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　６ 年　 ６ 月 ２１ 日現在

機関番号：１２６１２
研究種目：基盤研究(C)（一般）
研究期間：2018～2023
課題番号：１８Ｋ１１２９２

研究課題名（和文）New Paradigm to Construct Public Key Cryptographic Schemes for Lightweight Devices with Provable Security against Quantum Attackers

研究課題名（英文）New Paradigm to Construct Public Key Cryptographic Schemes for Lightweight Devices with Provable Security against Quantum Attackers

研究代表者

ＳＡＮＴＯＳＯ　ＢＡＧＵＳ（SANTOSO, Bagus）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：４０５７１９５６

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：量子計算機の実現を目指した研究が飛躍的に進歩している．一方で，量子計算機は素因数分解問題や離散対数問題を効率的に解くことができるため，これらの問題の困難性を安全性の要とする標準的な暗号理論の方式にとって，量子計算機は脅威的な存在である．量子計算機の攻撃者を想定した暗号理論方式がいくつか提案されたが，多くの方式は理論的な安全性の保証と実装可能性の面に問題を抱えている．　本研究は純粋なGF(2)表現が可能な方式，量子計算機にも困難な判定型の計算問題，情報理論的安全性を軸にこの問題を解決する技術の開発に成功した．本研究の成果は複数の論文誌にすでに掲載され，査読付き国際会議に発表された．

研究成果の学術的意義や社会的意義
This project provided cryptographic schemes which are not only ensure security against quantum computers but are also implementable in practice. These schemes will safeguard the interconnected individuals in the next-generation network against the next-generation adversaries with quantum computers.

研究成果の概要（英文）：The research to construct practical quantum computers is making dramatic progress. However, the ability of quantum computers to efficiently solve prime factorization and discrete logarithm problems poses a threat to standard cryptography schemes, which rely on the difficulty of these problems for their security. Several cryptographic schemes have been designed to withstand attacks from quantum computers, but most of them suffer from issues related to theoretical security guarantees and implementation feasibility. In this research project, we have successfully developed cryptographic schemes that solve these problems based on the following paradigms: schemes with pure binary field representation, decision-type computational problems that are challenging even for quantum computers, and information-theoretic security. The results of this project have already been published in several journals and presented at peer-reviewed international conferences.

研究分野：cryptography

キーワード：quantum adversaries　encryption　authentication　digital signatures　privacy amplification

１．研究開始当初の背景

量子計算機の実現を目指した研究が飛躍的に進歩している．一方で，量子計算機は素因数分解問題や離散対数問題を効率的に解くことができるため，これらの問題の困難性を安全性の要とする標準的な暗号理論の方式（cryptographic schemes）にとって，量子計算機は脅威的な存在である．そこで，量子計算機を使用する攻撃者を想定して設計された新たな耐量子暗号理論方式（post-quantum cryptographic schemes, PQC 方式）がいくつか提案されていたが，多くの方式は以下の問題を抱えている．

(1) 提案された方式は理論設計にとどまり，実装の面をあまり考慮していないため，実用性が低く，適用可能な環境や装置が限られている．ある程度の実装が可能になっても，電力や計算のコストが高く，特に低資源装置では長期使用に適していない．
(2) 提案された方式は量子計算機を持つ攻撃者に対する安全性証明が不完全である．多くの方式では「公開情報から直接秘密情報を求めることは量子計算機を使用しても困難である」という保証にとどまっており，公開情報から直接秘密情報を求める以外の攻撃に関してはあまり議論されていなかった．

２．研究の目的

本研究は前章で示された既存の PQC 方式における問題を回避できる新たな構成法のフレームワークを開発することを主目的とする．既存研究における問題の原因を特定し, 本研究の具体的な目的は以下になる．

(1) 実用性を向上するために設計の時点で実装コストの見積もりが簡単に計算または予測できるような PQC 方式の設計フレームワークを実現する．このフレームワークが実現できれば, 設計の時点で実装コストが把握可能なので, 実装コストが抑えるように構造の設計が可能になる．
(2) 使用範囲を広くするためにどの装置でも効率的に実装できるような PQC 方式を設計するフレームワークを実現する．特に次世代のネットワークである Internet of Things (IoT) では多くの低資源装置が繋がっているので, 低資源装置にでも効率的に実装可能な設計方法の開発を目的とする．
(3) 量子計算機に対する安全性がより簡単に証明できる構造を利用した PQC 方式の設計するフレームワークを実現する．計算機の複製可能性に依存する安全性証明の構築方法が量子計算機には適応できないことが判明されたので, 計算機の複製可能性に依存しない安全性証明が可能な PQC 方式の新たな設計方法の開発を目的とする．

