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

平成　２９　年　　６　月　　１　日現在

機関番号：　１２１０１
研究種目：　研究活動スタート支援
研究期間：　2015～2016
課題番号：　１５Ｈ０６０６３

研究課題名（和文）フェイルセーフ暗号プロトコルの設計と安全性証明

研究課題名（英文）Construction and Security Proof of Fail-Safe Cryptographic Protocols

研究代表者
米山　一樹（Yoneyama, Kazuki）

茨城大学・工学部・准教授

研究者番号：５０７５９５７９

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：擬似ランダム関数を利用して乱数を秘密鍵と混ぜ合わせる手法やハッシュ関数の理想的な性質の一部だけを使って暗号文長を短くする手法などを利用し、秘密情報漏洩時でも安全な認証鍵交換、署名生成時の乱数漏洩時でも安全なグループ署名、脆弱性を持つハッシュ関数を用いても暗号文長を短くできる公開鍵暗号などを設計した。また、形式検証による安全性自動検証にも取り組み、グーグル社のブラウザ上で暗号化通信に用いられているQUICについて安全性解析を行い、従来の安全性モデルの不備を発見した。

研究成果の概要（英文）：By using the method to mix temporary randomness and the static secret key with pseudo-random functions and the method to shorten the ciphertext length with a part of ideal properties of idealized hash functions, we construct an authenticated key exchange secure under the secret key leakage, a group signature secure under leakage of randomness in the signature generation, and a compact public key encryption even with vulnerable hash functions. Moreover, we study automated security verification using formal methods, and find a flaw of the previous security model of QUIC which is used to establish secure channels in the browser of Google inc.

研究分野：　暗号理論

キーワード：　暗号プロトコル　フェイルセーフ性

１．研究開始当初の背景

クラウドやモノのインターネットの普及などネットワーク環境が高度化・複雑化するに従って、ネットワーク上で提供されるサービス・システムもまた多様化・複雑化している。公開鍵暗号や電子署名などの暗号理論における基本的な部品（以下、暗号プリミティブとよぶ）を組み合わせることで、こうしたネットワークに基づくシステム（以下、暗号プロトコルとよぶ）を安全に実現することができる。例えば、これまで、柔軟なアクセス制御機能を備えた認証鍵交換、公平に電子商取引を行う電子チケット交換プロトコル、計算を外部プロキシに委託可能な証拠証明方式などを設計・提案してきている。その他にも電子投票やオークションなど様々な暗号プロトコルが提案されてきているが、既存の方式の多くは、各ユーザが自分の秘密情報を適切に管理し、またシステム管理者は自らの権限を悪用しないという前提で設計されている。

しかし、現実社会では、管理者が悪意を持ってシステムにバックドアを仕込む、様々なシステムにライブラリとして使用されていた OpenSSL の脆弱性によりユーザの秘密情報が漏洩する、など、暗号プロトコル設計者が想定していなかった事態が最近ではしばしば発生している。そのため、たとえ安全な暗号プロトコルを使用していたとしても、これらの適切でない運用や正常系ではない事態（以下、インシデントとよぶ）が起きた場合には何も安全性を保証できなくなってしまうという問題がある。

２．研究の目的

本研究では、インシデントが起きたとしても、被害を最小限に留めることができる「フェイルセーフ性」という性質を暗号プロトコルの新たな要件として考え、フェイルセーフ性を満たす暗号プロトコル（以下、フェイルセーフ暗号プロトコルとよぶ）を新たに設計することを目的とした。すなわち、フェイルセーフ性を満たしていれば、インシデント発生時においても、何らかの（元より弱い）安全性を保持することが可能とする。また、新しい暗号プロトコルを提案する際には、数学的に安全性を証明する必要がある。よって、フェイルセーフ性を適切に捉えた安全性を定義し、設計した安全性を証明・評価する必要がある。

