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　５ 年　 ６ 月 １９ 日現在

機関番号：２７３０１
研究種目：若手研究
研究期間：2019～2022
課題番号：１９Ｋ２０２７２

研究課題名（和文）ブロックチェーンとIoT機器に最適化した署名技術の開発

研究課題名（英文）A Development of Signature Schemes Optimized to Blockchains and IoT Devices

研究代表者
福光　正幸（Fukumitsu, Masayuki）

長崎県立大学・情報システム学部・准教授

研究者番号：１０７３６１１９

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：本課題研究では，「ブロックチェーン」や「IoT機器」の基盤となる署名技術の開発が目標であり，このため，「圧縮可能性」（膨大な署名データ量を縮小できる性質）と「耐量子性」（量子コンピュータからの攻撃に耐えうる性質）を共に備えた署名技術を開発した．主成果として，両性質を満たす署名技術を開発した．これは，多重署名と呼ばれる圧縮可能性を有する署名技術であり，耐量子性のため，「格子」と呼ばれる数学的構造と「量子ランダムオラクル」と呼ばれるセキュリティモデルを採用した初の方式となる．なお，この主成果の実現と共に，ベースとなる署名技術の安全性分析と，ブロックチェーン・IoT機器に適した機能の検討を行った．

研究成果の学術的意義や社会的意義
本研究課題での署名技術は，ブロックチェーンの基盤やIoT機器から収集するデータの安全性（認証と改ざん検知）の保証が目的であった．これらはいずれもSociety5.0実現の根底をなす技術であり，開発した署名技術はこの実現の一助となることが社会的意義といえる．一方，開発の格子ベースの多重署名は，初の量子ランダムオラクルでの安全性を保証しているほか，この起点の署名技術であるFiat-Shamir型署名の安全性証明可能性分析までも実施していたが，これらの結果は理論安全性証明における新たな知見であることからも，学術的意義に値する．

研究成果の概要（英文）：The goal of this research project is to develop digital signature schemes that can be used as a foundation for blockchain and IoT devices. For this purpose, we developed a signature scheme with both compressibility (the property that can reduce a huge amount of signature data sizes) and quantum resistance (the property that can withstand attacks against a quantum computer). Namely, we developed the first lattice-based multi-signature secure in the quantum random oracle model. Moreover, we also conducted the security evaluation of the underlying signature schemes, i.e. the Fiat-Shamir-type signature schemes, and a study of functions desirable for blockchain and IoT devices.

研究分野：暗号理論

キーワード：ディジタル署名　多重署名　集約署名　格子　緊密性　量子ランダムオラクル

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年,「ブロックチェーン」や「IoT 機器」の活用に期待が高まっている．ブロックチェーンとは，ビットコインなどの仮想通貨において，サービス提供者が関与しなくとも，利用者同士で取引情報を安全に管理するための技術のことである．一方，IoT（Internet of Things）機器とは，インターネットに接続できる機器の総称のことである．これを用いることで，例えば，事故時の通報の自動化，車両盗難の際の追跡，リアルタイムな遠隔診療の実現が期待されており，実証実験も行われている．これらの認証と改ざん検知のため，署名技術（Digital Signature）と呼ばれる暗号技術が使われている．

しかし，署名技術をブロックチェーンや IoT 機器内で利用する場合，内在する次の 2 つの問題を考えなければならない．その 1 つ目は，生成される署名データ量の肥大化問題である．ブロックチェーンは，仮想通貨などの取引情報を安全に管理するための技術であるが，その堅牢性・改ざん不可能性の担保のため，署名技術が利用されている．実際，2016 年～2018 年にかけて，毎月約 4GByte ずつデータ量が増えており，2018 年 10 月現在の総量が 180GByte を超えている [LUXEMBOURG，2018]．一方，2020 年までに IoT 機器は世界全体で約 400 億万台が実稼働すると予測されており [総務省，2018]，それらからの膨大な収集データの真正性担保のために署名データを付与した場合，署名データ数が増大することは想像に難くない．つまり，このデータ量の多さは，システム全体のボトルネックとなり，その可用性を脅かす．

2 つ目の問題は，量子コンピュータが実用化された場合の安全性の破綻問題である．世界標準の署名技術は，量子コンピュータが実用化した場合，Shor のアルゴリズムにより，その安全性が破綻することが知られている．この場合，例えば，大量の IoT 機器になりすました攻撃が容易にできるようになり，その膨大さゆえ，これまでのサイバー攻撃の想像をはるかに超える脅威となりうる．すなわち，インターネット社会の安全性が破綻し，未曾有の事件へと繋がり兼ねない．この深刻さゆえ，NIST（National Institute of Standards and Technology：米国標準技術研究所）は 2016 年に量子コンピュータに対し耐性を持つ署名技術の公募を行い，その標準化を急いでいる [NIST，2023]．

