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 １７ 日現在

機関番号：１２１０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１８０６

研究課題名（和文）IoT社会に資するコンパクトな耐量子計算機高機能暗号プロトコルの探求

研究課題名（英文）Compact post-quantum advanced cryptographic protocols for IoT

研究代表者
米山　一樹（Kazuki, Yoneyama）

茨城大学・理工学研究科（工学野）・教授

研究者番号：５０７５９５７９

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：コンパクトな通信量を追求した耐量子高機能暗号プロトコルとして、(1)格子問題に基づく階層型IDベース認証鍵交換方式、(2)同種写像問題に基づく片側認証匿名認証鍵交換方式、(3)同種写像問題に基づくパスワード認証鍵交換方式をそれぞれ提案した。(1)と(2)では、通常の認証鍵交換よりも複雑な条件での認証を初めて量子計算機に対して安全に実現した。また、(3)では、従来の耐量子方式よりもコンパクトな通信量を実現した。さらに、安全性証明の自動化への取り組みとして、実用されているパスワードレス認証方式であるFIDO2や非接触充電規格Qi認証プロトコルについて、自動検証ツールを用いた検証を与えた。

研究成果の学術的意義や社会的意義
従来の耐量子高機能暗号プロトコルの多くは、（耐量子でない）プロトコルに比べて鍵サイズや通信量が大きいという欠点があった。特に、IoT環境では十分なストレージ容量や通信環境の確保が難しいため、鍵サイズや通信量をどこまで削減できるかが大きな課題であった。将来的にIoT環境でも耐量子安全性が必要になると予想される。本研究で提案した耐量子高機能暗号プロトコルは同種写像問題に基づくことにより、従来の方式よりも通信量や鍵サイズを大幅に小さくすることができており、IoT環境でも利用が可能であると考えられる。また、複雑な実用認証プロトコルの検証手法の創出は耐量子以外の研究課題においても活用できる可能性がある。

研究成果の概要（英文）：As post-quantum advanced cryptographic protocols pursuing compact communication cost, (1) a hierarchical identity-based authenticated key exchange scheme based on the lattice problem, (2) a one-sided anonymous authenticated key exchange scheme based on the isogeny problem, and (3) a password authentication key exchange scheme based on the isogeny problem are proposed, respectively. In (1) and (2), authentication under more complex conditions than the usual authenticated key exchange is realized securely against quantum computers for the first time. In 3), we achieved a more compact communication cost than the conventional post-quantum scheme. Furthermore, as an approach to the automated security proofs, we verify the FIDO2, a password-less authentication method in practical use, and the Qi authentication protocol, a contactless charging standard using an automated verification tool.

研究分野：暗号理論

キーワード：耐量子　高機能暗号プロトコル　形式検証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

様々なセキュリティプロトコル内で広く用いられている RSA 暗号や Diffie-Hellman 鍵交換は大規模な量子計算機が実現すると破れてしまう。近年、各国で多額の研究投資が行われており、想定されていたよりも早く実用的な量子計算機が実現する可能性が高まっている。そのため、量子計算機に対しても安全性を保つ耐量子計算機暗号（PQC）技術が盛んに研究されている。また、アメリカ国立標準技術研究所（NIST）は 2017 年から PQC の標準化活動を開始し、現在候補の選定が進んでいる。現状最も研究が進んでいる PQC は、格子問題に基づく格子暗号であり、グループ署名やアクセス制御など様々な高機能暗号プロトコルが提案されている。高機能暗号プロトコルは、多数の機器の管理が必要な IoT 環境に有用と考えられるが、格子暗号では十分な安全性を確保するためには大きなサイズ（数十キロバイト以上）の鍵や通信量を必要とするという問題があり、IoT 環境のようなストレージ（数メガバイト程度）やネットワーク帯域（数百 bps 程度）が限られた状況には向いていないという問題がある。

２．研究の目的

本研究では、超特異楕円曲線上の同種写像に基づく PQC に着目し、PQ 安全かつ鍵サイズや通信量が従来の（非 PQ 安全）暗号技術に匹敵するほどコンパクトな高機能暗号プロトコルの実現を目的とした。同種写像暗号は量子計算機に対して耐性を持ち、格子暗号よりも鍵のサイズや通信量を小さくできる（数百バイト程度）というメリットがあるが、従来の暗号技術と異なり群作用演算を行った後の集合に代数的構造が無いという制約が大きく、これまでに実現されているのは基本的な公開鍵暗号、鍵交換や電子署名に限られており、グループ認証やアクセス制御などの IoT 環境に有用な高機能暗号プロトコルは知られていない。よって、同種写像を用いたアクセス制御可能な認証鍵交換方式の設計と安全性証明を目標とした。安全性証明においては、形式手法を応用した計算機上の検証ツールを用いた自動検証を取り入れ、より信頼性の高い厳密な安全性を保証することを目指した。