３．研究の方法

本研究では上記の目的を達成するために次の項目に注視し研究を進めてきた．

【純粋なバイナリ・フィールド表現が可能な方式】 どの装置やオペレーティングシステムでもバイナリフィールド (GF(2)) の演算が必ず可能である．よって, GF(2) だけで実現できる PQC 方式は，低資源装置を含むどの装置にも実装可能である．本研究では，純粋な GF(2) だけで実現する PQC 方式の設計方法を開発する．PQC 方式の安全性は，その代数構造に依存する計算問題に大きく影響される．
本研究では，GF(2) だけで表現可能で，量子計算機に対しても効率的に解けないと予測される計算問題をベースにした PQC 方式の設計フレームワークを開発する．注目する計算問題は，符号理論に基づいた問題と多変数多項式問題である．

【判定問題に基づいた量子計算機に対する安全性証明】 暗号理論の安全性証明は，攻撃者から特定の計算問題の解答を取り出せるアルゴリズムを構成する形が一般的である．特に認証方式では，攻撃者を途中で止めたり巻き戻すことが必要であるが，量子計算機の攻撃者では物理法則により不可能である．
本研究では，計算問題の解答を求めない判定問題に注目し，それに基づいた量子計算機に対する安全性証明を開発する．これにより, 攻撃者の巻き戻しが不要になり, 量子計算機の攻撃者に対しても安全性証明が簡単に構成できると期待される．

４．研究成果

研究期間 (2018 年度～2023 年度) の間に本研究が得られた主な成果は次の通りである．

4.1 純粋な GF(2) で表現可能な判定問題に基づいた量子計算機の攻撃者に安全な認証方式

NP 困難な判定問題は平均的な場合にも量子計算機でも効率的に解くことができないと予測されている．本研究では，NP 困難な判定問題に注目し，さらにどの装置でも実装可能な方式を目指した．特に，純粋な GF(2) で表現可能な NP 困難な判定問題に重点を置き，量子計算機による攻撃にも耐えられる安全な認証方式を開発した．研究成果は以下の通り分類される．

■多変数多項式による計算問題に基づいた新たな認証方式　本研究は量子計算機にも困難と予測されている多変数多項式問題 Isomorphism of Polynomials with Two Secrets (IP2S) 問題を基に量子攻撃者にも耐性を有する新たな認証方式を構成することに成功した．本研究は既存研究で提案された認証方式の脆弱性を解析し，脆弱性が完全に無くなるように方式の変更方法を求め, それを基にし，新たな方式を構築した．計算問題 IP2S は GF(2) で表現できるので，構成された認証方式も GF(2) で直接表現でき，全ての演算は直接 XOR ゲートと AND ゲートに変換可能であり IoT のどの装置でも容易に実装できると考えられている．本研究の成果は論文誌 IEICE に掲載された．

■二面性を持つ計算問題に基づいた新たな対話的認証方式　多変数二次多項式（Multivariate Quadratic Polynomials (MQ)）問題は NP 困難であることが証明され，暗号理論への応用が期待されている．多くの MQ 問題ベースの暗号方式は, ある特殊な MQ 問題の困難性を基本仮定とする Hidden Field Equation (HFE) に基づいて構成された．しかし, HFE に基づいた暗号方式では, 攻撃手法を MinRank 問題の簡単に解けるインスタンスに帰着できる場合が多く, 提案された方式のほとんどが実際に破られてしまいました．これにより, MinRank 問題は暗号方式に対する攻撃の脅威的な道具として広く知られるようになりました．

しかし，MinRank 問題には攻撃道具としての側面とは別に，NP 困難であり，一般的には量子計算機でも効率的に解けないと予測される側面もある．本研究では，MinRank 問題に基づいた既存の Courtois 認証方式に注目し，新たな技法でなりすまし攻撃の成功確率を下げることに成功した．この成果に基づき，既存方式を改良し，新たな認証方式の構築に成功した．本研究の成果は査読付き国際会議 ISITA で発表された．

■符号理論ベースの計算問題に基づいた新たな認証方式　Syndrome Decoding (SD) 問題は NP 困難であり，符号理論の研究分野で長い歴史を持ち，実世界での困難性も様々な観点から研究されている．また，量子計算機にとっても困難であると予測されている．本研究では，SD 問題に基づいた認証方式について，以下の 2 つの方向で研究を進めた．

1. 同時攻撃を行う量子計算機の攻撃者に対しても安全性を証明できる新たな対話的認証方式の開発.
2. 標準的なハッシュ関数の使用を考慮しつつ，量子計算機の攻撃者に対しても安全性を証明できる新たな電子署名方式の開発.

