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　２６　日現在

機関番号：　１７３０１
研究種目：　若手研究(B)
研究期間：　2014～2016
課題番号：　２６７３００６７

研究課題名（和文）計算機を用いた暗号プロトコルの安全性に関する研究

研究課題名（英文）Computer-based Evaluation of Cryptographic Protocol Security

研究代表者
荒井　研一（ARAI, Kenichi）

長崎大学・工学研究科・助教

研究者番号：６０６４５２９０

交付決定額（研究期間全体）：（直接経費）　　1,500,000円

研究成果の概要（和文）：近年、暗号プロトコルはさまざまな要求に答えるために日々複雑になってきている。暗号プロトコルが複雑になるにつれて安全性評価は困難になるため、人為的なミスが発生しやすくなる。そのため、評価に誤りがある論文が多数存在し問題となっている。そこで本研究では、計算機を用いた暗号プロトコルの安全性評価の有効性に着目し、暗号プロトコルの安全性評価を厳密に行うことができる手法の実現に向けた検討を行った。本研究の成果は、暗号プロトコルの複雑化に伴う評価の誤りの増加といった深刻な問題に対して、有効な解決手段を提供するものとなる。

研究成果の概要（英文）：The complexity of cryptographic protocols has increased in recent years in response to various requirements. This increase in complexity makes the evaluation of cryptographic protocol security difficult and increases the likelihood of human error. For this reason, the problem has arisen that many studies contain evaluation errors. This study focuses on the effectiveness of computer-based evaluation of cryptographic protocol security and aims to realize a method for rigorously conducting such evaluations. The results of this research will provide an effective solution for the serious problem of the increase in evaluation errors due to the growing complexity of cryptographic protocols.

研究分野：　情報セキュリティ、フォーマルメソッド

キーワード：　暗号プロトコル　安全性　フォーマルメソッド　自動検証　自動証明　ProVerif　Mizar　CryptoVerif

## １．研究開始当初の背景

近年、さまざまな要求に答えるために暗号プロトコルは日々複雑になってきている。暗号プロトコルが複雑になるにつれて安全性評価（証明）は困難になるため、人為的なミスが発生しやすくなる。そのため、証明に誤りがある論文が多数存在し問題となっている。

暗号プロトコルの安全性証明のアプローチには、計算論的モデルと記号論的モデルがある。計算論的モデルは、確率的多項式時間チューリング機械を用いて安全性証明を行う。計算論的モデルは、暗号学研究者の標準的な方法として利用されてきた。しかしながら、暗号プロトコルが複雑になるにつれて安全性証明は困難になるため、証明に誤りがある論文が多数存在し問題となっている。一方、記号論的モデルは暗号プロトコルに用いられる暗号プリミティブを絶対に破られないといったブラックボックス（理想的なもの）として扱い安全性証明を行う。記号論的モデルは、形式的な取り扱いが容易であるため計算機を用いて安全性証明を自動化できるといった利点がある。しかしながら、暗号プリミティブをブラックボックスとしているため、計算論的モデルでは可能であった暗号プリミティブの特徴を利用した攻撃に対する議論を行うことができない。そのため、暗号学研究者にはあまり受け入れられてこなかった。

近年、計算論的モデルに対する記号論的モデルの有効性が注目されるようになり、計算論的モデルと記号論的モデルを融合する試みが盛んに研究されている。これらのモデルを融合する試みの一つとして、直接的手法がある。直接的手法は、計算論的モデルにおける安全性証明を形式体系の中で定式化した上で記号処理を適用するものである。直接的手法フレームワークの一つとして、Blanchet らの手法があげられる。CryptoVerif は、彼らの手法を実装したソフトウェアである。彼らは、計算論的モデルである game 列を用いて安全性証明を行う手法において、記号処理を用いて世界で初めて自動証明することに成功した。

暗号プロトコルの安全性証明において証明の誤りをなくすには、計算機を用いた安全性証明が有効である。なぜなら、従来からの手書きによる証明では暗号プロトコルが複雑になるにつれて証明が困難になるため人為的なミスが発生しやすくなるが、計算機を用いた証明は機械的に証明が行えるため証明による人為的なミスの減少が期待できるためである。CryptoVerif は、計算論的モデルである game 列を用いた安全性証明及びその自動証明も可能であるため非常に注目されている。CryptoVerif に代表されるような計算機を用いた暗号プロトコルの安全性証明は、証明の誤りをなくすことができるといった大いなる可能性を秘めている。しかしながら、計算機を用いた暗号プロトコルの安全性証明に関する研究は、注目を集めているものの発展途上である。また、CryptoVerif においても非常に有効なソフトウェアではあるが、厳密性に欠ける部分も存在する。よって、計算機を用いた暗号プロトコルの安全性証明について調査・研究を行い、さまざまな可能性を探り、計算機を用いた暗号プロトコルの安全性証明を厳密にできる手法の実現に向けた検討を行うことの意義は計り知れない。

