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　元 年　 ６ 月 １３ 日現在

機関番号：８２６２６
研究種目：基盤研究(B)（一般）
研究期間：2014～2018
課題番号：２６２８００４６

研究課題名（和文）第三者による安全性検証が容易な暗号技術の包括的設計手法に関する研究

研究課題名（英文）Research on Cryptographic Primitives with Easily Verifiable Security

研究代表者
花岡　悟一郎（Hanaoka, Goichiro）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・研究チーム長

研究者番号：３０４１５７３１

交付決定額（研究期間全体）：（直接経費）　　13,200,000円

研究成果の概要（和文）：先端的な高機能暗号技術の複雑化に伴い、それらの安全性証明についても極めて煩雑となっており、結果として実際には安全性証明に誤りが含まれているケースが多く生じている。本研究では、安全性証明の正当性を第三者が容易に検証可能とするための、高機能暗号技術の設計方法について検討を行い、従来よりも安全性をより信頼することが可能な方式の実現に向けて有用な知見が得られた。

研究成果の学術的意義や社会的意義
暗号技術の安全性は専門的な研究者であっても正確に把握することは困難であり、したがって一般的な開発者や利用者にとっては、その実態を理解することは一層難しい状況となっている。本研究は、方式設計の段階から、安全性の検証が容易となるように暗号技術を構成するための手法について検討を行うものであり、本研究によって得られた知見により、従来に比べて信頼性の高いセキュリティ技術の実現に寄与できるものと考えられる。

研究成果の概要（英文）：Due to the complicated functionalities of advanced cryptographic primitives, the security proofs for these are likewise highly complex, and as a consequence, critical flaws are often found in these proofs. In this research, we investigated design methodologies for constructing cryptographic primitives with security proofs that can easily be verified by third parties. As a result, we showed new techniques for evaluating the security of cryptographic primitives, and proposed concrete advanced cryptographic schemes with highly reliable security.

研究分野：情報セキュリティ

キーワード：暗号・認証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

クラウドを始めとする近年の高度ネットワークサービスでは、従来の暗号技術では安全で機能的な対応が非常に困難となっている。たとえば、電子カルテのような個人の健康情報に関するデータは、医療従事者による積極的で柔軟な活用が期待される半面、必要な範囲を超えて閲覧がなされることは著しいプライバシ侵害となる。そのため、先端的暗号理論研究においては、たとえば、最終的な復号者を指定せずにデータの暗号化を行いながら、送信者が意図した範囲での自由なデータの復号を許す暗号方式等、様々な高機能付き新暗号技術の設計が活発になされている。

上記のような新たな暗号技術の設計において、それが安全であることの根拠付けとして、数学的に安全性を証明するアプローチがとられることが一般的であり、また、数学的に安全性を証明可能であることは、実利用上の必須条件ともなっている。かつて、PKCS#1 ver.1.5 のように安全性証明が与えられていない暗号技術が広く普及してしまったため、後に非常に多くの実用システムにおいて深刻な安全性上の欠陥の指摘がなされている。最近も、そのような欠陥を利用して、同技術を利用した実システムがわずか 13 分で破られたという報告がなされている。

一方、近年の暗号方式に対する機能や性能の追求とそれによる方式自体の複雑化に伴い、それらに対する安全性証明もしばしば煩雑で長大にならざるを得ない状況が生じている。たとえば、国際標準化され既に広く利用されてきたガロア／カウンタ・モード（GCM）の安全性証明に誤りがあったことが最近になって指摘されるなど、設計者によって与えられた安全性証明が直ちに信用されない風潮が強まっている。実際、そのような安全性証明の誤りが頻繁に発見されている。また、暗号理論分野に関して最も権威ある国際会議である CRYPTO2012 においては、4 件の高機能暗号の論文が発表されているが、これらは平均して 34 ページあり、そのうち安全性定義及び安全性証明の記述は平均して 24 ページ以上にのぼる。その内容も難解な数式の羅列からなっており、専門的な研究者であっても、それらの安全性証明に誤りがないことを確信することは極めて困難となっている。このことはこれらの技術の実社会への導入の大きな阻害要因と考えられる。

