z}_q[x]/\Phi_m(x)$.
秘密鍵	秘密多項式$s \xleftarrow{\$} \chi$; 小さいエラー $e \xleftarrow{\$} \mathcal{D}_\sigma$. 分布$\chi = \mathcal{D}_\sigma$も可

暗号化：

ダミー $e_1, e_2, e_3 \xleftarrow{\$} \mathcal{D}_\sigma$をサンプルし,
暗号文$c = (c_1, c_2) = (e_1 a + e_2, e_1 b + e_3 + m \cdot \lfloor q/2 \rfloor)$

復号：

$m' = -c_1 s + c_2 = (e_1 e - e_2 s + e_3) + m \cdot \lfloor q/2 \rfloor$
$(e_1 e - e_2 s + e_3)$が小さいことを利用し，mを復元.

図 2　Ring-LWE ベース暗号方式の一例. $\Phi_m(x)$は円分多項式とし, $R_q[x]$は$\Phi_m(x)$を法とした多項式環$\mathbb{Z}_q[x]$の剰余環とする. $\mathcal{D}_\sigma$は標準偏差σである確率分布とする.

2.2.3 Ring Short Integer Solution 問題(Ring-SIS) [3]

R_q上n個の一様ランダムな多項式$\mathbf{a}_1, \dots, \mathbf{a}_n \xleftarrow{\$} R_q$をサンプルする。このとき、$\sum_{i=1}^{n} \mathbf{a}_i \mathbf{x}_i = \mathbf{0}$を満たすノルム上限付きの$n$個の多項式$\mathbf{x}_1, \dots, \mathbf{x}_n$ $(\|\mathbf{x}_i\| \leq \beta)$を探す問題を Ring Short Integer Solution 問題(Ring-SIS)という。

2.3 格子解読アルゴリズム

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。そこで、条件を緩くした近似 SVP と呼ばれる問題を解くアルゴリズムを使用し、暗号の安全性評価を行っている。近似 SVP を解くアルゴリズムは「**基底簡約アルゴリズム**」と「**格子点探索アルゴリズム**」の二つに大きく分けてることができる。近似 SVP や LWE 問題などの問題はその計算困難性の評価を目的とした、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”や“LWE Challenge”などがある[3]。

実用的な基底簡約アルゴリズムとしては、例えば、LLL 簡約アルゴリズム[5]が 1982 年に提案され、多項式時間計算量 $O(n^6 \cdot \log B)$ で高確率で近似 SVP を解くことができる（ただし、nは格子の次元であり、Bは与えられた基底ベクトルのなかの最も大きいノルムである)。しかしこれは、次元が高くなるにつれ近似 SVP を解く確率が低くなる。そのため、LLL アルゴリズムと計算量が$2^{O(n^2)}$である格子点列挙法(ENUM)とを組み合わせた BKZ 簡約アルゴリズムが提案されている[6]。その後、格子簡約アルゴリズムの改良・開発に関して様々な結果が報告されている[7]。

一方、代表的な格子点探索アルゴリズムは上記の ENUM の他、2001 年に Ajtai らが提案した格子篩法(Sieve)がある[8]。Sieve の時間計算量は$2^{O(n)}$であり ENUM より高速だが、空間計算量も$2^{O(n)}$となる。さらに、2010 年には、Micciancio らによって改良版である GaussSieve[9] が提案され、様々な改良や実装により SVP Challenge で記録が更新されていった。2018 年には、Ducas により SubSieve アルゴリズムが提案された[10]。さらに、2019 年には、Albrecht らにより、SubSieve アルゴリズムのメカニズムを利用した General Sieve Kernel アルゴリズム(G6K)[11]が提案され、2021 年 3 月時点の SVP Challenge にて 180 次元の近似最短ベクトルを見つけている。

3. 本共同研究の目的

格子暗号は現在の RSA、ECC と比べて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、安全なパラメータの決定が困難であることから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。本共同研究の目的は、耐量子計算機暗号のさらなる発展のために、新たな格子暗号方式・署名方式の設計、格子問題の解析によるパラメータ評価、高速実装などを行うことである。本共同研究では、格子暗号の発展動向を踏まえて以下の課題に取り組むために、内部討論会と公開型ワークショップを開催した。

