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　 ６ 月　 ８ 日現在

機関番号：１１３０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ１１２８８

研究課題名（和文）ビッグデータ収集を行うＩｏＴデバイスに特化した暗号プロトコルの開発

研究課題名（英文）Developing cryptographic protocols designated for IoT devices and Big data

研究代表者
長谷川　真吾（Hasegawa, Shingo）

東北大学・データ駆動科学・AI教育研究センター・助教

研究者番号：８０５６７２１４

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：本研究では、IoTデバイスネットワークおよびブロックチェーンでの利用に特化したディジタル署名方式、特にマルチ署名方式および集約署名方式の開発を行った。具体的には、高い効率性と安全性を両立するため、格子構造を利用したマルチ署名方式の開発を中心に行った。
また、研究の遂行にあたり、基礎研究としてディジタル署名方式の安全性として求められる安全性証明の構築条件について考察を行い、種々の制約条件、およびそれを回避し高い安全性を持つデジタル署名方式の構成方法を考案した。

研究成果の学術的意義や社会的意義
本研究は現在幅広く利用されているブロックチェーンならびにIoTネットワークのセキュリティを担保、および向上させるための研究である。具体的には、現在それらの中で使用されている暗号技術の分析・改良を行い、より効率性と安全性の高い実装を目指すためのものである。

研究成果の概要（英文）：We propose digital signature schemes, multisignature schemes and aggregate signature schemes designated for IoT device networks and blockchains.
We construct several signature schemes based on lattice problems in order to achieve high efficiency and security.
Additionally, we consider several conditions and properties so that signature schemes can have security proofs, especially with tight reductions. We give some impossilibilities on proving the security of signature scheme, and also give several constructions of signature scheme to avoid such impossibilities.

研究分野：暗号理論

キーワード：ディジタル署名　安全性証明　マルチ署名　集約署名　ブロックチェーン　IoTネットワーク

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

IoT(Internet of Things) と呼ばれる、PC やスマートフォンなどの従来型情報通信機器以外のデバイスをインターネットに接続する試みが急速に拡大している。IoT デバイスの例としては、温度計や速度計などの各種センサーが挙げられ、それらから得られる情報を利用することでビッグデータ収集やその分析が可能になる。今後 IoT デバイスの普及はさらに加速することが予想されている。

上記のような IoT デバイスの急速な増大に伴い、IoT デバイスを対象にしたサイバー攻撃も多数報告されている。代表的なものとしては IoT デバイスを攻撃目標とするマルウェア「Mirai」が挙げられ、50 万台以上の IoT デバイスに感染し DDOS 攻撃を行ったことが報告されている。IoT デバイスは従来のサーバや PC とは異なり、必ずしも十分なセキュリティを確保するだけのリソースを持たないこともあり、IoT デバイスをターゲットとしたサイバー攻撃は今後も増加すると予想され、企業システムに対するサイバー攻撃のうち 25%が IoT デバイスを対象にしたものになるという予測もある。

以上のような状況を見るに、IoT デバイスにおけるセキュリティ対策は急務である。しかしながら、そのセキュリティ対策における問題として、既に述べたように IoT デバイスのリソース不足が挙げられる。一般に、IoT デバイスにおけるリソースは従来のサーバや PC と比べて非常に不足している。そのため、それら従来型情報通信機器での使用を念頭に設計されている情報セキュリティ技術、特にその中核をなす暗号プロトコルがそのまま使用できないことが IoT デバイスにおけるセキュリティ危機につながっている。よって、IoT デバイスでの使用を念頭においた、高効率な暗号プロトコルの開発が必要である。