本研究の成果は，論文誌 JUCS および査読付き国際会議 ISPEC に発表された．

■Tensor Rank 問題に基づいた新たな NP 困難な計算問題　Tensor Rank 問題は NP 困難であり，量子計算機にとっても効率的に解けないと予測されている．しかし，暗号理論の方式においては Tensor Rank 問題の扱いが難しく，この問題に基づいた方式は存在しなかった．本研究では，Tensor Rank 問題の NP 困難性を維持しつつ，問題をより扱いやすい形にすることを目指した．その結果，Tensor Rank 問題の特殊形に基づき，NP 困難性を満たした新たな計算問題である Bilinear Decomposition with Rank (BDR) 問題の開発に成功した．さらに，BDR 問題に基づいた新たな対話的認証方式も構成した．本研究の成果は，情報セキュリティ関連の国内学会 SCIS および国内研究会 ISEC に発表された．

4.2 多変数多項式問題に基づいた暗号方式に対する新たな安全性の評価

多くの多変数多項式問題ベースの暗号方式は, Hidden Field Equation (HFE) に基づいて構成されたが, 提案された方式のほとんどが実際に破られてしまいました．本研究は多変数多項式問題ベースの暗号方式を構成するための別の手法を開発し, その安全性の評価を行うことを目指した．本研究の成果は次のように分類される．

■IP2S 問題の一般化に基づいた新たな暗号方式　純粋な IP2S 問題から構成された暗号方式では秘密情報を表す変数の数が少なすぎたため, 暗号方式は簡単に破られた. 本研究は IP2S 問題の一般的な形に拡張し, 新たな計算問題を構成した. さらに, 構成された計算問題に基づいて理論的な安全性が証明可能である新たな暗号方式を開発した. 本研究の成果は査読付き国際会議 PQCRYPT に発表された.

■一般的な多項式同型問題に基づいた暗号方式の安全性評価　本研究は, 上記の研究成果も含めて一般的な多項式同型問題に基づいた暗号方式の実世界の安全性に注目した. 本研究はそれらの暗号方式における共通な脆弱性を発見した. さらに, 本研究は発見した脆弱性を利用して, ほぼ全ての多項式同型問題に基づいた暗号方式が実世界で簡単に破られることも明らかにした. 本研究の成果は査読付き国際会議 Inscrypt に発表された.

4.3 情報理論的安全性フレームワーク上の共通鍵暗号方式の安全性強化

情報理論的安全性のフレームワークでは想定された攻撃者が無限の計算能力を持っているので, 情報理論的安全性を満たす暗号方式は自動的に量子計算機に対する安全性を満たしている. 本研究は特に共通鍵暗号方式における情報理論的安全性に注目した. 本研究の成果は次の通り分類される.

■分散暗号化の秘匿性強化　分散暗号化において各ノードでの暗号機で使用されている鍵が相関が持つ場合, 各ノードの暗号文を盗聴し, まとめた盗聴結果を解析する攻撃者には各ノードにおける平文がより効率的に見るかる危険性がある. 本研究はこの問題に注目し, 秘密鍵の乱数性を増やすことなく, 暗号文の圧縮捜査だけで秘匿性を強化する技術を開発した. 本研究の結果は論文誌 IEEE Trans. on Information Forensics and Security に掲載され, 査読付き国際会議 ISIT にも発表された.

■サイドチャンネル攻撃に対する秘匿性の強化　暗号化における物理的な捜査から漏れたサイドチャンネル情報 (電波や電力の増減など) を利用して暗号文から秘密鍵がより推定しやくなる危険性がある. 本研究はこの問題に注目し, 暗号文に対する低コストの追加捜査で秘密鍵の秘匿性を強化する技術を開発した. 本研究の結果は論文誌 Entropy に掲載され, 査読付き国際会議 ISIT にも発表された.