つまり，次の 2 要件を共に満たす署名技術が要求される．

- 圧縮可能性：署名データの保管の際，そのデータ量を縮小できる性質
- 耐量子性：量子コンピュータを用いた攻撃に耐えうる性質

２．研究の目的

本研究では,「圧縮可能性」と「耐量子性」を共に備えた署名技術を開発する．圧縮可能性を満たす署名技術として,「多重署名（Multi-signature）」や「集約署名（Aggregate Signature）」が挙げられる．多重署名は，1 データに対し，特定の複数人が署名したことを認証できる署名技術であり，集約署名は，各人が生成した署名データを 1 つの署名データに集約できる署名技術である．これらは共通して，膨大な署名データを 1 署名データに集約することで，圧縮可能性を実現している．一方，耐量子性を満たす署名技術として,「格子署名」に着目する．そもそも，現代の暗号技術は,数学的構造をベースに設計していくが,格子署名はその中でも,格子（Lattice）と呼ばれる数学的な構造を基にした署名技術であり，耐量子性を満たす代表的な構造として知られている．実際，NIST の公募において，いくつかの格子署名が耐量子性を満たす署名技術として採用されており，その関心は高い．なお，格子署名の研究の中には，計算効率や機能性を高めるものが多くある．そこで，本研究課題では特に，耐量子性を満たす署名技術のうち「格子署名」に着目し，この実用的な多重・集約化手法の開発を目指す．

３．研究の方法

本研究課題遂行には，目的である多重・集約署名の開発に向けた基盤の確立や，本課題の応用先であるブロックチェーンや IoT 機器に特化した機能の検討も同時に行っていく必要があると考えた．そこで，次の 3 つの内容に大別して実施する．

(1) 多重・集約署名のベースとなる署名技術の選定と安全性評価

多重・集約署名を構成する際には，通常のディジタル署名技術をベースとすることが一般的である．実際，格子ベースの多重署名のうち El Bansarkhani，Sturm の方式 [El Bansarkhani，Sturm，2016] は，Fiat-Shamir 変換 [Fiat，Shamir，1987] と呼ばれる技法によって開発された署名技術（以降，Fiat-Shamir 型署名）を基にしていた．本研究課題においても，Fiat-Shamir 型署名を起点に多重・集約署名を開発していく．一方，署名技術をはじめとする暗号技術を開発

した際には，安全性証明（Security Proof）と呼ばれるフレームワークを用いて理論的安全性を保証していくことがデファクトスタンダードとなっている．これに対し，Fiat-Shamir 型署名についても，安全性証明により，その安全性が保証されている．しかし，その安全性はランダムオラクルモデル（Random Oracle Model）と呼ばれる制限されたセキュリティモデル上でのみの保証となっていた．さらに，このセキュリティモデルの場合，耐量子性について考慮しきれていなかった．格子構造に加え，更なる耐量子性を追求するため，この制限のないセキュリティモデルである標準モデル（Standard Model）や，耐量子性も考慮した量子ランダムオラクル（Quantum Random Oracle Model）と呼ばれるモデルでの安全性証明が望ましい．そこで，両モデルでの安全性証明可能性について議論する．

(2) 圧縮可能性と耐量子性を両立する署名技術の開発
本研究課題での主目的である「圧縮可能性」と「耐量子性」を満たす署名技術を開発する．この開発について，第 1 段階として，研究方法(1)での分析を基に本研究課題の起点となる格子ベースの多重署名を開発する．第 2 段階として，第 1 段階で実現した方式から，安全性証明が可能な多重署名の一般的な構成法（Generic Construction）を実現する．最終段階として，標準モデルか量子ランダムオラクルでの安全性を有する初の多重署名を実現する．

(3) ブロックチェーン・IoT 機器に適した署名技術の付加機能
ブロックチェーン・IoT 機器への応用を目指す多重・集約署名の付加機能に関する研究開発も現在進行形で多く実施されている．そこで，既存研究の結果について調査し，ブロックチェーン・IoT 機器への応用に向け必要な署名技術への付加機能についても議論する．