他方、暗号の安全性証明にとどまらず、複雑な対象（例えばソフトウェアの実装の正しさ等）をより確実に検証する技術として、計算機を用いた検証技術、所謂、機械検証への期待は近年ますます増大している。その応用も着実に広がっており、暗号分野においても本申請課題の分担者により、ISO/IEC 9798 として標準化されている認証プロトコルのいくつかについて脆弱性の存在が機械検証により発見されるなど、顕著な成果も報告されている。そのため、安全性証明の正当性を、これらの技術により検証しようとする研究が活発になされているが、現段階においては、ほとんどの研究者が安全性証明に誤りがないことをすでに確信しているような、基本的で単純な方式の安全性を機械により追検証する程度に留まっている。

したがって、高度で有用な機能をもつ新たな暗号技術の提案がなされても、それが安全であることを第三者に確信させるための手段は全く確立しておらず、また、それが解決しない限り、先端的暗号技術の導入によるネットワーク社会の高機能・高安全化は見込めない状況にある。

２．研究の目的

本研究においては、このような極めて逼迫した事態を鑑み、上記の問題を抜本的に解決することで、先端的暗号技術の導入障壁を取り除き、さまざまな高度ネットワークサービスを安心して活用できる社会の実現を促すことを目的とする。また、この目的に関して応募者らは、安全性の検証が容易であり誰もが安全であることを確信できる暗号技術を設計するための包括的方法論を構築することで問題の解決を目指す。特に、本研究においては、先端的暗号技術の安全性証明の正当性について、現在の機械検証技術で検証を行うことが困難であることの主たる理由が、機械検証技術が未成熟であるためではなく、従来の暗号技術の設計思想にこそ問題があることを見出し、そのような観点から暗号設計の方法論自体の見直しを行う。上記問題に関し、従来の他の研究においては、機械検証技術の性能を向上させるアプローチが取られていたのに対し、本研究では、暗号技術の設計方針に改良を加えることが問題解決を図ろうとする点が、特に新規性が高い。

応募者らが、上記のような研究方針の着想に至った背景には、先端的暗号技術の安全性証明テクニックの著しい高度化がある。すなわち、近年提案がなされている一連の先端的暗号技術においては、非直感的で難解な式変形が随所に登場するようになり、そもそもこれらを機械検証システムが認識できる形式に書き下すことが困難となっている。たとえば、近年提案されている高安全な公開鍵暗号方式の安全性証明において、Boneh-Boyen テクニックと呼ばれる式変形が頻繁に用いられているが、これは人間にとっても非常に非直感的であり、応募者が知る限り機械検証によって安全性証明の正当性の検証がなされた事例は知られていない。それに対し、本研究代表者である花岡は、Boneh-Boyen テクニックの使用を回避し、基本的な演算処理の直接的な使用だけで安全性証明を書き下すことが可能な公開鍵暗号方式の設計に成功している。また、同方式の安全性定義、安全性証明は合計して高々2 ページ程度となっている。したがって、同手法を発展させることで、安全性証明が人間と機械の両方にとって極めて理解が容易な高機能付き暗号技術の設計が可能になるものと思われる。

３．研究の方法

本研究においては、まず、研究代表者らにより設計がなされた簡潔な安全性証明をもつ公開鍵暗号方式に対して実際に機械検証を試みることで、暗号技術の安全性証明に機械検証を適用する際の具体的な障害の所在の詳細な特定を行い、次に、これらの障害を回避するための手法を明らかにし、基盤理論の体系化を行う。また、不可避な障害が存在する場合、それらについても明らかにする。最終段階として、構築した理論に基づき様々な高機能付き暗号技術を設計し、それらに対して機械検証を適用することで、理論の有効性を示す。