①NIST PQC 標準化第3ラウンドに入るものを含めて既存の格子暗号方式に利用された困難問題を融合した新しい暗号プロトコルの設計と評価

②格子篩法と基底簡約アルゴリズムの実験的、理論的計算量評価の解析

③数論アルゴリズムや並列計算などによる暗号方式や上記格子アルゴリズムの高速実装

格子暗号に焦点を当て共同研究を推進することにより、来たる量子情報社会でも安全に使用できる耐量子計算機暗号を構築することを目指す。

4. 研究内容と研究成果

内部討論会では、格子暗号を中心として、格子暗号プロトコルの設計、格子解読アルゴリズムの解析、安全性評価などについて組織委員から講演してもらい、提起した課題に取り組んだ。一方、公開型ワークショップでは産・学・官からの参加登録者が 90 名超え、想定以上の聴講者を集めることができた。そこでは、量子鍵配送と格子暗号に関する研究の最新動向が講演され、内部討論会で行う課題の発掘を行った。各講演に対しては、参加者から多くの質問があり、活発な議論がなされ、非常に有意義なワークショップとなった。

以下では本共同研究で実施した研究内容と得た研究成果について、公開型ワークショップと内部討論会に分けて述べる。

4.1 公開型ワークショップ

ワークショップ現場の様子

4.1.1 量子鍵配送技術の発展について

「超長期セキュア分散ストレージシステム　量子セキュアクラウドの紹介」

藤原 幹生（NICT 量子 ICT 研究室・室長）

まず、情報通信研究機構量子 ICT 研究室の藤原室長より量子暗号技術の発展状況に関して紹介して頂いた。量子鍵配送(QKD)は離れた二者間で乱数を共有できる情報理論的に安全な技術である。QKD と Vernams's one time pad 暗号を組み合わせることにより、情報理論的に安全なデータ伝送が可能となる。しかしながら、QKD では情報媒体が単一光子であり、チャネルの損失の影響を強く受けるため、ファイバでの伝送距離は 50～100km 程度となっている。サービス範囲の拡大のためには信頼できる局舎(trusted node)を介し、鍵リレーが実施されなくてはいけない。QKD をネットワーク化し、さらに分散ストレージの機能を持たせたものを"量子セキュアクラウド"といい、その機能の充実化が現在行われている。本講演において**量子セキュアクラウドの様々な応用例を紹介して頂き、将来展望について述べられた。**

4.1.2 格子暗号プロトコルの設計・実装について

「Optimizing Lattice-based Cryptography」

Chitchanok Chuengsatiansup（The University of Adelaide・講師）

「A New Simple Technique to Bootstrap Various Lattice Zero-Knowledge Proofs to QROM Secure NIZKs」

勝又 秀一（AIST サイバーフィジカルセキュリティ研究センター・主任研究員）

格子暗号プロトコルの設計および実装に関してアデレード大学の Chitchanok 講師と産業技術総合研究所の勝又主任研究員より講演を行なって頂いた。格子暗号は、量子コンピュータの計算能力に耐えるだけでなく、完全準同型暗号などの高機能な暗号方式を構築できる。そのうえ、基本演算がシンプルな行列の乗算であることが主な利点となる。一方、格子暗号の理論的な構築は

可能だが、物理的なデバイスの制約などにより、実用的な実装につなげることは容易ではない。さらに、実装を助けるハードウェアの利点もあるが、数学的モデルには反映されてない。特に、Chitchanok 講師の講演では、実装の観点から格子暗号アルゴリズムの最適化について解説して頂いた。また、暗号攻撃とその対策（ソフトウェアサイドチャネルなど）についても言及がなされた。そこで、デバイスの計算能力や計算モデルの設計の制限により、**格子暗号プロトコルは実応用まで効率性と安全性を配慮しつつ実装の最適化がまだまだ重要な課題であることがわかった**。