## ２．研究の目的

CryptoVerif は、証明対象となる暗号プロトコルへの攻撃モデル（初期 game）及び安全性の根拠となる暗号プリミティブの安全性を与えると、暗号プロトコルの安全性証明を自動証明できる。しかしながら、安全性の根拠となる暗号プリミティブの安全性は、観測等価性を満たす２つのプロセスとして記述する必要があり、その記述及びその記述が観測等価性を満たすことの証明は、人手で行わなければならない。観測等価性を満たすことの記述及びその証明は CryptoVerif では自動証明できないため、それらに誤りが存在すると正しい結果を得ることができない。この欠点を補うために、本研究では他ソフトウェア（ツール）援用による欠点解決を試みる。

研究代表者は、計算機を用いた暗号プロトコルの安全性証明においてアプローチ毎に研究を行ってきた。計算論的モデルにおいては、形式化記述された数学定理の証明の正しさを機械的に検証するプルーフチェッカと呼ばれるソフトウェアの一種である Mizar を用いた研究、記号論的モデルにおいては、Blanchet らによって実装された形式モデルに基づくソフトウェアである ProVerif を用いた研究、計算論的モデルと記号論的モデルを融合する試みにおいては、CryptoVerif を用いた研究を行ってきた。これらの研究に従事する上で、各ソフトウェアにおける利点欠点がみえてきた。さらに、研究を進めていく上で、あるソフトウェアの欠点を他のソフトウェアの利点で補うことで暗号プロトコルの安全性証明を厳密にできる手法の実現可能性を見出した。以上より、CryptoVerif の観測等価性を満たすことの証明に他ソフトウェアを援用することにより、計算機を用いた暗号プロトコルの安全性証明を厳密にできる手法の実現を目指すことが本研究の目的である。

## ３．研究の方法

計算機を用いた暗号プロトコルの安全性証明を厳密にできる手法の実現に向けた検討を行うために、以下の２つの方針に分けて研究を行う。

（1）Mizar 援用による観測等価性を満たすことの証明の実現に向けた検討：

Mizar は、厳密な数学的形式記述が可能であり、なおかつ強力な推論機能を有している。そのため、観測等価性を満たすことの証明の形式記述を行い証明の正しさを検証することにより、証明の誤りをなくすことが期待できる。なお、観測等価性を満たすことの証明には暗号プリミティブが関係している。そのため、多数の暗号プリミティブを取り扱うためには、さまざまな数学的な定義及び定理が必要となる。しかしながら、Mizar には暗号プリミティブを取り扱うために必要な数学的な定義及び定理のライブラリはいくつか存在するものの Mizar を用いた観測等価性を満たすことの証明を実現するには不十分である。よって、暗号プリミティブを取り扱うために必要な数学的な定義及び定理のライブラリを充実させることにより、Mizar 上での観測等価性を満たすことの証明の実現を目指す。

（2）ProVerif 援用による観測等価性を満たすことの証明の実現に向けた検討：

CryptoVerif は「ある暗号プロトコルがある安全性を満たす」ということを証明できるソフトウェアであり、暗号プロトコルに脆弱性が存在した場合にその攻撃方法を導出することはできない。攻撃方法を導出できるソフトウェアとして ProVerif がある。よって、ProVerif を用いた安全性評価も同時に進め、攻撃方法に関しても考慮することにより、CryptoVerif を用いた暗号プロトコルの安全性証明のさらなる厳密化の可能性を探る。さらに、さまざまな暗号プロトコルに対する安全性評価を行うことで、ProVerif 上での観測等価性を満たすことの証明の実現を目指す。

## 4．研究成果

（1）Mizar 援用による観測等価性を満たすことの証明の実現に向けた検討：

CryptoVerif における観測等価性を満たすことの証明を Mizar 上で実現するために、不足しているライブラリの充実化を図った。実数値関数上の差分（forward difference、backward difference、central difference）の形式化記述は既に存在するが、ベクトル値関数上の差分の形式化記述は存在しない。ベクトル値関数上の差分は、観測等価性を満たすことの証明（特に、共通鍵暗号方式の安全性）を実現するために重要であるため、その形式化記述を行った。結果として、不足しているライブラリの充実化を図ることに成功した。