方式の設計にあたっては、従来の高機能暗号プロトコルの設計手法を参考にするが、前述の代数的制約により、新たな設計手法の考案が必要となる。また、同種写像暗号では方式設計のノウハウが少なく安全性証明の方法論が確立されていない。よって、形式手法を応用して計算機を用いた厳密な安全性検証を行うことで信頼性を確保することが学術的独自性である。既存の PQC の研究であまり考慮されてこなかった IoT 環境に適した方式を考えるところに創造性がある。さらに、新しい設計理論や計算機による PQ 安全性の検証手法の創出は、それ自体が価値を持つことに加え、PQC 以外の研究課題においても活用できる可能性があり、暗号理論に新しい観点をもたらす波及効果が期待できる。

３．研究の方法

3 つのフェーズに分けて研究を進めた。フェーズ 1（R2 年度）は、PQ 安全性の数学的定式化、フェーズ 2（R3 年度）は PQ グループ署名/認証と PQ グループ鍵管理の設計、フェーズ 3（R4 年度）は形式手法を応用した安全性証明の自動化である。それぞれのフェーズにおいて、国際会議や論文誌等で得られた成果を発表し、研究コミュニティに安全性モデルと提案方式を周知する活動を平行して行った。外部の勉強会を積極的に利用し、最新の暗号理論や形式手法に関する情報収集と本研究に対する外部からのフィードバックを得ることで効果的に研究を進めた。不可能性への抵触にも留意しつつ、適宜フェーズ間における相互フィードバックを行い、成果を継続的に改善した。

４．研究成果

(1)フェーズ 1 の研究成果

研究実施計画に基づき、量子攻撃に関する考察と新たな攻撃手法の提案、同種写像に基づくコンパクトな公開鍵暗号方式の設計と提案、に取り組んだ。

量子攻撃に関しては、高機能暗号の部品として用いられる共通鍵暗号について、量子アルゴリズムに基づく周期発見を応用した攻撃について考察した。代表的な共通鍵暗号構造である 3 ラウンド Feistel 暗号については、Simon の周期発見アルゴリズムを用いた量子識別攻撃が知られている。本研究では、Bernstein-Vazirani 量子アルゴリズムに基づく周期発見を用いて、より効率的な量子攻撃が可能であるか考察した。結果として、量子オラクルに関して強い仮定が必要となる代わりに、従来の識別攻撃より量子ビット数や計算量を改善した攻撃を示した。

公開鍵暗号方式の設計に関して、2019 年に国際会議で発表した方式について、量子ランダムオラクルモデルにおける詳細な安全性証明を与えた。また、同種写像に基づく従来の公開鍵暗号方式と計算量や暗号文長の詳細な比較を行うことによって、提案方式の優位性を明らかにした。

(2)フェーズ 2 の研究成果

研究実施計画に基づき、格子問題に基づく階層型 ID ベース認証鍵交換方式の設計と提案、同種写像問題に基づく片側認証匿名認証鍵交換方式の設計と提案、に取り組んだ。

階層型 ID ベース認証鍵交換に関しては、階層型 ID ベース鍵カプセル化メカニズムを部品として、一般的な構成法を与えた。また、安全性証明における新たなシミュレーション手法を考案し、適応的 ID 安全性を実現することを初めて示した。提案方式を格子問題に基づく具体的な鍵カプセル化メカニズムで実装することによって、初めての格子問題に基づく階層型 ID ベース認証鍵交換を実現できる。

片側認証匿名認証鍵交換に関しては、疑似ランダム関数と鍵カプセル化メカニズムを部品として、一般的な構成法を与えた。疑似ランダム関数の利用において、2 つの関数を組み合わせることにより、1 つの乱数から安全性証明上独立となる見かけ上の 2 つの乱数を生成する手法により、片側認証匿名認証鍵交換における強い安全性を示した。提案方式を前年度の成果による具体的な鍵カプセル化メカニズムで実装することによって、初めての同種写像問題に基づく片側認証匿名認証鍵交換を実現できる。