本研究では、IoT デバイスに必要とされる暗号プロトコルとして、改ざんを防止するためのディジタル署名に注目する。これは収集されたビッグデータを利用して分析を行うためには、データの信頼性が不可欠であるからである。また、このディジタル署名方式を設計・実装する数学的構造も重要な意味を持つ。暗号プロトコルの設計においては、何らかの数学的構造を採用し、その上でプロトコルの設計を行う。ここで、同じような機能を持つ暗号プロトコルでも、土台とする数学的構造によって実装時の効率が大きく変わることが知られている。暗号プロトコル用の数学的構造の代表的なものとして、素数を法とする巡回群、楕円曲線上の巡回群、格子構造が知られている。これらのうち、最も IoT デバイス用暗号プロトコルに適した数学的構造は格子構造である。格子構造は近年暗号プロトコルに使用されるようになった数学的構造であり、その上で構成される暗号プロトコルは、他の数学的構造上で構成される同じ機能を持つ暗号プロトコルよりも、高い効率性を持つことが知られている。

２．研究の目的

本研究の目的は、IoT デバイスに特化した暗号プロトコルの開発、具体的には格子構造上で構成されるディジタル署名方式の開発である。格子構造上では様々なディジタル署名方式が考案されているが、特に IoT デバイスネットワークやブロックチェーンにおける利用が期待されるマルチ署名方式、および集約署名方式をターゲットとする。マルチ署名方式とは、複数の署名者が協力して１つの署名を作成する方式であり、特にブロックチェーンとの親和性が高い。集約署名方式はマルチ署名方式をさらに一般化したものであり、複数の署名者が作成した複数の署名を単一の署名に集約・圧縮可能な方式である。集約署名方式は、その機能から IoT デバイスネットワーク上で測定されたデータの効率的な改ざん防止に役立つと期待できる。

３．研究の方法

（１）ディジタル署名方式における安全性証明構築のための基礎研究

ディジタル署名方式をはじめとする現代の公開鍵系暗号プロトコルでは、その安全性を保証するために、安全性証明と呼ばれる数学的証明を構成し付加することが実質的に標準の安全性保証手段となっている。すなわち、ディジタル署名方式を設計する際には、それに付随する安全性証明の構成も考慮しなければならない。しかしながら、どのような方式でも安全性証明が構成できるという訳ではなく、一部の条件の下では安全性証明を構成することがそもそも不可能であるという研究も行われてきている。すなわち、やみくもに方式の設計を行い、安全性証明を構成できるか試行する、というアプローチは非効率であるといえる。

よって、本研究を進める上では、まず安全性証明が構成できる、またできないための条件を明らかにすることを基礎研究として行う。研究を進めるにあたっては、２大安全性モデルであるランダムオラクルモデルと標準モデルの２つについて、署名方式が安全性証明を持つための条件解明を行う。ランダムオラクルモデルとは、理想的なハッシュ関数を仮定するモデルであり、方式の構成が効率的になる、安全性証明が簡素になるなどの利点がある。標準モデルとは、現実に運用されているハッシュ関数をモデル化したものであるため、より現実世界での安全性に直結した安全性解析が可能になる。

（２）　具体的なディジタル署名方式、および高機能署名方式の開発

研究の目標であるマルチ署名方式、および集約署名方式を開発する。まず、上記（１)で得られた結果を参考に、通常のディジタル署名方式、およびそれをベースとしたマルチ署名方式の開発を行う。安全性証明において採用するモデルは、現実世界への影響を考慮し、標準モデルでの構成を基本とするが、開発方式の処理効率が悪くなる場合には、ランダムオラクルモデルでの開発も検討することとする。続いて、マルチ署名方式の開発にて得られた知見を基に、集約署名方式の開発を行う。

４．研究成果

(1) ディジタル署名方式の安全性証明における基礎研究

ディジタル署名方式における安全性証明について、特に Fiat-Shamir 型ディジタル署名方式に対し、従来より強力な仮定を用いても標準モデルでは安全性証明を構成できないことを理論的に示した。本結果は Fiat-Shamir 型ディジタル署名方式の安全性証明可否について従来進められてきた研究の発展にあたるものであり、この結果によりディジタル署名方式の理想的な安全性のひとつされている、標準モデルにおける安全性証明を Fiat-Shamir 型ディジタル署名方式が達成することは極めて難しいことが明らかとなった。

