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　２ 年　 ６ 月　 ９ 日現在

機関番号：１２１０１
研究種目：若手研究(B)
研究期間：2017～2019
課題番号：１７Ｋ１２６９５

研究課題名（和文）エンドツーエンド暗号化通信の数理的安全性モデルに関する研究

研究課題名（英文）Study on Formal Security Model of End-to-End Encryption

研究代表者
米山　一樹（YONEYAMA, KAZUKI）

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）　　3,100,000円

研究成果の概要（和文）：エンドツーエンド暗号化通信の代表的方式であるLINE encryptionの長期鍵が漏れた後の安全性を保証するフォワード安全性について、形式手法に基づく安全性の定式化と検証を行い、既存研究では示されていなかった明示的な攻撃を発見した。
また、エンドツーエンド暗号化通信に関連する実利用方式として、ICカード-リーダ/ライタ間の認証プロトコルについての安全性評価を行い、認証途中で生成されたセッション鍵を外部システムで利用するなどの運用を行った場合の危険性を明らかにした。
さらに、非同期環境におけるグループ鍵共有について、IDベース暗号基盤に基づく方式、証明書不要暗号基盤に基づく方式をそれぞれ設計した。

研究成果の学術的意義や社会的意義
従来では、サービス提供者はそれぞれが独自の基準で曖昧な安全性を主張していたため、ユーザは「本当に主張されている安全性が満たされているか？」について知ることは困難であった。もし致命的な脆弱性により想定外の攻撃が行われた場合、大規模な被害が発生し混乱や社会不安を引き起こすことが懸念される。本研究により、数理的に評価可能な安全性をモデル化することにより、ユーザは客観的に各サービスが満たす安全性を比較し、各々のユーザが望む安全性を備えたサービスを取捨選択することができる。将来的な想定外の被害を未然に防ぐことに繋がり、ユーザを守ると同時にサービス提供者にとっても訴訟などのリスクを避けることができる。

研究成果の概要（英文）：We formalize and verify the forward security (which guarantees the secrecy of the session key after revealing static private keys) of LINE encryption as a representative end-to-end encryption scheme and find a new explicit attack.
Also, we evaluate the security of an authentication protocol between IC-card reader/writer as a practical scheme related to end-to-end encryption and clarify vulnerability when the session key generated in an authentication session is used in other external systems.
Moreover, we construct ID-based and certificateless group key exchange protocols secure in asynchronous networks.

研究分野：暗号理論

キーワード：形式手法

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

インターネット上で安全に暗号化通信をするための技術として、Diffie-Hellman 鍵交換を始めとした認証鍵交換方式が古くから研究されてきた。これまで担当者は、漏洩耐性を備えた高安全方式、耐量子計算機安全方式、パスワードに基づく方式などを設計・提案してきた。ほとんどの既存の認証鍵交換方式は、SSL/TLS のように 2 者が直接通信し共通のセッション鍵を生成する通信モデルである。一方で、近年では手軽なリアルタイムコミュニケーション手段として、LINE や WhatsApp などのメッセージングサービスが急速に普及し利用されるようになってきた。これらのサービスでは、ユーザ同士は直接通信せずサーバを介して通信が行われ、サーバは送信者から送られてきたメッセージやその他の情報を受信者に転送する。よって、ユーザ-サーバ間で SSL/TLS などの秘匿通信を用いたとしても、サーバは通信内容を全て見ることが可能となる。しかし、サービス提供者が政府機関に対してユーザの通信内容を提供しているとする訴えが起きるなど、プライバシ保護に対する社会的な要請を受けて、中継するサーバにすら通信内容を秘匿することを目的としてエンドツーエンド（E2E）暗号化通信が提供されるようになってきた。例えば、LINE は Letter Sealing、WhatApp は Signal Protocol という E2E 暗号化通信方式を 2016 年から導入している。

しかし、E2E 暗号化通信では統一的な指標による厳密な安全性評価が行われておらず、サービス提供者の主張する安全性が満たされているか明らかではない。もしこれらの方式が未知の脆弱性を内包している場合、脆弱性を攻撃者に悪用され、なりすましや情報漏洩などの被害をユーザが受ける危険性がある。認証鍵交換では暗号理論に基づく数理的安全性モデルが確立され、標準化されている方式の多くは安全性が明らかになっているが、通信モデルや利用環境が異なるため E2E 暗号化通信にはそのまま適用できない。