4.1.3 格子解読アルゴリズムの大規模並列化について

「格子基底簡約とその大規模並列化の紹介」

安田 雅哉（立教大学・准教授）

立教大学の安田准教授から大規模分散計算による格子解読実験の結果に関して解説して頂いた。格子暗号の本質的な安全性は近似最短ベクトル問題や近似最近ベクトル問題などの格子問題の計算量困難性に依存している。一方、任意の与えられた格子基底から、各ベクトルが短くかつ互いに直交に近い基底にユニモジュラ変換する格子基底簡約アルゴリズムは格子問題を効率的に解く強力なツールである。本講演では、代表的な格子基底簡約アルゴリズム(deep-LLL、deep-BKZ)を紹介すると共に、その大規模並列化アプローチと最短ベクトル問題に対する求解実験結果について紹介して頂いた。安田准教授のスーパーコンピュータを使った大規模並列アルゴリズムでは複数の簡約アルゴリズムを同時に走らせる必要があり、そのために各ノード間で短いベクトルの情報を共有しているとのことであるが、これが簡約型と格子篩法(Sieve)型のハイブリッドの自然な実現になっているのではないかと思われる。このことに関して、このアルゴリズムが簡約型と格子篩法(Sieve)型のハイブリッドの自然な実現になっているのではないかとの意見があり、**この点を理論的に説明する方法を見つけることで、最短ベクトル問題のヒューリスティックアルゴリズムをさらに進化させられる可能性があり、今後の課題として取り組むこととなった**。さらに、大規模分散計算で得たベクトルに対し、長さだけでなく、ベクトルの角度も考慮した抽出方法を見つけることができれば、さらなる簡約アルゴリズムの改良が期待できる。

4.1.4 鍵回復攻撃・サイドチャネル攻撃・故障利用攻撃

「格子暗号への平文・鍵確認オラクルを用いた鍵回復攻撃とサイドチャネル攻撃・故障利用攻撃」

草川 恵太（NTT 社会情報研究所・研究員）

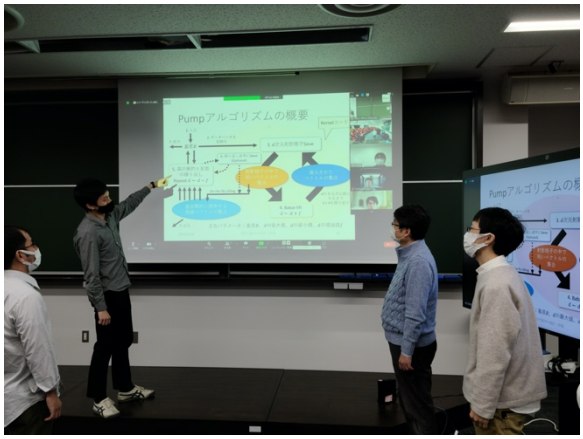
「Misuse シナリオにおける格子暗号への秘密鍵・乱数復元攻撃」

岡田 怜士（東京大学・博士前期課程）

最後に、NTT 社会情報研究所の草川研究員と東京大学の修士 2 年生の岡田氏より鍵再利用攻撃やサイドチャネル攻撃などを用いた格子暗号の安全性評価に関して講演を行なって頂いた。NIST PQC 標準化において格子ベースの KEM（CRYSTALS-Kyber、NTRU、CRYSTALS-Saber、

FrodoKEM、NTRU Prime）が標準化候補として残っている。草川研究員の講演では、各 KEM に対する平文・鍵確認オラクルを用いた鍵回復攻撃をサーベイして頂いた。また ARM Cortex-M4 のベンチマークである pqm4 フレームワーク上での実装に対して故障利用攻撃やサイドチャネル攻撃を用いることで平文・鍵確認オラクルを実現出来ること紹介して頂いた。岡田氏の講演では、鍵を再利用するシナリオで CRYSTALS-Kyber と Saber については Bob の公開しないエラー乱数をそれぞれ高々4、6 クエリで復元する新たな攻撃手法を解説してもらった。この攻撃は、全ての攻撃手法において復元成功率 100%を実現している。**これらの鍵再利用の仮定に基づいた攻撃に関して内部討論会で組織委員で議論し、攻撃ではサーバ側は一定数の誤請求に対する防御対応してない特定なケースと見做し、サーバ側は適切な遮断防御機能を起動すればその攻撃に回避できるという結果を得た。**また、草川氏に説明頂いた、実装プログラムの一部をスキップすることで脆弱性を生み出す Fault-Injection 攻撃およびサイドチャネル攻撃に関しては、**プログラムの並列実行やプログラムスキップを予め想定した構成にする必要があり、現実では対処に難しいことが分かった。**