(2) 緊密な安全性証明を持つディジタル署名方式の構成

安全性証明において、特にその証明過程における帰着効率が緊密であるか否かは暗号方式の安全性に直結する重要なポイントとされている。ディジタル署名方式の場合においては、緊密な方式を構成するための条件や構成方法について様々な研究が行われている。その中の１つである、緊密な安全性証明を構成するための一般的手法として知られている損失認証方式に対し、その新たな構成例を開発した。具体的には、決定性 RSA 仮定と呼ばれる暗号学的仮定を利用し、損失認証方式を構成した。この成果は、決定性 RSA 仮定が暗号プロトコルの設計において有効な性質を持つ暗号学的仮定であることを示唆している。また、構成した方式は従来の RSA 仮定およびその派生仮定に基づく方式の中で最良の効率を持つものである。

(3)ID ベース署名方式における構成の体系化と安全性の向上

ディジタル署名方式の発展型方式である ID ベース署名方式において、効率的な実行処理が知られている Galindo-Garcia 型 ID ベース署名方式に対し、その構成手法の一般化を行った。具体的には、Galindo-Garcia 型 ID ベース署名方式の構成を詳細に解析し、構成のベースとなっている通常のディジタル署名方式に求められる条件を明らかにした。これは、ディジタル署名方式を構成することで効率的な ID ベース署名方式を自動的に得られることを意味する。

また、この Galindo-Garcia 型 ID ベース署名方式に対し、その安全性証明を改良し緊密な安全性証明を持つ ID ベース署名方式を構成した。具体的には Galindo-Garcia 型 ID ベース署名方式のベースとなっている Schnorr 署名を緊密な安全性証明を持つ Katz-Wang 型ディジタル署名に置き換えることで緊密な安全性証明を持つ ID ベース署名方式を構成することに成功した。本手法を応用することで、緊密な安全性証明を持つ ID ベース署名方式の効率的な構成が増加することが期待される。

(4) 格子構造上におけるマルチ署名方式の開発

緊密な安全性証明を持つ、格子構造を利用したマルチ署名方式の開発を行った。開発した方式は、格子構造を利用するマルチ署名方式の中で初めて緊密な安全性証明を達成するものである。また、この方式は格子構造を利用する通常のディジタル署名方式を利用して構成されているものの、その構造は一般の Fiat-Shamir 型ディジタル署名方式に容易に応用可能なものであるため、本結果を応用した更なる効率の良い方式の構成が期待される。

また、上記の結果、および結果(2)にて使用した損失認証方式を使用するディジタル署名方式の構成方を応用し、緊密な安全性証明を持つマルチ署名方式の一般的構成を開発した。

(5) 量子計算機の攻撃に耐性を持つマルチ署名方式の開発

格子構造を用いたマルチ署名においては、その効率性だけでなく、量子計算機による攻撃への耐性が期待されている。これは、格子構造上で利用される暗号学的仮定に対し、量子計算機を用いても効率的な解読方法が知られていないためである。しかしながら、既存の格子構造上の方式においての安全性証明は全て古典計算機モデル上のものであり、量子計算機を使用できる攻撃モデル上の結果は知られていなかった。本研究では量子計算機を用いた攻撃モデルにおいても安全性を証明できるマルチ署名方式の構成を初めて開発した。提案方法は既に耐量子ディジタル署名方式として期待されている Dilithium 方式をマルチ署名に拡張したものであり、理論上だけでなく実用上においても高い効率と安全性が期待できる。

(6) 鍵集約機能を持つマルチ署名方式の開発

マルチ署名方式のブロックチェーンへの応用を考える上で重要となる、鍵の集約機能を持つマルチ署名について、緊密な安全性証明を持つ方式を初めて構成した。

(7) 緊密な安全性証明を持つ集約署名方式の構成

マルチ署名方式をより一般的な機能に拡張した高機能署名が集約署名方式である。この集約署名についてはペアリング演算を使用しない具体例が長年知られていなかったが、集約タイミングを制限することでペアリング演算に頼らない構成が可能な、事前通信つき集約署名が近年提案された。この事前通信つき集約署名について、緊密な安全性証明を持つ方式を初めて構成した。