４．研究成果

「研究の方法」で述べた 3 つ方法それぞれについての研究成果を示す．

(1) Fiat-Shamir 型署名の安全性証明可能性の評価
Fiat-Shamir 型署名の安全性証明可能性について，ランダムオラクルモデルにて安全性証明できないとする結果が知られている [Paillier, Vergnaud, 2005]．特に，この不可能性の理由として，ランダムオラクルモデル特有の性質である「プログラミング性（Programmability）」と呼ばれる性質が Fiat-Shamir 型署名の安全性証明には本質的に必要とされていた．しかし，この理由　示唆する既存研究では，強力な暗号学的な仮定での安全性を考慮していなかった．安全性証明可能性における現状に対し，本研究成果の一つとして，強力な暗号学的な仮定を用いたとしても，プログラミング性がない場合，Fiat-Shamir 型署名の安全性を証明できないことを示した．すなわち，Fiat-Shamir 型署名について，標準モデルでの安全性証明が根本的に困難であることが示唆された．
この状況から，安全性証明の土台となるセキュリティモデルとして，量子ランダムオラクルモデルの採用が必要と考えた．量子ランダムオラクル上での Fiat-Shamir 型署名の安全性について，現在進行形で議論が続いているが，本研究課題では，Kiltz, Lyubashevsky, Schaffner による，「Lossiness」と呼ばれる性質を持つ Fiat-Shamir 型署名に対する安全性証明の結果に着目した [Kiltz, Lyubashevsky, Schaffner, 2018]．この結果は，単に量子ランダムオラクルでの安全性を肯定的に示しただけでなく，「緊密性（Tightness）」と呼ばれる安全性と署名データサイズの効率性の両立に直結する安全性にも着目した結果となっていた．この結果に対し，本研究課題では，マルチユーザ安全性（Multi-user Security）と呼ばれる署名技術を基盤とするシステムの複数の利用者を対象とした，いわば実社会に則した安全性にも着目し，Lossiness を有しない Fiat-Shamir 型署名の緊密な安全性の証明可能性や，量子ランダムオラクル上で緊密なマルチユーザ安全性を有するための Fiat-Shamir 型署名の拡張方法について議論した．
上述の成果については，暗号と情報セキュリティシンポジウム（SCIS）やコンピュータセキュリティシンポジウム（CSS）などの国内シンポジウムで発表したほか，CT-RSA 2020 などの査読付き国際会議や，電子情報通信学会や International Journal of Networking and Computing などの査読付き論文誌に採択されている．

(2) 耐量子性と圧縮可能性を両立する多重署名の開発
研究結果(1)の成果から，安全な署名設計には緊密性がキーであり，その実現の有力候補は，Lossiness を有する Fiat-Shamir 型署名と考えられる．
本研究課題の主目的である「耐量子性」と「圧縮可能性」を満たす多重署名の実現のため，Abdalla, Fouque, Lyubashevsky, Tibouchi による格子ベースの Fiat-Shamir 型署名をベースとした多重署名を開発した．本方式は，従来の多重署名に比べ，緊密性が高い方式となっている．
この成果から，Lossiness は，通常の Fiat-Shamir 型署名のみならず，これをベースとした多重署名においても，効果が発揮されることが示唆された．そこで，この結果を基に，Lossiness を有する Fiat-Shamir 型署名から，緊密性が高い多重署名の実現のための一般的な構成法を開発した．ただし，通常の Fiat-Shamir 型署名と異なり，本研究課題の一般的な構成法では，

Lossiness のみならず，Linearity と呼ばれる性質も同時に有する Fiat-Shamir 型署名を対象とすることで圧縮可能性を実現した．この一般的構成法を用いることで，格子ベースの多重署名のほか，部分和問題（Subset Sum Problem）という格子とはまた別の数学的構造をベースとした耐量子性を満たす方式が得られることも示すことができた．

さらに，Lossiness を満たす Fiat-Shamir 型署名からの多重署名に対し，上述の Kiltz, Lyubashevsky, Schaffner による量子ランダムオラクル上での安全性証明技法を適用することで，量子ランダムオラクルでの安全性を有する多重署名の実現が期待できる．この結果を基に，量子ランダムオラクルで安全性証明可能な格子ベースの多重署名を初めて実現できた．この実現は，Kiltz, Lyubashevsky, Schaffner の証明技法を多重署名に応用するための新たな証明技法を開発することで行っている．

以上の結果については，研究成果(1)と同様，SCIS や CSS などの国内シンポジウムで発表や，ProvSec 2020，などの査読付き国際会議や，電子情報通信学会や Journal of Internet Technology などの査読付き論文誌に採択されている．なお，Journal of Internet Technology は査読付き国際会議 AsiaJCIS 2020 からの招待論文となっている．