4.2 内部討論会



内部討論会の様子

内部討論会では、青野、梶田、照屋が、それぞれ量子計算における格子問題、格子署名方式、解読アルゴリズムに関して発表し、課題を提起した。そして、組織委員とゲスト(須賀、岡田)と共にそれら課題の解決に以下のように取り組んだ。

4.2.1 量子コンピュータで Shor のアルゴリズムを動かした後の後処理で出てくる格子問題について

青野　良範(情報通信研究機構・テニュアトラック研究員)

情報通信研究機構の青野研究員が Shor の量子解読アルゴリズムを用いて離散対数問題を解く際の後処理で出てくる格子の最短ベクトル問題について発表を行った。量子コンピュータの出力にノイズが含まれない場合には通常の格子アルゴリズムを用いることで正しい解が非常に高い

確率で出力されることが、ヒューリスティックな仮定の上で証明されている。一方で、現在の量子コンピュータの出力はノイズを多く含んでおり、そのようなデータを格子アルゴリズムに入力しても正解を得る確率は高くはならない。**本発表において、量子コンピュータの出力を、格子の性質を用いて補正する方法、およびノイズ耐性のある格子アルゴリズムの開発について議論を行った。**そのうえ、**ビットの反転を反映した形での距離空間を設計した上での格子アルゴリズムや、符号理論の誤り訂正が使えるのではないかとのアイディアが出され、青野と共に今後のテーマとして研究を続けていくこととなった。**

4.2.2 SIS 仮定/RSIS 仮定に基づく署名について

梶田 海成(日本放送協会 放送技術研究所・研究員)

国際会議 PKC2010 と ASIACRYPT2016 にて Boyen らより提案された SIS ベース署名と、CRYPTO2014 にて Ducas らより提案された Ring-SIS ベース署名について梶田研究員から解説があり、さらに、梶田らが ProvSec2020 にて提案した Ring-SIS ベース署名[12]について紹介された。格子署名方式は大きく二つのカテゴリに分けられる:(1) Hash-and-sign のパラダイムに従い、トラップドアとする GPV サンプリング[13]を使用し、鍵の基底を生成する。これらの方式はコンパクトで計算が速く、出力が小さいことが利点である。一方、パラメータの制限があり、高速実装が難しいところが実用化には比較的不向きであると考えられている。また、サイドチャネル攻撃に耐性を持たないことも欠点の一つである。(2)もう一つのカテゴリとしては、Fiat-Shamir のフレームワークに従い、rejection sampling などのテクニックを適用して格子署名方式を構成するものである。これらの署名方式はより広いパラメータセットを利用できることと、高速実装がシンプルであり、サイドチャネル攻撃に耐性を持つなど様々な利点を持っている。ところが、rejection sampling の計算でより時間かかることと、署名長がより大きいことが欠点だと考えられる。

共同研究では、**Hash-and-sign 署名で用いるトラップドア関数の構成を考察し、安全性評価を行った。**特に、**標準モデルは効率が悪いため、安全性を保ちながら効率性を向上できるランダムオラクルモデル(ROM)と量子ランダムオラクルモデル(QROM)の利用の必要性について議論を行った。**さらに、**パラメータ評価方法について王から解説があった。議論を受けて引き続き梶田と共に提案方式[12]および Hash-and-Sign 署名におけるパラメータ評価方法を研究していく。**