平成 26 年度においては、まず、関数暗号、代理再暗号化などの高機能付き暗号技術および暗号技術の安全性証明に対する機械検証の適用手法について、関連する国際会議への参加などにより、研究動向調査を行い、得られた知見を元に本研究目的を達成するための第一段階となる研究を行う。具体的には、花岡（本研究代表者）、今井、小川、渡邊により設計がなされた極めて簡潔な安全性証明を持つ公開鍵暗号（以下、HIOW 暗号と呼ぶ）を起点として、HIOW 暗号が極めて簡潔な安全性証明を提供可能となったことに関する、最も本質的な要因を明らかにし、より汎用的な設計手法および証明技法として確立させることを想定している。また、同手法を用いて、公開鍵暗号以外の暗号技術について、安全性証明が簡潔な方式の設計を行うことを予定する。平成 27-28 年度においては、本研究計画の第二段階として、前年度までに研究によって得られた成果をもとに、簡潔な安全性証明をもつ高機能付き暗号技術を設計するための一般的手法の確立を目指す。具体的には、まず、HIOW 暗号の安全性証明テクニックを一般化した手法について、汎用性が十分に高まるように改良を推し進めることを想定する。その後、これらの研究成果に基づき、機械検証等の適用が容易な安全性証明をもつように高機能付き暗号技術を設計するための方法論を明らかにしていく。得られた方法論に基づき、簡潔な安全性証明をもつ高機能暗号として、たとえば ID ベース暗号、電子署名、関数暗号等の設計を行い、定理証明ツールを用いた機械検証をそれらの安全性証明に適用することで同方法論の有効性の評価を行うことを予定する。さらに、この過程において洗い出された問題に対する解決方法を検討し、それを反映することで方法論を洗練していくものとする。これらの一連の研究において、適宜、中間的な成果に関して国際会議や査読付国際誌に投稿し、発表を行っていくほか、最新の研究動向についても継続的に調査を進めていく。平成 29-30 年度においては、本研究計画の第三段階として、平成 27-28 年度までに確立した方法論を用いて、実際に様々な高機能暗号技術の設計を行う。具体的には、同方法論を用いて、関数暗号、代理再暗号化、グループ署名、準同型署名等の設計を行い、それらに対して簡潔な安全性証明を与えるとともに、機械検証等を用いて容易にその正当性を容易に納得できることを確認する。これらの技術はいずれも、従来において非常に長大で繁雑な安全性証明を要したものばかりであり、本研究において構築した方法論の有効性を確認するうえで非常に適しているだけでなく、極めて有用な機能を提供するものであることから、安全性を容易に確信できる方式を実現することでネットワーク社会全体の機能性と安全性を同時に著しく向上させることが可能となる。また、これらの設計の過程において新たな問題が明らかになった場合、解決方法の検討を行い、それを反映した改良を加え、構築した方法論の完成度を高めていくものとする。なお、平成 30 年度は、研究計画の最終年度になることから、得られた成果を積極的に国際会議や査読付国際誌に投稿し、発表を行っていくものとする。

４．研究成果

（研究実績の概要・平成２６年度）

平成２６年度においては、安全性証明の理解の容易さを追求する研究の一環として、選択暗号文攻撃に対して安全な公開鍵暗号の新たな方式設計と安全性証明について研究を行ったほか、それらの知見を用いて、鍵依存平文安全性と呼ばれる高度で複雑な安全性の概念について、それに比べ比較的簡潔な安全性のみをもつ方式のみに基づき達成する手法の提案を行っている。

平成２７年度においては、極めて小さい平文空間しか持たない公開鍵暗号を用いて、一般的に、十分に大きな平文空間に拡張する変換手法の提案や、ある特定の種類の属性ベース暗号からさまざまな種類の属性ベース暗号を一般的に変換する手法などの提案を行っている。これらの手法を用いることで、変換前の基礎となる方式の安全性の検証を行うことで、自動的にさまざまな方式の安全性の検証を行ったことになり、本研究の目的の一部が達成されたものと考えられる。

平成２８年度においては、高度な機能を持つ暗号技術をより単純な機能のみを持つ暗号技術から一般的に構成するさまざまな手法の検討を進めた。具体的には、完全群構造維持署名や非対話開示可能公開鍵暗号一般的構成や、秘密情報の値のみならずサイズをも秘匿可能なマルチパーティ計算の実現手法を明らかにしている。特に、完全群構造維持署名の一般的構成を用いることで、通常の（弱い性質のみをもつ）多くの群構造維持署名を一括して完全群構造維持署名に変換可能となるため、非常に多くの新たな完全群構造維持署名を同時に設計することに成功している。また、これらの安全性についても一括して証明がなされている。さらに、範囲による条件付けが可能な属性ベース暗号の設計方法などの提案などを行った。これらの手法を用いることで、構成要素となる基本的暗号技術の安全性の検証を行うだけで自動的にさまざまな高度な機能を持つ複雑な暗号技術の安全性検証を行ったこととなり、本研究の目的の一部が達成されたものと考えられる。