(3)フェーズ 3 の研究成果

研究実施計画に基づき、同種写像問題に基づく認証鍵交換方式の設計と提案、実用的認証プロトコルの自動安全性検証、に取り組んだ。

認証鍵交換に関しては、CRYPTO2022 で提案された同種写像問題に基づくパスワード認証鍵交換方式の構成を改良し、計算量と通信量を効率化できる方式を考案した。また、安全性証明において先行研究では通信が逐次的なケースに限定した安全性モデルでの証明となっていたが、本研究ではより汎用的な同時実行可能なケースも含む安全性モデルでの証明を行った。さらに、IoT 環境に適したビックデータに基づく認証鍵交換の一般構成を提案し、具体的に同種写像問題から実現できることを示した。

実用的認証プロトコルの自動安全性検証に関しては、次世代のパスワードレス認証規格である FIDO2 および非接触充電における充電器認証規格である Qi Authentication について、自動検証ツールを用いた形式化を与え、検証を行った。FIDO2 については従来研究で捉えられていなかった攻撃を発見し、Qi Authentication についてはなりすまし攻撃などへの耐性を明らかにした。

(4) 得られた成果の国内外における位置づけとインパクト

アクセス制御に利用できる高機能暗号として、暗号文の復号権限を受信者の属性によって制御できる属性ベース暗号がある。格子問題に基づく属性ベース暗号が知られているが、格子ベースの公開鍵暗号（数百キロバイト）以上の鍵サイズと通信量を必要とする。同種写像暗号は、PQC の候補の中で最もコンパクトな方式を実現できるが、代数的制約により基本的な公開鍵暗号などの方式しか実現されておらず、複雑なアクセス制御を行う認証鍵交換などの高機能暗号プロトコルは知られていない。

このように、PQ 安全性を満たし、かつ鍵サイズや通信量がコンパクト（1 キロバイト未満）なアクセス制御方式は現状知られていない。本研究の意義は、上記のような性質をもった IoT 環境に適した PQ 安全な高機能暗号プロトコルの初めての実現であると位置づけられる。

(5) 今後の展望

本研究では、アクセス制御可能な認証鍵交換について、数理的な安全性の定式化とコンパクトな方式を与えた。また、安全性自動検証への展開として、実用認証プロトコルの形式検証手法を与えた。しかし、提案 PQ 安全認証鍵交換方式の自動検証までは至っていないため、形式化手法の考察を進めていくことで、PQ 安全性の自動検証手法の確立を目指す。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 YONEYAMA Kazuki	４．巻 E104.A
２．論文標題 Post-Quantum Variants of ISO/IEC Standards: Compact Chosen Ciphertext Secure Key Encapsulation Mechanism from Isogenies	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 69～78
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020CIP0011	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 ISHIBASHI Ren、YONEYAMA Kazuki	４．巻 E105.A
２．論文標題 Adaptive-ID Secure Hierarchical ID-Based Authenticated Key Exchange under Standard Assumptions without Random Oracles	５．発行年 2022年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1252～1269
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021DMP0002	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 Ren Ishibashi, Kazuki Yoneyama	４．巻 E106.A
２．論文標題 Post-Quantum Anonymous One-Sided Authenticated Key Exchange without Random Oracles	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 -
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 オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Ishibashi Ren、Yoneyama Kazuki
２．発表標題 Adaptive-ID Secure Hierarchical ID-Based Authenticated Key Exchange Under Standard Assumptions Without Random Oracles
３．学会等名 ACNS 2021（国際学会）
４．発表年 2021年

１．発表者名
Ishibashi Ren、Yoneyama Kazuki

２．発表標題
Post-quantum Anonymous One-Sided Authenticated Key Exchange Without Random Oracles

３．学会等名
PKC 2022（国際学会）

４．発表年
2022年

１．発表者名
石橋 錬，米山 一樹

２．発表標題
標準モデル安全な耐量子一方向匿名認証鍵交換

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2021年

１．発表者名
石橋 錬，米山 一樹

２．発表標題
強フォワード秘匿性を満たす匿名一方向認証鍵交換

３．学会等名
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
八藤後 彬，米山 一樹

２．発表標題
Bernstein-Vazirani量子アルゴリズムに基づく周期発見を用いた3ラウンドFeistel暗号に対する量子識別攻撃とその検証

３．学会等名
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 Takanori Daiza, Kazuki Yoneyama
２．発表標題 Quantum Key Recovery Attacks on 3-Round Feistel-2 Structure without Quantum Encryption Oracles
３．学会等名 IWSEC 2022（国際学会）
４．発表年 2022年

１．発表者名 Ren Ishibashi, Kazuki Yoneyama
２．発表標題 Compact Password Authenticated Key Exchange from Group Actions
３．学会等名 ACISP 2023（国際学会）
４．発表年 2023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