4.2.3 格子解読アルゴリズム G6K の GPU 拡張について

照屋 唯紀(産業技術総合研究所・主任研究員)

産業技術総合研究所の照屋主任研究員が格子解読アルゴリズムの実装である G6K の GPU 拡張を ABCI(大規模 AI クラウド計算システム)上で実行した結果について報告を行った。G6K はいくつかのアルゴリズムの実装モジュールとそれらを組み合わせて構成されたいくつかのソルバーからなる。そのうち、簡約アルゴリズムと Sieve アルゴリズムを組み合わせたモジュールが主要なものであり、近似最短ベクトル問題を高速に解くソルバーの核として利用されている。ダルムシュタッ

ト工科大学がホストしている SVP Challenge の世界記録を見ると、簡約型アルゴリズムは Sieve 型のアルゴリズムを使用している G6K の記録に大きく水をあけられている状況である (https://www.latticechallenge.org/svp-challenge/halloffame.php)。それは近年の計算機がメモリを大量に搭載していることに加えて、一度見つけたベクトルの情報を再利用しているという面が大きいと考えられる。そこで、王から格子基底ベクトルの順序を並び替えることで格子探索アルゴリズム ENUM の効率を向上できるという研究成果[14]を紹介した。この並び替え手法は、基底ベクトルを並べ替えても格子の体積が変わらない性質を利用し、双対基底も利用して射影ベクトルの長さでベクトルを並び替えて ENUM に入力する手法である。[14]の実験結果によると、45 次元の格子に対して ENUM の計算量が平均 32.8%削減することができた。この**並び替え手法が Sieve か G6K に適用できるのか検討し、今後の研究課題としてあげた。**本研究では、**ベクトルの射影ベクトルの長さやベクトル間の角度により Sieve 内のサブルーチンへの入力順序を並び替え、最終的に計算量を削減できる可能性があると考える。**本課題については照屋と王は研究を続けていく。

5 まとめ

今回の共同研究では格子暗号を中心として、格子暗号プロトコルの設計、格子解読アルゴリズムの解析、安全性評価などの課題をめぐって公開型ワークショップを開催したと共に、非公開の内部討論会を実施した。

最先端の格子暗号技術と解読技術に関する研究成果を踏まえ、耐量子計算機暗号が実応用まで見据えたセキュアな高速実装、および解読アルゴリズムの改良において様々な新しい課題を発掘できた。例えば、大規模並列分散計算に対するベクトルの抽出方法をうまく理論化することができれば、最短ベクトル問題のヒューリスティックアルゴリズムはさらに進化できると思われる。これは今後の課題として展開していく。また、量子コンピュータで離散対数問題を解く際の出力を、格子の性質を用いて補正する方法、およびノイズ耐性のある格子アルゴリズムの開発について議論を行なったが、ビットの反転を反映した形で、距離空間を設計した上で格子アルゴリズムや、符号理論の誤り訂正を導入することでよりうまい補正方法を開発できる可能性があり、引き続き研究を続けていく予定である。さらに、格子暗号に対する安全性評価では、格子解読アルゴリズムの開発・改良・実装が重要な課題となるが、本共同研究では、既存研究の並び替え手法を考察し、最新式の G6K 解読アルゴリズムにうまく適用できれば、G6K の計算量を削減できる可能性を議論し、引き続き今後の課題として取り組んでいくこととなった。

以上、格子暗号の発展のために情報交換と共同作業を行い、非常に実りある共同研究となった。

6 謝辞

本共同研究の開催に支援頂いた九州大学マス・フォア・インダストリ研究所に深くお礼申し上げる。

(以上)

参考文献:

[1] P.W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring”, In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, IEEE Computer Society, 1994.

[2] V. Lyubashevsky, C. Peikert, O. Regev, “On ideal lattices and learning with errors over rings”, In proceedings of EUROCRYPT 2010, pp. 1-23, Springer, 2010.

[3] C. Peikert, A. Rosen, “Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices”, In: Proc. TCC 2006, vol. 3876 of LNCS, pp. 145-166, Springer, 2006.