平成２９年度においては、前年度までの研究により培われた安全性証明技法を適用し、具体的な公開鍵暗号技術の安全性評価に貢献を行った。特に、実用的な量子計算機の完成後も安全性を保障可能な公開鍵暗号の候補として設計された新たな暗号技術に関し、その安全性を比較的簡潔な数学的問題の困難性に帰着可能であることを明示した。また、その際、受動的安全性のみならず能動的な適応的攻撃者に対する安全性を持つことも明らかにした。また、その他、これまでに設計を行った高度な機能をもつ暗号技術についての応用についても検討を行った。具体的には、属性ベース暗号を用いた有料放送における視聴制御システムの構成について検討を行い､同システムが従来技術に比べ柔軟な視聴制御が可能となっていることを明らかにした。同システムで用いられている属性ベース暗号は機能が複雑であり、そのため安全性証明も煩雑となるが、本研究により第三者による安全性検証も容易になるものと期待できる。

平成３０年度においては、前年度までに検討を行ったさまざまな安全性証明技法について具体的暗号技術に関する安全性評価への適用をさらに推し進めることで、本研究において開発した技術の有効性を明らかにした。特に、従来手法に比べ、格段に表現力が向上された属性ベース署名を開発し、そのような複雑な機能を持つ暗号技術に対しても実際に安全性証明が可能であることを示した。さらに、安全性証明において基盤となる数学的問題への帰着アルゴリズムを構成する際に、帰着アルゴリズムの記憶領域が制限されている場合について検討を行い、そのような状況における原理的な限界を明らかにした。さらに、否認可能性と呼ばれる特殊な性質を持つグループ署名技術を用いて非対話開示機能を持つ公開鍵暗号を構成する際、自動的に実現される機能および安全性を明らかにし、その証明を行った。また、そこで得られた知見をもとに、ID ベース暗号に対して非対話開示機能を付与する手法について議論を行い、得られた方式の安全性を証明した。同様に、付加的な機能を持つ検索可能暗号を用いて、属性ベース暗号を一般的に構成可能であることを明らかにし、その安全性証明を行った。本研究により培われた安全性証明技法により安全性証明がなされた技術を用いることで第三者による安全性検証も容易になるものと期待できる。

５．主な発表論文等

〔雑誌論文〕（計０件）

〔学会発表〕（計１８件）

① Yusuke Sakai, Shuichi Katsumata, Nuttapong Attrapadung, Goichiro Hanaoka, Attribute-Based Signatures for Unbounded Languages from Standard Assumptions, 24th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018), 2018 年

②Ai Ishida, Yusuke Sakai, Goichiro Hanaoka, A Consideration on the Transformation from Deniable Group Signature to Disavowable PKENO, 2018 International Symposium on Information Theory and Its Applications (ISITA2018), 2018 年

③Yusuke Sakai, Goichiro Hanaoka, A Remark on an Identity-Based Encryption Scheme with Non-interactive Opening, 2018 International Symposium on Information Theory and Its Applications (ISITA2018), 2018 年

④Junichiro Hayata, Masahito Ishizaka, Yusuke Sakai, Goichiro Hanaoka, Kanta Matsuura, Generic Construction of Adaptively Secure Anonymous Key-Policy Attribute-Based Encryption from Public-Key Searchable Encryption, 2018 International Symposium on Information Theory and Its Applications (ISITA2018), 2018 年

⑤Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka, Fully Anonymous Group Signature with Verifier-Local Revocation, 11th Conference on Security and Cryptography for Networks (SCN 2018), 2018 年

⑥Keisuke Hara, Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka, Simulation-Based Receiver Selective Opening CCA Secure PKE from Standard Computational Assumptions, 11th Conference on Security and Cryptography for Networks (SCN 2018), 2018 年

⑦Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka, Memory Lower Bounds of Reductions Revisited, 37th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018), 2018 年