２．研究の目的

本研究では、E2E 暗号化通信における統一的安全性指標の確立と既存・新規方式の厳密な安全性評価・分類を目的とする。従来の（主にサービス提供者による）安全性指標は自然言語による定性的なものだったのに対して、数理的に安全性をモデル化する必要がある。また、既存の実用化されている方式に対して、数理モデルに基づき安全性を評価・比較できることが望ましい。既存方式を上回る安全性と効率を持つ次世代の E2E 暗号化通信方式も今後必要となると思われる。

数理的モデルの定式化にあたって、E2E 暗号化通信では様々な攻撃が考えられる。例えば、盗聴による情報漏洩や中間者によるなりすましなどの典型的なものから、ユーザの秘密情報を奪取した上で過去のセッション鍵の情報を得ようとするような入り組んだ攻撃なども考慮する必要がある。よって、「安全性」と一言で言っても、様々なレベルが存在する。本研究では既存方式の安全性を細かく分類することを目標としているため、モデル化を行う前に E2E 暗号化通信における起こりうる攻撃パターンを網羅的に抽出し、満たす安全性レベルに応じて複数の安全性モデルを暗号理論や形式手法を利用して定式化する。これによりきめ細かい安全性の比較が可能となる。

既存方式の安全性評価にあたっては、主要な方式の仕様に対して定式化した数理的モデルに従い評価を行う。各国・地域で高いシェアを持つメッセージングサービスの安全性を網羅的に評価し、統一的指標による比較が可能な安全性の分類を初めて与えることを目標とする。効率的に評価を行うため、計算機を用いた自動検証を活用する。

安全性評価の結果として、モデル・方式が長年議論されてきた認証鍵交換とは違い、既存の E2E 暗号化通信方式では漏洩耐性などの高安全性と効率性を両立した方式は存在しないことが予想される。よって、認証鍵交換設計で培った知見を活かし、新しい次世代向け方式を設計する。提案方式は、定式化したモデルにおける最強の安全性と既存方式に伍する効率性を両立することを目指す。

３．研究の方法

3 つのフェイズに分けて研究を進めた。フェイズ 1（H29 年度）は、E2E 暗号化通信における防ぐべき攻撃パターンの具体化と安全性モデルの定式化、フェイズ 2（H30 年度）は評価対象の仕様調査と安全性評価、フェイズ 3（H31 年度）は次世代方式の設計である。それぞれのフェイズにおいて、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 E2E 暗号化通信の数理的モデルと次世代方式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)フェーズ 1 の研究成果

研究実施計画に基づき、攻撃パターンの網羅的分類、形式手法に基づく記号論的安全性モデルの定式化、に取り組んだ。

特にエンドツーエンド暗号化通信の代表的な方式として、LINE encryption を取り上げ、既知のなりすまし攻撃（spoofing）と再送攻撃（reply）に関する調査を行い、形式手法に基づく安

全性を定式化した。定式化は一般的な中間者攻撃を捉えるため、Dolev-Yao モデルに基づいて行った。さらに、長期鍵が漏れた後の安全性を保証するフォワード安全性についても、定式化を行った。ホワイトペーパーを用いて LINE encryption の仕様を調査し、定式化した記号論的安全性モデルを満たしているかの検証を行った。自動検証ツールとしては、扱える安全性の汎用性を考慮し、ProVerif を用いた。なりすまし攻撃、再送攻撃、フォワード安全性についてそれぞれ検証を行ったところ、なりすまし攻撃と再送攻撃については既知の攻撃を検出した。またフォワード安全性については、既存研究では明示的な攻撃は示されていなかったが、ProVerif により新たな攻撃を発見した。

(2)フェーズ 2 の研究成果

研究実施計画に基づき、主要な方式の仕様調査、記号論的安全性の計算機自動検証、計算理論的安全性の証明、各方式の安全性・効率性の比較、に取り組んだ。

エンドツーエンド暗号化通信に関連する実利用方式として、IC カード-リーダ/ライタ間の認証プロトコルについて安全性評価に取り組んだ。結果として、認証鍵交換としてプロトコルを利用した場合、過去のセッション鍵が漏洩することで、過去の認証結果を再利用する事が可能であることを示した。また、暗号理論的な認証鍵交換の安全性モデルである Bellare-Rogaway モデルにおいて、認証再利用がどのように定式化できるかを明らかにした。上記の結果より、本来の認証だけの用途で用いる場合には問題ないが、認証途中で生成されたセッション鍵を外部システムで利用するなどの運用を行った場合の危険性が明らかになった。

