様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

2012 年３月３１日現在

機関番号：82636
研究種目：若手研究(B)
研究期間：2010 年度～2011 年度
課題番号：22760287
研究課題名（和文）　ユーザビリティを有する暗号プロトコルと安全性モデルに関する研究

研究課題名（英文）　A Research on Usable Cryptographic Protocol and its security model

研究代表者　松尾　真一郎（MATSUO SHINICHIRO）
（独）情報通信研究機機構・ネットワークセキュリティ研究所セキュリティアーキテクチャ研究室・室長
研究者番号：20553960

研究成果の概要（和文）：省リソースデバイスのような、計算機能力とユーザーインターフェースが制約を受けている中でも、ユーザインターフェースの特徴を行かして、認証と通信路の暗号化が可能な暗号プロトコルを開発した。また、上記のようなデバイスの特徴を踏まえた、安全性評価のモデルを確立し、このモデルに従って開発した認証付きが機構間プロトコルの安全性評価を行った。さらに、上記のようなデバイスにおいて基礎的なプロトコルを実装し、そのフィージビリティの確認を行った。

研究成果の概要（英文）：In this research, we build authenticated key agreement protocol which is used to establish secure channel on resource constrained devices. This protocol can be performed on the devices which have small computational capabilities and tiny user interfaces. We also establish a security evaluation model for these devices including the specifications of these devices. Then we prove the security of the proposed authenticated key agreement protocol in the model. We also implement basic protocol on the iOS tablet and confirm feasibility of the proposed protocol.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	700,000	210,000	910,000
2011 年度	900,000	270,000	1,170,000
年度			
年度			
年度			
総　計	1,600,000	480,000	2,080,000

研究分野：工学
科研費の分科・細目：電気電子工学、通信・ネットワーク工学
キーワード：暗号プロトコル、安全性モデル

１．研究開始当初の背景

公開鍵暗号の発明以降、インターネット上で安全な通信路を確立する技術の研究が盛んに行われ、その多くはPKI（Public Key Infrastructure）のような形で広く利用されるようになっている。従来の同様の研究は、一般的なサーバとPC、そしてインターネットを利用することを前提に実施されている。これらの研究では、プロトコルの処理性能を確保することと同時に、安全性の数理的証明を付

けることが求められている。その際、プロトコルに対する攻撃者のモデル化を行い、その攻撃者が攻撃に成功する確率を、素因数分解問題や離散対数問題のような数学的に困難な問題に安全性を帰着させる方法が一般的である。例えば、安全な通信路を確保するにあたり最も重要になる鍵交換技術においては、論文（M. Bellare, D. Pointcheval and P. Rogaway, “Authenticated Key Exchange Against Dictionary Attack,” Eurocrypt 2000）などで一般的な攻撃者と安全性のモデルが示されている。

一方で、現在携帯電話をはじめとして、携帯情報端末が広く普及しており、このような環境においても、一般的な状況設定と同様の安全性を確保する技術を確立することが求められる。このような状況下において、特に留意が必要な点として、携帯情報端末のユーザーインターフェースと処理性能がPCに比べて制限されるため、一般的に利用されるセキュリティプロトコルが利用されないということが挙げられる。例えば、公開鍵暗号を利用する際に必要なPKIでは公開鍵証明書の有効性を検証するために、公開鍵証明書に関する数多くの管理情報を各端末が管理する必要があるが、これは実際には現実的ではない。そのため、これらの端末に対して特化したプロトコルを新たに設計する必要がある。

このような条件における暗号プロトコルの研究は盛んに行われているものの、安全性のモデルや安全性証明については、合意がとれる知見が得られていない。また、近年、セキュリティ技術のユーザビリティに関する研究が注目を浴びており、SOUPS、USECなどの国際会議が新たに開かれるようになっている。これらのユーザビリティに関する研究成果を取り込むことは、現実的に利用される暗号プロトコルをターゲットにするために必要不可欠である。

２．研究の目的

本研究では、上記のような、ユーザーインターフェースをはじめとして、端末に制約がある状況の中で、安全な認証付き鍵交換を行うための暗号プロトコルの安全性モデルを確立するとともに、この安全性モデルにおいて安全な暗号プロトコルを設計し、その安全性を数理的に証明することである。特に新たに研究が必要な点は以下の 3 点である。

- 現在の一般的な暗号プロトコルの安全性定義では、性能やユーザインターフェースが限られた状況でのプロトコルの設計が困難であり、本研究により当該環境における現実的な定義を与える。
- 安全性モデル、および設計方式の評価にユーザビリティに関する知見を導入することにより、より効果の高い安全性モデルの実現を図る。
- 安全性の検証において、形式化手法などの数理的技法を利用し、プロトコル設計者に対しても利便性の高い環境の提供を図る。

さらに、単に安全性のモデルを構築するだけでは、現実のコンピューティング環境において実用性のない技術となってしまう。特に、本研究の対象となる省リソースデバイスにおいては、その制約においても十分実用的な性能を達成しなければいけない。そのため、本研究では、提案する暗号プロトコルを実際のデバイスにおいて実装し、そのプロトタイプ実装を元に、端末に制約がある状況での暗号プロトコルのフィージビリティの評価を行うこととする。

