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	20210017	
1.研究計画題目	高機能耐量子電子署名方式の考案			
2.新規・継続	新規			
3.種別	若手研究			
4.種目	短期研究員			
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	2022年02月03日(木曜日)～2022年02月09日(水曜日)			
7.キーワード	耐量子暗号；電子署名方式			
8.参加者人数	3人			

9.本研究で得られた成果の概要

格子暗号、多変数多項式暗号、符号ベース暗号など耐量子計算機暗号(PQC)の候補として、近年盛んに研究が進められている。例えば、米国国立標準技術研究所(NIST)は2016年からPQCの標準化プロジェクトを進めてきた。2020年7月に第3ラウンドに採択した暗号方式4件と電子署名方式3件を発表した。そこで、本プロジェクト担当者のDustin Moody氏は「安全と応用の観点から、電子署名候補の多様性不足に心配」と2021年1月にメーリングリストにて世界中の暗号研究者に発信した。

本研究ではまず、格子のCVPγの困難性に基づいた落とし戸付き関数(TDF)を新しく設計した。また、提案TDFをGPV署名方式に適用し、計算量を減らすことができた。さらに、提案TDFでは秘密情報を保護できるため、GPVの棄却サンプリング法を取除くことができる可能性もあると考える。つまり、今回の研究ではGPV署名方式を改良し、新しい署名方式を提案することに成功した。今後、引続き提案署名方式の安全性証明、パラメータの提案、実装などを行い、国際会議で発表するまで研究を続けていく予定である。本研究によって、耐量子電子署名方式の多様性が高まると考えられる。

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-短期研究員

“高機能耐量子電子署名方式の考案”
(Studying High-functioning Post-Quantum Digital Signature Schemes)

成果報告書

目次

1. 実施状況

本事業(若手研究-短期研究員)は 2021 年 4 月に採択された。その後、7 月、8 月、11 月に九州大学マス・フォア・インダストリ研究所の池松泰彦先生とアドバイザーの秋山浩一郎氏で zoom オンラインミーティングを行い、研究内容、研究実施期間、実施形式などを決定した。以下では、本共同研究の情報、実施期間 2022 年 2 月 3 日(木)～2 月 9 日（水）において行なった内容について簡単に説明する。

参加者

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

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

プロジェクト概要ウェブサイト:

https://www.imi.kyushu-u.ac.jp/kyodo-riyo/research_chooses/view/20210017

研究実施期間:

2022 年 2 月 3 日(木)～2 月 9 日（水）

事前準備および実施概要:

2021 年 7 月、8 月、11 月に 3 回 zoom オンラインミーティングを行い、2022 年 2 月の実施期間に王と池松氏は九州大学に現地参加し、秋山氏は zoom オンラインで参加した。最初は、本研究の背景、目的、研究計画、実施期間などについて王から説明した。次に、本研究テーマと関連する先行研究のサーベイを実行し、王から代表的な研究成果[GPV08][MP12][HPSSW14]などを発表し、落とし戸付き関数(TDF: Trapdoor Function)の開発に取り組んだ。さらに、王らが提案した格子ベース暗号方式[WIY21]から署名方式に変更可能かを検討した。最後は格子の近似最近ベクトル問題(CVP_γ)に基づいた TDF を提案し、[GPV08]に挙げられた署名方式に適用して新しい署名方式を提案できた。

2. 研究背景

現代の情報社会では、電子署名方式の RSA、DSA、ECDSA などが電子決済や仮想通貨などの領域で幅広く利用されている。これらの暗号技術により偽造や改竄などを防止できる通信経路を実現し、情報通信の安全性を強化している。ただし、量子アルゴリズムの提案により、これらの暗号技術を短時間に攻撃できて非常に脅威になることが知られている。そのため、耐量子計算機暗号(PQC)の研究開発が世界的な急務となっている。その中、格子暗号、多変数多項式暗号、符号

ベース暗号など PQC の候補として、近年盛んに研究が進められている。例えば、米国国立標準技術研究所(NIST)は 2016 年から PQC の標準化プロジェクトを進めてきた。2020 年 7 月に第 3 ラウンドに採択した暗号方式 4 件と電子署名方式 3 件を発表した。そこで、本プロジェクト担当者の Dustin Moody 氏は「安全と応用の観点から、電子署名候補の多様性不足に心配」と 2021 年 1 月にメーリングリストにて世界中の暗号研究者に発信した。