(3)フェーズ 3 の研究成果

研究実施計画に基づき、次世代エンドツーエンド暗号化通信方式の設計、検証実験・安全性証明、に取り組んだ。

エンドツーエンド暗号化通信では、非同期環境においてグループ間でセッション鍵を共有する必要があるが、お互いの公開鍵証明書を事前に共有するのは難しいため、証明書無しで鍵共有する方式の設計に取り組んだ。結果として、ID ベース暗号基盤に基づく方式、証明書不要暗号基盤に基づく方式をそれぞれ設計した。非同期で通信を行うため送信者はサーバを介して受信者に任意のタイミングでセッション鍵を共有するための情報を送信する必要があるが、サーバにセッション鍵を漏らさずに実現するため、ブラインド鍵カプセルメカニズムを応用して、方式設計を行った。

(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

E2E 暗号化通信は大量のユーザに実利用され、社会インフラとして大変重要なプロトコルであるにも関わらず、これまで数理的な安全性を厳密に定式化・評価した研究はなかった。特に、秘密情報の一部が漏れた場合の安全性などは想定されていない。担当者がこれまで培ってきた認証鍵交換における数理的安全性の定式化に関する知見を用いて、漏洩耐性を含む初めての数理的定式化を与えたことが学術的な特色である。

安全性の評価においては、認証鍵交換と同様に暗号理論に基づく計算量理論的な解析手法を利用することに加えて、多数の既存方式を効率的に評価するために形式手法に基づく計算機自動安全性検証を活用した。自動検証は暗号プロトコルの安全性検証に活用されつつあるものの、検証例はまだまだ少ない。よって、E2E 暗号化通信のような実用的なプロトコルに対して自動検証が有効であることが示せた学術的なインパクトは大きい。

さらに、高安全性と効率性を両立する次世代方式の設計は、システムや要件の違いから認証鍵交換の既存のテクニックだけでは達成困難であったため、新しい設計理論を考案する必要があり、学術的にチャレンジングな課題であった。

(5) 今後の展望

本研究では、代表的な E2E 暗号化通信方式について、数理的な安全性の定式化と形式手法による安全性検証を与えた。しかし、汎用的な方式に対する安全性の定式化までは至っていないため、その他の方式も含めて定式化と検証を進めていくことで、汎用的な数理的安全性の確立を目指す。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Cheng Shi, Kazuki Yoneyama	４．巻 E102.D, No.8
２．論文標題 Verification of LINE Encryption Version 1.0 using ProVerif	５．発行年 2019年
３．雑誌名 IEICE Trans. on Information and Systems	６．最初と最後の頁 1439-1448
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018FOP0001	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6件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 中林 美郷，小林 鉄太郎，村上 啓造，岡野 裕樹，米山 一樹
２．発表標題 IDベース非同期多者間鍵交換
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 2020年

１．発表者名 岡野 裕樹，小林 鉄太郎，村上 啓造，中林 美郷，米山 一樹
２．発表標題 証明書不要非同期グループ鍵交換プロトコル
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 2020年

１．発表者名 Cheng Shi, Kazuki Yoneyama
２．発表標題 Verification of LINE Encryption Version 1.0 Using ProVerif
３．学会等名 IWSEC（国際学会）
４．発表年 2018年

１．発表者名
勝野 凌介，米山 一樹

２．発表標題
ICカードとリーダ/ライタ間の認証プロトコルにおける認証再利用と暗号理論的安全性モデルの関係

３．学会等名
電子情報通信学会情報セキュリティ研究会

４．発表年
2019年

１．発表者名
師 成，米山 一樹

２．発表標題
LINE Encryption Version 1.0のProVerifによる検証

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
2018年

１．発表者名
岡野 裕樹，小林 鉄太郎，西巻 陵，吉田 麗生，米山 一樹

２．発表標題
ビジネスチャットにおけるエンドツーエンド暗号化を実現するためのグループメッセージングプロトコルの提案

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
2018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