(3) ブロックチェーン・IoT 機器に適した機能を有する署名技術の検討

圧縮可能性に関して，ブロックチェーンで利用される署名技術を考える場合，署名データのみならず，公開鍵データのデータ量削減も重要な課題であることが既存研究の研究調査により判明した．そこで，上述の緊密性と鍵の圧縮可能性を両立できる多重署名を開発した．なお，この成果から，鍵圧可能性も有する対話型集約署名（Interactive Aggregate Signature）を実現できることも示した．また，多重・集約署名の場合，公開鍵データはランダムに選択された巨大な値であることが一般的であった．そのため，メールアドレスなどのユーザ固有の文字列をこの公開鍵データとして利用できる ID ベース署名に着目し，本研究課題では，グループタグ付き ID ベース多重署名（ID-based Multi-signature with Group Tag）という新たな概念を提唱した．また，耐量子性のため，格子ベースの実例を与えた．この方式は，複数人で制作されたコンテンツの NFT（Non-Fungible Token）の実現の応用を念頭に置いている．

一方，IoT 機器から収集した署名付きデータの圧縮に適した集約署名として，事前計算付き集約署名（Aggregate Signature with Pre-Computation）と呼ばれる最新の署名技術に関する研究を発見した．本研究課題では，緊密性を有する事前計算付き集約署名の実現方法を検討した．さらに，収集データ所有者のプライバシー保護も重要な課題であることから，これを考慮した署名技術の実現についても議論した．

以上の結果は，CSS や査読付き国際ワークショップ STM2021 などで発表したほか，International Journal of Networking and Computing などの査読付き論文誌に採択されている．

＜参照文献＞

Amos Fiat, Shamir Adi. (1987). How to prove yourself: practical solutions to identification and signature problems. CRYPTO '86, 186–194.

Rachid El Bansarkhani, Jan Sturm. (2016). An Efficient Lattice-Based Multisignature Scheme with Applications to Bitcoins. CANS 2016, 140–155.

Eike Kiltz, Vadim Lyubashevsky, Christian Schaffner. (2018). A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model. EUROCRYPT 2018, 552–586.

BLOCKCHAIN LUXEMBOURG. (2018 年 9 月 28 日). Blockchain Size. 参照先：https://www.blockchain.com/explorer/charts/

NIST. (2023 年 6 月 7 日). Post-Quantum Cryptography PQC. 参照先：https://csrc.nist.gov/projects/post-quantum-cryptography

Pascal Paillier, Damien Vergnaud. (2005). Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log. ASIACRYPT 2005, 1–20.

総務省. (2018). 平成 30 年版　情報通信白書.

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6件／うち国際共著　0件／うちオープンアクセス　6件）

１．著者名 Masayuki Fukumitsu, Shingo Hasegawa	４．巻 -
２．論文標題 Toward Tight Security of the Galindo-Garcia Identity-based Signature	５．発行年 2023年
３．雑誌名 Interdisciplinary Information Sciences	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） 10.4036/iis.2022.R.04	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 Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa	４．巻 12
２．論文標題 Group Signatures with Designated Traceability over Openers’ Attributes	５．発行年 2022年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 493～508
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.12.2_493	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 Masayuki Fukumitsu, Shingo Hasegawa	４．巻 11
２．論文標題 A Tightly Secure DDH-based Multisignature with Public-Key Aggregation	５．発行年 2021年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 319～337
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.11.2_319	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 Masayuki Fukumitsu, Shingo Hasegawa	４．巻 22
２．論文標題 Linear and Lossy Identification Schemes Derive Tightly Secure Multisignatures	５．発行年 2021年
３．雑誌名 Journal of Internet Technology	６．最初と最後の頁 1157～1168
掲載論文のDOI（デジタルオブジェクト識別子） 10.53106/160792642021092205018	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 Masayuki Fukumitsu, Shingo Hasegawa	４．巻 E104.A
２．論文標題 Tighter Reduction for Lattice-Based Multisignature	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1685～1697
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAP1131	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 Masayuki Fukumitsu, Shingo Hasegawa	４．巻 E104.A
２．論文標題 Impossibility on the Schnorr Signature from the One-More DL Assumption in the Non-Programmable Random Oracle Model	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1163～1174
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020DMP0008	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　0件／うち国際学会　11件）

１．発表者名 福光 正幸, 長谷川 真吾
２．発表標題 Quantum Random Oracle Model上でのSequential OR SignatureのMulti-user Security
３．学会等名 SCIS 2023: 2023年暗号と情報セキュリティシンポジウム
４．発表年 2023年