３．研究の方法

2010 年度に、安全性モデルの検討、および携帯機器環境における基本となる鍵交換プロトコルの評価を行った。安全性モデルの検討においては、暗号プロトコルの安全性モデルの世界的第一人者である、Columbia 大学 Moti Yung 教授との議論を通じて、国際的な視点での知見を多く取り組んで実施した。また、iOS 端末（iPod touch、および iPad）の実機を使い、パスワードベース認証付き鍵交換（Password based Authenticated Key Exchange: PAKE）プロトコルを実装するとともに、その性能測定を行い、これらの省リソースデバイスにおけるべき乗剰余演算、および共通鍵暗号系の演算の処理速度から、省リソースデバイスにおける暗号プロトコル設計の方針を得ることとした。

また、2011 年度においては、2010 年度に検討した安全性モデルにおいて、携帯機器環境における制約とインターフェースを活かし認証付き鍵共有プロトコルを設計し、その安全性を数理的に証明した。このプロトコルにおいては、2010 年度のフィージビリティ評価の知見から、公開鍵系のべき乗剰余演算を使わない構成とすることとし、共通鍵系の演算だけで構成可能なプロトコル設計とすることを目指した。また、スマートフォンや外部メディアの I/F の特徴と耐タンパ性に関する分析を行い、この分析を元に、異なるユーザインターフェースの特徴を活かすプロトコル設計とすることにした。

この際、文献調査や、引き続き Columbia 大学 Moti Yung 教授との意見交換を通じ、セキュリティの技術のユーザビリティに関する最新動向を調査するとともに、ユーザビリティの評価に関する新たな知見を確立することとした。

４．研究成果

2010年度は、(1)携帯機器環境の制約の分析と、(2)数理的安全性モデルの確立の2つのステップの研究を実施した。

(1)については、普及している携帯機器用OSであるiOSとAndroidを対象に、それぞれのセキュリティ機能、セキュリティ機能を実現する機構、基盤となる暗号演算の制約について調査を行った。特に暗号演算については、AESなどの一般的な処理の一部はAPIが用意されているが、基礎的な数学的な演算については用意されていないことがわかった。そのため、一般的な暗号ライブラリであるOpenSSLをiOSに移植するとともに、PAKEプロトコルを実装し、性能面では問題があることを示した。

上記の制約を把握した上で、OS に用意された暗号演算を用いながら、安全な通信路を確立するためのモデルとして、利用者は簡単に記憶できる秘密情報を用いながら、耐タンパデバイスを外部装置として使うことにより、PAKE と同様の安全な通信路を構築する方法と、その方法のための安全性モデル、安全性の定義を構築した。この構築にあたっては、同分野の世界的権威である Moti Yung 教授との議論を実施した。このモデルにおいては、耐タンパ装置にも秘密情報が含まれるため、鍵交換ではなくセッションごとの鍵更新のような構造になるが、一方でパスワードをプロトコルに含めることにより、エンティティ認証の要素を持たせることが可能となる。携帯機器の特性と、ユーザビリティを加えた現実的なモデルの提案はこれまでに提案されておらず、世界的に見ても新しい提案となる。このモデルについて、電子情報通信学会・情報通信システムセキュリティ研究会において発表を行った。

2011年度は(3)ユーザビリティに関する知見の集約とモデルへの反映、(4)プロトコルの

設計、(5)提案プロトコルの安全性評価の3つのステップの研究を実施した。
(3)については、現在普及しつつあるスマートフォンや携帯機器のハードウエア・ソフトウエアの仕様を調査するとともに、プログラムから利用可能なインターフェース、人間が利用可能なインターフェースについて調査と検討を行い、認証付き鍵交換を実現するプロトコルを実装するにあたり、SDカードのインターフェースで実装された耐タンパデバイスと、通常のスマートフォンOSとアプリケーション、そしてパスワードなどを入力するインターフェースからなる機構を、携帯機器におけるシステムモデルとして、上記の機構における情報漏洩が発生する可能性がある箇所をセキュリティモデルとして定めた。その上で(4)として、情報漏洩に耐性のある疑似ランダム関数、メッセージ認証コードとチャレンジ&レスポンスプロトコルを組み合わせることで、単一の情報漏洩では将来の認証の安全性が脅かされない、パスワードを含む多要素認証付き鍵交換プロトコルが実現できることを示した。(5)としてこの分野の世界的権威であるMoti Yung教授との議論を行い安全性の証明を与えることができた。このプロトコルについては、世界的にもまだ例が無く新しい提案となる。このプロトコルについて、査読付き国際会議であるINTRUST2011と、暗号と情報セキュリティシンポジウム2012で発表を行った。

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）

〔学会発表〕（計３件）

1. 松尾真一郎, 森山大輔, Moti Yung, “多要素認証付き鍵更新,” 暗号と情報セキュリティシンポジウム 2012, 2012 年 1 月 30 日, 金沢エクセルホテル東急, 石川.

2. Shin’ichiro Matsuo, Daisuke Moriyama and Moti Yung, “Multifactor Authenticated Key Renewal,” In Proc. of INTRUST2012, International Exchange Center of Beijing Institute of Technology, China, Nov. 29, 2011.

3. 松尾真一郎, Moti Yung, “モバイル機器に適した暗号プロトコルのための安全性モデル,” 電子情報通信学会情報通信システムセキュリティ研究会、2011 年 3 月 25 日, 機械振興会館, 東京（東日本大震災のため口頭発表は中止）.

６．研究組織
(1)研究代表者
松尾真一郎（MATSUO SHINICHIRO）
（独）情報通信研究機構・ネットワークセキュリティ研究所セキュリティアーキテクチャ研究室・室長
研究者番号：20553960

(2)研究分担者
（　　）
研究者番号：

(3)連携研究者
（　　）
研究者番号：