本研究期間において、不足しているライブラリの充実化を図ったが、不足しているライブラリが多数存在したため、Mizar 援用による観測等価性を満たすことの証明を実現するに至らなかった。しかしながら、上記の成果を含め、ライブラリは着実に整備されつつあるため、引き続きライブラリの充実を図り、Mizar 援用による観測等価性を満たすことの証明を実現する。以上より、Mizar 援用による観測等価性を満たすことの証明の実現は今後の課題としたい。

（2）ProVerif 援用による観測等価性を満たすことの証明の実現に向けた検討：

① ProVerif を用いた暗号プロトコルの安全性評価として、Bluetooth のセキュアシンプルペアリングの形式的検証を行った。Yeh らは Bluetooth のセキュアシンプルペアリングで用いられるプロトコルの 1 つである Numeric Comparison プロトコルに対して脆弱性を指摘し、その改良方式を提案している。本研究では Yeh らの提案方式に対する形式的検証を行った。結果として、Yeh らの提案方式に対する攻撃方法、すなわち、なりすましに対する脆弱性を発見することに成功した。さらに、本研究ではその脆弱性に対する対策方法を提案することに成功した。

本成果により計算機を用いた暗号プロトコルの安全性評価において証明の誤りをなくすといった可能性を示すことができた。

② ProVerif を用いた暗号プロトコルの安全性評価として、ワンタイムパスワード（OTP）認証方式の形式的検証を行った。OTP 認証方式に対する攻撃方法として、サーバに保存されている情報を利用しなりすましを行う攻撃（Hybrid Theft Attack）、通信データを改ざんしサーバとユーザ間の認証を不可能にする攻撃（DoS Attack）、上記２つを組み合わせた攻撃（Theft DoS Attack）が挙げられる。Isawa らは上記の攻撃全てに耐性のある OTP 認証方式を提案している。本研究では Isawa らの提案した OTP 認証方式に対する形式的検証を行った。結果として、サーバに保存されている情報を利用しなりすましを行う攻撃（Hybrid Theft Attack）及びサーバに保存されている情報を利用し、サーバとユーザ間の認証を不可能にする攻撃（Theft DoS Attack）に対する脆弱性を発見することに成功した。

これまで、ProVerif を用いた OTP 認証方式の安全性評価は、その形式化記述が困難であったため行われてこなかった。その問題に対して、研究代表者は OTP 認証方式における ProVerif 上での形式化記述手法を提案した。その手法を用いて、Isawa らの提案した OTP 認証方式を形式化記述し、その安全性評価を行った結果、脆弱性を発見することに成功した。本成果により計算機を用いた安全性評価のさらなる厳密化の可能性を示すことができた。

③ インターネット技術の標準化推進団体 IETF において標準化の議論が進められている TLS 1.3（Transport Layer Security TLS Protocol Version 1.3）のハンドシェイクプロトコルに対して ProVerif を用いて形式的に記述し、その安全性評価を行った。具体的には、TLS 1.3 のドラフト-06 以降（draft-18 まで）の仕様を継続的に形式化記述し、その安全性評価を行った。結果として、TLS 1.3 フルハンドシェイクプロトコルに対する安全性（Secrecy（秘匿性）、Authentication（認証）、さらには Forward Secrecy（前方秘匿性））を示すことに成功し、その結果を TLS 1.3 の標準化に反映させることに成功した。また、本成果は国際的な協力体制で暗号プロトコルの安全性評価に取り組んでいる暗号プロトコル評価技術コンソーシアム（CELLOS）の活動にも貢献した。

④ ProVerif は（暗号プロトコルの構成部品である）暗号プリミティブの形式化記述の正しさを検証する仕組みがないため、その検証は困難である。よって、ProVerif における暗号プリミティブの形式化記述に関する研究を行った。結果として、暗号プリミティブを暗号プロトコルの一種として形式化記述することで、形式化記述の正当性を検証する手法を提案することに成功した。これにより、ProVerif における暗号プリミティブの表現能力を向上させることに成功した。さらに、上記手法を拡張し、公開鍵暗号方式に求められる安全性の概念である CCA（CCA1、CCA2）安全性の形式化記述及びその検証に成功した。これにより、ProVerif における暗号プリミティブの形式化記述能力をさらに向上させ、安全性評価の信頼性を高めることに成功した。