3. 研究目的

本研究の目的は、耐量子性を持つ格子ベース高機能電子署名方式を提案することである。電子署名方式の中核となる落とし戸付き関数(TDF: Trapdoor Function)の設計が最も重要な課題だと考える。本研究構想としてはまず、格子暗号における LWE 問題、CVP 問題、NTRU 問題などに基づいた TDF を考察する。その上、新たな TDF を開発することを目指す。また、これらの TDF を用いて提案された署名方式を研究し、様々な署名技術を利用して開発した TDF をベースとした高機能な署名方式を提案し、高速実装を行う。本研究によって、耐量子電子署名方式の多様性が高まると考えられる。

4. 研究内容と研究成果の概要

本研究成果がまだ公表されていないため、研究成果の一部を公開する。現段階では理論の提案ができたが、提案方式に対する安全性解析および実装に関して引続き研究を続けていく予定となった。最終的に、まとめた論文を国内学会と国際会議に発表することを目指す。以下、研究内容に関する基礎理論や先行研究について簡単に説明する。

4.1 格子

n個の一次独立なベクトル$\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$の整数係数の線形結合全体の集合$L$を$\mathbb{R}^m$の格子(Lattice)と呼ぶ。$L$は以下のように定義される。

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

格子の元を格子点または格子ベクトルと呼ぶ。ベクトルの組$B = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$を基底(Basis)または格子基底と呼ぶ。整数$n$を格子$L$の次元(Dimension)と呼び、$n = m$のとき、格子は完全階数(full-rank)であるという。

4.2 近似最近ベクトル問題(CVP$_\gamma$: γ −Approximate Closest Vector Problem)

n次元の整数格子$L \subseteq \mathbb{Z}^n$の基底$\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$とターゲットベクトル$\boldsymbol{t} \in \mathbb{Z}^n$が与えられたとする。 与えられた近似因子$\gamma(n) \geq 1$に対して

$$\|\mathbf{v} - \mathbf{t}\| \leq \gamma(n)\|\mathbf{u} - \mathbf{t}\| \ (\forall \mathbf{u} \in L)$$

を満たす格子ベクトル$\mathbf{v} \in L$を見つけよ。

4.3 **落とし戸付き関数**(TDF: Trapdoor Function)

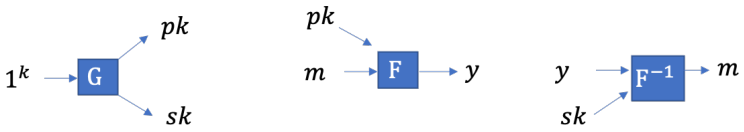

図.1 TDF の公開鍵暗号方式への応用例

落とし戸付き関数(TDF)とは、一方向の計算は容易だが、逆方向の計算は「落とし戸」の情報なしでは困難になる関数のことである。TDF は一方向性関数の特殊な例であり、公開鍵暗号方式(PKC)で広く利用されている。例えば PKC ではpkを公開鍵とし、skを秘密鍵とする。図 1 に示したように、TDF の一方向の安全性は、ランダムなpk, mが与えられたとき、Fの逆関数F^{-1}の情報がなければ、$(pk,\ F(pk,\ m)) \xrightarrow{?} m$の計算困難性を根拠としている。

4.4 **ガウス分布**(Gaussian Distribution)

- **連続ガウス分布：** $\boldsymbol{v} \in \mathbb{R}^m$を分布の中心(center)とし、$\sigma$は標準偏差(standard deviation)とする。$\mathbb{R}^m$の連続ガウス分布(continuous Gaussian distribution)は

$$\rho_{\boldsymbol{v},\sigma}^m(\boldsymbol{x}) = \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^m e^{-\frac{\|\boldsymbol{x}-\boldsymbol{v}\|^2}{2\sigma^2}}$$

で定義する。特に、$\boldsymbol{v} = \boldsymbol{0}$のとき、$\rho_\sigma^m(\boldsymbol{x})$で表す。

- **離散ガウス分布：** $\boldsymbol{v} \in \mathbb{Z}^m$を分布の中心(center)とし、$\sigma$は標準偏差(standard deviation)とする。$\mathbb{Z}^m$の離散ガウス分布(discrete Gaussian distribution)は

$$D_{\boldsymbol{v},\sigma}^m(\boldsymbol{x}) = \rho_{\boldsymbol{v},\sigma}^m(\boldsymbol{x}) / \rho_\sigma^m(\mathbb{Z}^m)$$

で定義する。$\rho_\sigma^m(\mathbb{Z}^m) = \sum_{\boldsymbol{z}\in\mathbb{Z}^m} \rho_\sigma^m(\boldsymbol{z})$は確率分布関数にするためのスケーリング因子となる。 任意の$\boldsymbol{v} \in \mathbb{Z}^m$に対して、$\rho_{\boldsymbol{v},\sigma}^m(\mathbb{Z}^m) = \rho_\sigma^m(\mathbb{Z}^m)$が成り立つ。そのため、任意の$\boldsymbol{v}$にとって、スケーリング因子は同一となる。