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　7件／うち国際共著　1件／うちオープンアクセス　6件）

１．著者名 Philipp Stratil, Shingo Hasegawa, Hiroki Shizuya	４．巻 27
２．論文標題 Supersingular Isogeny-based Cryptography: A Survey	５．発行年 2021年
３．雑誌名 Interdisciplinary Information Sciences	６．最初と最後の頁 1～23
掲載論文のDOI（デジタルオブジェクト識別子） 10.4036/iis.2020.R.02	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 該当する

１．著者名 Shingo Hasegawa, Shuji Isobe	４．巻 25
２．論文標題 Lossy Identification Schemes from Decisional RSA	５．発行年 2019年
３．雑誌名 Interdisciplinary Information Sciences	６．最初と最後の頁 59-66
掲載論文のDOI（デジタルオブジェクト識別子） 10.4036/iis.2019.R.01	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 －

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 Shingo Hasegawa, Masashi Hisai, Hiroki Shizuya	4．巻 11
2．論文標題 Public-Key Projective Arithmetic Functional Encryption	5．発行年 2021年
3．雑誌名 International Journal of Networking and Computing	6．最初と最後の頁 299-318
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.11.2_299	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 1159-1170
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11件（うち招待講演　0件／うち国際学会　11件）

1．発表者名 Masayuki Fukimitsu, Shingo Hasegawa
2．発表標題 Linear Lossy Identification Scheme derives Tightly-Secure Multisignature
3．学会等名 2020 15th Asia Joint Conference on Information Security (AsiaJCIS 2020)（国際学会）
4．発表年 2020年

１．発表者名
Masayuki Fukimitsu, Shingo Hasegawa

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

３．学会等名
Provable and Practical Security (ProvSec 2020)（国際学会）

４．発表年
2020年

１．発表者名
Masayuki Fukimitsu, Shingo Hasegawa

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

３．学会等名
2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW'20)（国際学会）

４．発表年
2020年

１．発表者名
Shingo Hasegawa, Masashi Hisai, Hiroki Shizuya

２．発表標題
Public-key Projective Arithmetic Functional Encryption

３．学会等名
2020 Eighth International Symposium on Computing and Networking (CANDAR'20)（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 Lattice-Based Multisignature.

３．学会等名
6th ASIA Public-Key Cryptography Workshop (APKC ’19)（国際学会）

４．発表年
2019年

１．発表者名
Masayuki Fukumitsu, Shingo Hasegawa

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

３．学会等名
Topics in Cryptology - CT-RSA 2020（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 Generic Construction of an Identity-based Signature from a Sigma Protocol

３．学会等名
2018 International Symposium on Information Theory and Its Applications (ISITA 2018)（国際学会）

４．発表年
2018年

１．発表者名
Masayuki Fukumitsu, Shingo Hasegawa

２．発表標題
A Galindo-Garcia-like Identity-based Signature with Tight Security Reduction, Revisited

３．学会等名
2018 Sixth International Symposium on Computing and Networking (CANDAR'18)（国際学会）

４．発表年
2018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
17th International Workshop on Security and Trust Management (STM2021)（国際学会）

４．発表年
2021年

１．発表者名 Hiroaki Anada, Masayuki Fukumitsu, Shingo Hasegawa
２．発表標題 Group Signatures with Designated Traceability
３．学会等名 2021 Ninth International Symposium on Computing and Networking (CANDAR'21)（国際学会）
４．発表年 2021年

１．発表者名 Anaelle Le Devehat, Hiroki Shizuya, Shingo Hasegawa
２．発表標題 On the Higher-bit Version of Approximate Inhomogeneous Short Integer Solution Problem
３．学会等名 20th International Conference on Cryptology And Network Security (CANS2021)（国際学会）
４．発表年 2021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