具体的なフェイルセーフ性の例としては、例えば漏洩耐性が挙げられる。一部の秘密情報が漏れたとしても何らかの安全性を保証できるようにする必要がある。また、漏洩耐性の他に、ユーザの誤使用や OpenSSL のような実装ミス、暗号ハードウェアに対するタンパリング、悪意のある管理者などを考慮する必要がある。すべての種類のインシデントに対するフェイルセーフ性を同時に扱うことは困難なので、本研究ではまずそれぞれのケースについて、フェイルセーフ暗号プロトコルを設計し、様々な個々の種類のインシデントに対して対応した方式が構成可能であることを明らかにすることを目標とした。

また、インシデントに応じた安全性の段階的な変化について、どのような弱め方が現実環境で許容されうるかを考察する。例えば、認証鍵交換プロトコルの結果生成されたセッション鍵の値が、インシデント前の元々の安全性では攻撃者に 1 ビットも分からないことを保証していたのに対し、インシデント後は、何らかの部分情報は分かるかもしれないがセッション鍵そのものは導出できない、という安全性に弱まるような状態であれば、直ちになりすまし等が可能となるわけではないため、現実的には許容可能であろうと思われる。このように、プロトコルの種類に応じて、現実環境での利用のされ方を考慮に入れた上で、新しい安全性を定義することで、適切な安全性モデルを数学的に明らかにする。

さらに、フェイルセーフ暗号プロトコルでは安全性定義が複雑になると予想されるので、安全性証明の見落としやミスが発生しやすくなるため、安全性証明を簡単にするための工夫も必要となってくる。よって、証明を簡単化する手法をフェイルセーフ暗号プロトコル用に新たに考案し明らかにする。

３．研究の方法

2 つのフェイズに分けて研究を進めた。フェイズ 1 は、具体的なフェイルセーフ暗号プロトコルの設計であり、フェイズ 2 は安全性モデルの確立と安全性証明を簡単化する手法の提案である。平成 27 年度は主にフェイズ 1 を進め、インシデントの分類、フェイルセーフ性が必要とされる暗号プロトコルの選定、具体的な設計を行い、計算機シミュレーションによる実証実験を行った。平成 28 年度は主にフェイズ 2 を進め、安全性の数学的定式化、形式手法による安全性証明の簡単化を行い、計算機を用いた安全性自動検証実験を行った。両フェイズにおいて、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フェイルセーフ暗号プロトコルの概念を普及させ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、適宜フェイ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) 研究の主な成果

①フェーズ 1 の研究成果

研究計画にそって、具体的なフェイルセーフ暗号プロトコルの設計を行った。まず、インシデントを分類し、秘密情報の漏洩とハッシュ関数の脆弱性に注目した。次に、設計対

象のプロトコルとして、認証鍵交換、公開鍵暗号、グループ署名などに対して、フェイルセーフ性を持たせる意義があることを考察した。

選定したプロトコルについて、フェイルセーフ性を持つような方式の設計を行った。擬似ランダム関数を利用して乱数を秘密鍵と混ぜ合わせる手法やハッシュ関数の理想的な性質の一部だけを使って暗号文長を短くする手法などを利用し、秘密情報漏洩時でも安全な認証鍵交換、署名生成時の乱数漏洩時でも安全なグループ署名、脆弱性を持つハッシュ関数を用いても暗号文長を短くできる公開鍵暗号などを設計した。

②フェーズ 2 の研究成果

安全性モデルの確立と安全性証明の簡単化を行った。まず、動的マルチキャスト鍵配送について、フェイルセーフ安全性のモデル化と具体的方式の構成を行った。提案モデルでは、過去のセッション鍵・長期秘密鍵・短期秘密鍵・セッション中の内部状態などが運用ミスなどによって漏洩したとしても、組み合わせ次第によっては、セッション鍵の秘匿性が保たれるように定式化した。

また、安全性証明を簡単にするアプローチとして、計算機による安全性自動検証技術に着目した。インターネット上で実際に使用されているセキュリティプロトコルである TLS や QUIC の安全性を形式検証を用いて検証し、TLS に対しては既知の攻撃が自動検証ツールで検出できること、QUIC に対しては安全性の定義の不備を発見した。