１．発表者名 Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa
２．発表標題 Dynamic Group Signatures with Message Dependent Opening and Non-Interactive Signing
３．学会等名 CANDAR 2022: The 10th International Symposium on Computing and Networking（国際学会）
４．発表年 2022年

１．発表者名
Masayuki Fukumitsu, Shingo Hasegawa

２．発表標題
On Multi-user Security of Schnorr Signature in Algebraic Group Model

３．学会等名
WICS2022: 9th International Workshop on Information and Communication Security（国際学会）

４．発表年
2022年

１．発表者名
Kyoya Anzai, Masayuki Fukumitsu, Hiroaki Anada, Shingo Hasegawa

２．発表標題
Group Signatures with Equality Test on Signers

３．学会等名
WICS 2022: 9th International Workshop on Information and Communication Security（国際学会）

４．発表年
2022年

１．発表者名
Hiroaki Anada, Kyoya Anzai, Masayuki Fukumitsu

２．発表標題
Attribute-Based Signatures of Fiat-Shamir Type in Bilinear Groups: Scheme and Performance

３．学会等名
PlatCon 2022: 2022 International Conference on Platform Technology and Service（国際学会）

４．発表年
2022年

１．発表者名
Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa

２．発表標題
Group Signatures with Designated Traceability over Openers' Attributes in Bilinear Groups

３．学会等名
WISA 2022: The 23rd World Conference on Information Security Applications（国際学会）

４．発表年
2022年

１．発表者名
福光 正幸, 長谷川 真吾

２．発表標題
Lattice Trapdoorに依存しない格子を基にしたIDベースマルチ署名に向けて

３．学会等名
CSS 2022: コンピュータセキュリティシンポジウム2022

４．発表年
2022年

１．発表者名
福光 正幸, 長谷川 真吾

２．発表標題
Algebraic Group Model上でのSchnorr署名のMulti-User Securityに関する一考察

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

４．発表年
2022年

１．発表者名
Masayuki Fukumitsu, Shingo Hasegawa

２．発表標題
An Aggregate Signature with Pre-communication in the Plain Public Key Model

３．学会等名
STM 2021: The 17th International Workshop on Security and Trust Management（国際学会）

４．発表年
2021年

１．発表者名
福光 正幸, 長谷川 真吾

２．発表標題
Algebraic Group ModelにおけるFiat-Shamir変換

３．学会等名
CSS 2021: コンピュータセキュリティシンポジウム2021

４．発表年
2021年

１．発表者名
福光 正幸, 長谷川 真吾

２．発表標題
Algebraic Model上でのLyubashevsky署名のTightnessについて

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

４．発表年
2021年

１．発表者名
Masayuki Fukumitsu, Shingo Hasegawa

２．発表標題
Linear Lossy Identification Scheme derives Tightly-Secure Multisignature

３．学会等名
AsiaJCIS 2020: The 15th Asia Joint Conference on Information Security（国際学会）

４．発表年
2020年

１．発表者名
Masayuki Fukumitsu, Shingo Hasegawa

２．発表標題
A Tightly Secure DDH-based Multisignature with Public-Key Aggregation

３．学会等名
WICS 2020: 7th International Workshop on Information and Communication Security（国際学会）

４．発表年
2020年

１．発表者名
Masayuki Fukumitsu, Shingo Hasegawa

２．発表標題
A Lattice-Based Provably Secure Multisignature Scheme in Quantum Random Oracle Model

３．学会等名
ProvSec 2020: The 14th International Conference on Provable and Practical Security（国際学会）

４．発表年
2020年

１．発表者名
Fukumitsu Masayuki, Hasegawa Shingo

２．発表標題
One-More Assumptions Do Not Help Fiat-Shamir-type Signature Schemes in NPROM

３．学会等名
CT-RSA 2020: The Cryptographers’ Track at the RSA Conference 2020（国際学会）

４．発表年
2020年

１．発表者名
福光 正幸, 長谷川 真吾

２．発表標題
量子ランダムオラクルモデルで安全性証明可能な格子ベースのマルチ署名方式の実現に向けて

３．学会等名
SCIS 2020: 2020年暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
Masayuki Fukumitsu, Shingo Hasegawa

２．発表標題
A Tightly-Secure Lattice-Based Multisignature

３．学会等名
APKC '19: Proceedings of the 6th on ASIA Public-Key Cryptography Workshop（国際学会）

４．発表年
2019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

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