[4] SVP Challenge, available at https://www.latticechallenge.org/ svp-challenge/.

[5] A. K. Lenstra, H. W. Jr. Lenstra and L. Lovász, “Factoring polynomials with rational coefficients”, Math. Ann., vol. 261, no. 4, pp. 515–534, 1982.

[6] C. P. Schnorr and M. Euchner, “Lattice basis reduction: improved practical algorithms and solving subset sum problems”, Math. Program., vol. 66, no. 1–3, pp. 181–199, 1994.

[7] Y. Chen and P. Q. Nguyen, “BKZ 2.0: Better lattice security estimates”, Asiacrypt 2011, LNCS, vol. 7073, pp. 1–20, 2011.

[8] M. Ajtai, R. Kumar, and D. Sivakumar, “A sieve algorithm for the shortest lattice vector problem”, In Proceedings of the thirty-third annual ACM symposium on Theory of computing, pp. 601-610, 2001.

[9] D. Micciancio and P. Voulgaris, “Faster exponential time algorithms for the shortest vector problem”, In Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms, pp. 1468-1480. SIAM, 2010.

[10] L. Ducas, “Shortest vector from lattice sieving: a few dimensions for free”, In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 125-145, Springer, 2018.

[11] M. R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. W. Postlethwaite, and M. Stevens, “The general sieve kernel and new records in lattice reduction”, In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 717-746, Springer, 2019.

[12] K. Kajita, K. Ogawa, K. Nuida, T. Takagi, “Short Lattice Signatures in the Standard Model with Efficient Tag Generation” The 14th International Conference on Provable Security, ProvSec 2020, LNCS 12505, pp.85–102, Springer, 2020.

[13] C. Gentry, C. Peikert, and V. Vaikuntanathan, “How to use a short basis: Trapdoors for hard lattices and new cryptographic constructions”, In proc. of STOC, pp. 197–206, ACM, 2008.

[14] K. Yamamura, Y. Wang, and E. Fujisaki, “Improved Lattice Enumeration Algorithms by Primal and Dual Reordering Methods”, The 24th Annual International Conference on Information Security and Cryptology (ICISC 2021), Springer LNCS, to appear, 2021.

九州大学 IMI 共同利用・短期共同研究　公開プログラム

新世代暗号の設計・評価

Design and Evaluation for New-generation Cryptography

日　　時：2021年11月16日（火）13:25 ～ 16:40
11月17日（水）13:30 ～ 16:45

場　　所：ハイブリッド(Zoom & 九州大学 伊都キャンパス ウエスト1号館
D棟 4階 IMIオーディトリアム(W1-D-413))

研究代表者：王　イントウ（北陸先端科学技術大学院大学・助教）

※プログラムは都合により変更になる場合がありますので予めご了承ください。
最新情報はホームページをご覧ください。

11 月 16 日（火）

13:25-13:30
オープンニング

13:30-14:30
藤原 幹生（NICT 量子 ICT 研究室・室長）
超長期セキュア分散ストレージシステム　量子セキュアクラウドの紹介

14:35-15:35
草川 恵太 (NTT 社会情報研究所・研究員)
格子暗号への平文・鍵確認オラクルを用いた鍵回復攻撃とサイドチャネル攻撃・故障利用攻撃

15:40-16:40
安田 雅哉 (立教大学・准教授)
格子基底簡約とその大規模並列化の紹介

11 月 17 日（水）

13:30-14:30
Chitchanok Chuengsatiansup (The University of Adelaide・講師)
Optimizing Lattice-based Cryptography

14:35-15:35
勝又 秀一 (AIST サイバーフィジカルセキュリティ研究センター・主任研究員)
A New Simple Technique to Bootstrap Various Lattice Zero-Knowledge Proofs to QROM Secure NIZKs

15:40-16:40
岡田 怜士 (東京大学・博士前期課程)
Misuse シナリオにおける格子暗号への秘密鍵・乱数復元攻撃

16:40-16:45
クロージング

※研究実施期間:2021 年 11 月 15 日(月)～11 月 19 日(金)