(2) 得られた成果の国内外における位置づけとインパクト

フェイルセーフ性により、インシデント発生時でもシステムの安全性は即座には破綻しないため、管理者がインシデントに気づくのが遅れたとしても、安全な状態への復帰（鍵の再発行や新たなシステムの導入）まである程度の安全性を保つことができる。社会的には、震災を経てシステムのレジリエンスが重要視されるようになってきており、フェイルセーフ性を満たす暗号プロトコルの使用は、レジリエンスを高める有用な技術になり得ると期待できる。

また、学術的観点では、秘密情報や運用の適切性をどの程度厳重に守るかという管理のコストと保証できる安全性のトレードオフを実現するためのテクニックを創出することにより、暗号理論に新しい観点をもたらし、フェイルセーフ性を実現する以外の研究課題においてもテクニックの転用が可能になると期待できる。特に、QUIC は実際に広く使用されている重要なセキュリティプロトコルであるため、その安全性を明らかにすることは非常に意義があり、実際に国際会議で発表した際には、標準化策定を行っているコミュニティからも多数の質問を受けた。

(3) 今後の展望

本研究では、いくつかのプロトコルに対してフェイルセーフ安全な方式を設計したが、対象外としたプロトコルに対してもフェイルセーフ性が必要な場合が考えられる。よって、その他のプロトコルに対しても、フェイルセーフ安全性のモデル化と設計を進めていく必要がある。

また、実用されているセキュリティプロトコルに対する安全性自動検証に成功したが、フェイルセーフ安全性の検証までは至らなかった。今後は、安全性のモデル化の知見と自動検証の知見を合わせて。フェイルセーフ安全性の自動検証の研究を進めていく予定である。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

① Kazuki Yoneyama 、『 Computational Soundness of Asymmetric Bilinear Pairing-based Protocols』、IEICE Trans. on Fundamentals、vol.E100.A, No.9,2017、査読有

② Jae Hong Seo, Keita Emura, Keita Xagawa, Kazuki Yoneyama、『Accumulable optimistic fair exchange from verifiably encrypted homomorphic signatures』、International Journal of Information Security 、 Online First,2017、査読有

③ Naoto Itakura, Kaoru Kurosawa, Kazuki Yoneyama 、『 Oblivious Polynomial Evaluation in the Exponent, Revisited』、IEICE Trans. on Fundamentals 、vol.E100.A, No.1, pp.26-33,2017、査読有

④ Kazuki Yoneyama、『"Formal Modeling of Random Oracle Programmability and Verification of Signature Unforgeability Using Task-PIOAs 』、International Journal of Information Security、Online First,2017、査読有

〔学会発表〕（計 16 件）

① Hideki Sakurada, Kazuki Yoneyama, Yoshikazu Hanatani, Maki Yoshida 、『 Analyzing and Fixing the QACCE security of QUIC』、SSR 2016、2016.12.5、US National Institute of Standards and Technology（Gaithersburg・アメリカ）

② Kazuki Yoneyama, Reo Yoshida, Yuto Kawahara, Tetsutaro Kobayashi, Hitoshi Fuji, Tomohide Yamamoto 、

『 Multi-Cast Key Distribution: Scalable, Dynamic and Provably Secure Construction 』、 ProvSec 2016 、 2016.11.10 、 Nanjing Shuangmenlou Hotel（南京・中国）

③ Shogo Kimura, Kazuki Yoneyama 、『Security Proof of Identity-based Signature under RSA Assumption, Reconsidered』、ISITA 2016、2016.10.30、Hyatt Regency Monterey Hotel（モントレー・アメリカ）

④ Kaoru Kurosawa, Keisuke Sasaki, Kiyohiko Ohta, Kazuki Yoneyama 、『 UC-Secure Dynamic Searchable Symmetric Encryption Scheme』、IWSEC 2016、2016.9.12、sola city Conference Center（東京都・千代田区）

６．研究組織

(1)研究代表者

米山　一樹（YONEYAMA　KAZUKI）
茨城大学・工学部・准教授
研究者番号：50759579