4.5 **[GPV08]の電子署名方式**

GPV 署名方式[GPV08]は hash-and-sign パラダイムに基づいて構築された。GPV では離散ガウスサンプリング手法(GaussianSampler)と、rejection sampling と呼ばれる棄却サンプリング法(PreImageSamp)を利用している。また、GPV で用いる TDF の安全性はCVP_γ問題の困難性に基づいている。以下、GPV 署名方式のフレームワークを示す。

- H: $\Sigma^* \to \mathbb{Z}_q^n$をハッシュ関数(hash function)とする。
  - 鍵生成 KeyGen(1^n): 与えられたパラメータセット$\{n, m,\ q, \sigma\}$で TrapSamp($n, m,\ q, \sigma$)を実行し、鍵ペア $(A,\ A') = (bad\ basis\ pk = A,\ good\ basis\ sk = A')$ を生成して出力する。

- 署名 Sign(msg, sk=A'): $\boldsymbol{y} = H(msg)$を計算し、短いベクトル $\boldsymbol{u}$ ←PreImageSamp($A', \boldsymbol{v}, \sigma, \boldsymbol{y}$)を出力する。例えば$L(A) \ni \boldsymbol{v} \leftarrow$ GaussianSampler$(A', \boldsymbol{y}, \sigma)$で計算して$\boldsymbol{u} = \boldsymbol{y} - \boldsymbol{v}$を得る。
- 検証 Verify($\boldsymbol{u}, msg$, $pk = A$): $\boldsymbol{y} = H(msg)$を計算する。$\boldsymbol{u} - \boldsymbol{y} \in L(A)$と$\|\boldsymbol{u}\| < 2\sigma\sqrt{m}$を両方とも満たすときのみ、Accept する。

■ 利用する TDF: 秘密鍵のA'から公開鍵A を計算することが容易であるが、逆にA からA'を計算するのが困難である(CVP$_\gamma$の困難性による)。

■ PreImageSamp(): 格子署名方式の transcript secure を保証するために[Lyu09]に提案された rejection sampling を使うことが一般的である。ただし、[HPSSW14]の解析によると、[Lyu09]の手法では棄却されるサンプルの比率が全体の 90%を超えている。

■ GaussianSampler(): GPV 署名方式では、“Randomized NearestPlane using discrete Guassian”を利用し、計算コストが$\Omega(n^3)$になる。さらに、高精度な実数演算で前処理をかけると、離散ガウスサンプルの計算量が$O(n^2)$まで改良できる[Pei10]。

4.6 研究結果

本研究ではまず、CVP$_\gamma$の困難性に基づいた TDF を新しく設計した。また、提案 TDF を GPV 署名方式に適用し、離散ガウスサンプラーを使わず提案手法でターゲットベクトルをサンプルできた。そのため、離散ガウスサンプラーと比較すると前処理の手間を省略することにより計算量を減らすことができた。さらに、提案 TDF では秘密情報を保護できるため、GPV の rejection sampling を取除くことができる可能性もあると考える。つまり、今回の研究では GPV 署名方式を改良し、新しい署名方式を提案することに成功した。今後、引続き提案署名方式の安全性証明、パラメータの提案、実装などを行い、査読付き国際会議で発表するまで研究を続けていく予定である。

5. 謝辞

本研究の実施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:

[HPSSW14] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, and W. Whyte, “Transcript secure signatures based on modular lattices”, In proc. of PQCrypto, LNCS, vol. 8772, pp. 142-159. Springer, 2014.

[GPV08] 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.

[MP12] D. Micciancio and C. Peikert, “Trapdoors for lattices: Simpler, tighter, faster, smaller”, In proc. of EUROCRYPT, LNCS, vol. 7237, pp. 700–718, Springer, 2012.

[WIY21] Y. Wang, Y. Ikematsu, T. Yasuda, “Public Key Cryptosystems Combining Lattice and Multivariate Polynomial”, In proc. of SCIS, 3A3-3, pp. 1-7, 2021.

[Pei10] C. Peikert, “An Efficient and Parallel Gaussian Sampler for Lattices”, In Proc. of CRYPTO, LNCS, vol. 6223, pp. 80-97, Spinger, 2010.

[Lyu09] V. Lyubashevsky, “Fiat-Shamir with aborts: applications to lattice and factoring-based signatures”, In Proc. of ASIACRYPT, vol. 5912, pp. 598–616, Springer, 2009.