⑧Kazuto Ogawa, Sakurako Tamura, Goichiro Hanaoka, Key Management for Versatile Pay-TV

Services, 13th International Workshop on Security and Trust Management (STM 2017), 2017年

⑨Koichiro Akiyama, Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida, Goichiro Hanaoka, A Public-Key Encryption Scheme Based on Non-linear Indeterminate Equations, 24th Conference on Selected Areas in Cryptography (SAC 2017), 2017年

⑩Yuyu Wang, Zongyang Zhang, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka, How to Obtain Fully Structure-Preserving (Automorphic) Signatures from Structure-Preserving Ones, 22nd International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 2016), 2016年

⑪Kazumasa Shinagawa, Koji Nuida, Takashi Nishide, Goichiro Hanaoka, Eiji Okamoto, Size-Hiding Computation for Multiple Parties, 22nd International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 2016), 2016年

⑫Nuttapong Attrapadung, Goichiro Hanaoka, Kazuto Ogawa, Go Ohtake, Hajime Watanabe, Shota Yamada, Attribute-Based Encryption for Range Attributes, 10th Conference on Security and Cryptography for Networks (SCN 2016), 2016年

⑬Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka, On the Key Dependent Message Security of the Fujisaki-Okamoto Constructions, 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2016), 2016年

⑭Takahiro Matsuda, Goichiro Hanaoka, An Asymptotically Optimal Method for Converting Bit Encryption to Multi-Bit Encryption, 21st International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2015), 2015年

⑮Nuttapong Attrapadung, Goichiro Hanaoka, Shota Yamada, Conversions Among Several Classes of Predicate Encryption and Applications to ABE with Various Compactness Tradeoffs, 21st International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2015), 2015年

⑯Takahiro Matsuda, Goichiro Hanaoka, Constructing and Understanding Chosen Ciphertext Security via Puncturable Key Encapsulation Mechanisms, Twelfth Theory of Cryptography Conference (TCC 2015), 2015年

⑰Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka, Efficient Key Dependent Message Security Amplification Against Chosen Ciphertext Attacks, 17th International Conference on Information Security and Cryptology (ICISC 2014), 2014年

⑱Kazuki Yoneyama, Goichiro Hanaoka, Compact Public Key Encryption with Minimum Ideal Property of Hash Functions, Eighth International Conference on Provable Security (ProvSec 2014), 2014年

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

○取得状況（計０件）

〔その他〕
ホームページ等
https://www.itri.aist.go.jp/crypto/researcher/hanaoka.html

６．研究組織

(1)研究分担者
研究分担者氏名：Attrapadung Nuttapong
ローマ字氏名：アッタラパドゥン　ナッタポン

所属研究機関名：国立研究開発法人産業技術総合研究所
部局名：情報・人間工学領域
職名：研究チーム長
研究者番号（8 桁）：40515300

研究分担者氏名：吉田　真紀
ローマ字氏名：ヨシダ　マキ
所属研究機関名：国立研究開発法人情報通信研究機構
部局名：サイバーセキュリティ研究所セキュリティ基盤研究室
職名：主任研究員
研究者番号（8 桁）：50335387

研究分担者氏名：松田　隆宏
ローマ字氏名：マツダ　タカヒロ
所属研究機関名：国立研究開発法人産業技術総合研究所
部局名：情報・人間工学領域
職名：主任研究員
研究者番号（8 桁）：60709492

研究分担者氏名：縫田　光司
ローマ字氏名：ヌイダ　コウジ
所属研究機関名：東京大学
部局名：大学院情報理工学系研究科
職名：准教授
研究者番号（8 桁）：20435762

研究分担者氏名：江村　恵太
ローマ字氏名：エムラ　ケイタ
所属研究機関名：国立研究開発法人情報通信研究機構
部局名：サイバーセキュリティ研究所セキュリティ基盤研究室
職名：主任研究員
研究者番号（8 桁）：30597018

研究分担者氏名：松尾　真一郎
ローマ字氏名：マツオ　シンイチロウ
所属研究機関名：国立研究開発法人情報通信研究機構
部局名：社会還元促進部門
職名：統括
研究者番号（8 桁）：20553960

(2)研究協力者
なし