本成果の暗号プリミティブを暗号プロトコルの一種として形式化記述することで形式化記述の正当性を検証する手法は、CryptoVerif において自動証明できない観測等価性を満たすことの記述及びその証明において、観測等価性を満たすことの記述に対してその記述の正しさを検証する手法として用いることができる。具体的には、安全性の根拠となる暗号プリミティブの安全性において観測等価性を満たす２つのプロセスとして記述する際に、本手法を用いることで２つのプロセスの記述が観測等価であるかの検証を行うことができる。

以上より、本成果により CryptoVerif において自動証明できない観測等価性を満たすことの記述についてその記述の正しさを検証することは、ProVerif 援用することにより実現できたが、観測等価性を満たすことの証明を実現するには至らなかった。しかしながら、計算機を用いた暗号プロトコルの安全性証明を厳密にできる手法の実現に向けて、ある程度の方向性を示すことには成功したと考えられる。今後は、ProVerif と Mizar を併用する方向で観測等価性を満たすことの証明の実現を目指す。

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１件）


① Kenichi Arai, Ken Wakabayashi, Hiroyuki Okazaki, Difference of Function on Vector Space over F, Formalized Mathematics, 査読有, Vol. 22, No. 3, Pages 269-275, 2014. DOI: 10.2478/forma-2014-0027


〔学会発表〕（計９件）


① 荒井研一、岡崎裕之、布田裕一、ProVerif における phase について、2017 年 暗号と情報セキュリティシンポジウム（SCIS2017）、2A1-1、2017 年 1 月 24 日～27 日、ロワジールホテル那覇（沖縄県那覇市）.

② 荒井研一、岡崎裕之、ProVerif での形式化における技術的な注意点について、日本応用数理学会 2016 年度 年会 予稿集、2D-2、2016 年 9 月 12 日～14 日、北九州国際会議場（福岡県北九州市）.

③ 荒井研一、徳重佑樹、櫻田英樹、ProVerif による TLS1.3 ハンドシェイクプロトコルの形式検証（その 2）、2016 年 暗号と情報セキュリティシンポジウム（SCIS2016）、1A1-4、2016 年 1 月 19 日～22 日、ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市）.

④ 岡崎裕之、荒井研一、Proverif を用いた暗号プリミティブの形式化、2016 年 暗号と情報セキュリティシンポジウム（SCIS2016）、1A1-1、2016 年 1 月 19 日～22 日、ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市）.

⑤ 荒井研一、ProVerif による TLS1.3 ハンドシェイクプロトコルの形式検証、Small-workshop on Communications between Academia and Industry for Security 2016 (SCAIS2016)、2016 年 1 月 18 日、熊本市国際交流会館（熊本県熊本市）.

⑥ 荒井研一、暗号プロトコル評価ツール ProVerif による TLS1.3 ハンドシェイクプロトコルの形式検証、”暗号プロトコル技術評価コンソーシアム（CELLOS）シンポジウム 2015、2015 年 12 月 17 日、株式会社インターネットイニシアティブ（東京都千代田区）.

⑦ 荒井研一、渡辺大、櫻田英樹、ProVerif による TLS1.3 ハンドシェイクプロトコルの形式検証、コンピュータセキュリティシンポジウム 2015（CSS2015）論文集、2015(3)、pp.1003-1010、2015 年 10 月 21 日～23 日、長崎ブリックホール（長

崎県長崎市).

⑧ 岩本智裕、荒井研一、金子敏信、ProVerif による Theft DoS Attack に耐性のあるワンタイムパスワード認証方式の形式的検証、2015 年暗号と情報セキュリティシンポジウム(SCIS2015)、4F2-3、2015 年 1 月 20 日～23 日、リーガロイヤルホテル小倉（福岡県北九州市).

⑨ Kenichi Arai, Toshinobu Kaneko, Formal Verification of Improved Numeric Comparison Protocol for Secure Simple Paring in Bluetooth Using ProVerif, Proceedings of the 2014 International Conference on Security and Management (SAM'14), pp.255-261, July 21-24, 2014, Monte Carlo hotel (Las Vegas, Nevada, USA).（査読有）

## ６．研究組織

(1)研究代表者

荒井　研一（ARAI, Kenichi）
長崎大学・工学研究科・助教
研究者番号：60645290

(2)研究分担者　　なし

(3)連携研究者　　なし