4.4 判定問題に基づいた多重署名方式の新たな構成法

多重署名方式は複数の署名者の署名を信頼性を失うことなく圧縮する技術である. この技術は分散データの安全性向上や暗号資産技術における認証の効率向上に広く使用されている. しかし, 従来の多重署名方式は署名者間のやりとりのコスト削減と理論的な安全性の両立が困難という問題がる. 本研究はこの問題に注目し, 判定問題を使用したやりとりのコスト削減と理論的な安全性を両立させる新たな手法を開発した. 本研究の成果は論文誌 IEICE に掲載された.

５．主な発表論文等

〔雑誌論文〕　計30件（うち査読付論文　18件／うち国際共著　16件／うちオープンアクセス　8件）

１．著者名 Kaoru Takemure, Yusuke Sakai, Bagus Santoso, Goichiro Hanaoka, Kazuo Ohta	４．巻 AdvPub
２．論文標題 More Efficient Two-Round Multi-Signature Scheme with Provably Secure Parameters for Standardized Elliptic Curves	５．発行年 2023年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1-25
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2023EAP1045	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 Bagus Santoso, Yasuhiko Ikematsu, Shuhei Nakamura, Takanori Yasuda	４．巻 ISITA
２．論文標題 Three-Pass Identification Scheme Based on MinRank Problem with Half Cheating Probability	５．発行年 2022年
３．雑誌名 International Symposium on Information Theory and Its Applications (ISITA) 2022	６．最初と最後の頁 59-63
掲載論文のDOI（デジタルオブジェクト識別子） なし	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

１．著者名 Yasuhiko Ikematsu, Shuhei Nakamura, Bagus Santoso, Takanori Yasuda	４．巻 13007
２．論文標題 Security Analysis on an ElGamal-Like Multivariate Encryption Scheme Based on Isomorphism of Polynomials	５．発行年 2021年
３．雑誌名 Information Security and Cryptology. Inscrypt 2021. Lecture Notes in Computer Science. Springer,	６．最初と最後の頁 235～250
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-88323-2_12	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

１．著者名 Bagus Santoso	４．巻 LNCS 12100
２．論文標題 Generalization of Isomorphism of Polynomials with Two Secrets and Its Application to Public Key Encryption	５．発行年 2020年
３．雑誌名 PQCrypto 2020	６．最初と最後の頁 340～359
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-44223-1_19	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 －

１．著者名 Bagus Santoso, Yasutada Oohama	４．巻 14
２．論文標題 Secrecy Amplification of Distributed Encrypted Sources With Correlated Keys Using Post-Encryption-Compression	５．発行年 2019年
３．雑誌名 IEEE Transactions on Information Forensics and Security	６．最初と最後の頁 3042～3056
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/tifs.2019.2907464	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

１．著者名 Bagus Santoso, Chunhua Su	４．巻 25
２．論文標題 A New Identification Scheme based on Syndrome Decoding Problem with Provable Security against Quantum Adversaries	５．発行年 2019年
３．雑誌名 J. UCS	６．最初と最後の頁 294～307
掲載論文のDOI（デジタルオブジェクト識別子） 10.3217/jucs-025-03-0294	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

〔学会発表〕　計19件（うち招待講演　4件／うち国際学会　1件）

１．発表者名 横田 明卓,竹牟禮 薫, Bagus Santoso
２．発表標題 新たなNP困難な Morphism of Polynomials 問題に基づいた本人確認方式
３．学会等名 Symposium on Cryptography and Information Security (SCIS) 2023
４．発表年 2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

BAGUS SANTOSO
https://researchers.uec.ac.jp/search/detail?systemId=10274c35334f2657520e17560c007669&lang=ja
BAGUS SANTOSO
http://kjk.office.uec.ac.jp/Profiles/71/0007002/profile.html
BAGUS SANTOSO
http://kjk.office.uec.ac.jp/Profiles/71/0007002/prof_e.html

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
研究分担者	太田　和夫 (Ohta Kazuo) (80333491)	電気通信大学・大学院情報理工学研究科・特任教授 (12612)	

	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
研究協力者	大濱　靖匡 (Ohama Yasutada) (20243892)	電気通信大学・大学院情報理工学研究科・教授 (12612)	

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