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

平成２４年　５月　８日現在

機関番号：14401
研究種目：若手研究（B）
研究期間：2009 年度～2011 年度
課題番号：21700015
研究課題名（和文）　暗号プロトコルに対する計算論的に健全な安全性検証技術と再設計支援技術の開発
研究課題名（英文）　Computationally sound symbolic analysis of security and assistance of redesign for cryptographic protocols
研究代表者
吉田　真紀（YOSHIDA MAKI）
大阪大学・大学院情報科学研究科・助教
研究者番号：50335387

研究成果の概要（和文）：本研究の目的は，暗号プロトコルに対して，現状において最も望ましい強さの安全性である汎用的結合可能安全性をもつことを検証するための基盤技術と，それに基づく再設計の支援も含めた検証技術を開発することである．

研究成果の概要（英文）：The purpose of this work is to develop a method to analysis universally composable security of cryptographic protocols and assist redesign insecure protocols.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,200,000	360,000	1,560,000
2010 年度	1,100,000	330,000	1,430,000
2011 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
キーワード：暗号プロトコル，安全性，汎用的結合可能性，形式的検証，計算量的に健全

１．研究開始当初の背景

情報通信システムにおいてセキュリティの実現が必須となり，秘匿や認証などの様々な機能を同時に実現する暗号プロトコルが数多く提案されている．それらの暗号プロトコルは複数の暗号技術を組み合わせて利用しており，構成がより複雑になっている．そのため，人間が安全性を証明すると多大な労力がかかるだけでなく，誤りが含まれやすい．また，安全性が望ましい強さでなければ，単体で安全であったとしても，他のプロトコルとの結合や，多重実行により互いに干渉し安全性が損なわれる場合がある．

近年，このような問題に対して，従来の暗号の安全性証明の集大成する「計算論的モデル」として，2001 年に汎用的結合可能(Universally Composable(UC)) 安全性のモデルが Canetti によって提案され，その形式的検証法として 2004 年に「記号論的モデル」に基づく検証法が Canett-Herzog によって提案された．その後，検証対象の拡張や実プロトコルの検証を目指し，多数の研究機関で精力的に研究が行われている．ただし，その検証基盤は本来，基本的な暗号技術ごとに個別に開発されたものか，暗号プロトコルの検証以外に開発されたものであり，以下の二つの深刻な問題を引き起こしている．

(A) 検証対象の拡張が容易でない：利用する暗号技術や実現する機能を増やすたびに，基盤となる記号論的モデルと検証法を拡張する必要がある．その際，記号論的モデルの記述能力と検証法の検証能力の両方を上げる必要があり，一般に拡張は自明ではない．

(B) 検証対象の記述が容易でない：検証対象によっては記号論的モデルで記述する際に，プロトコルの操作として計算論的モデルで明示的に記述されていない操作も記述する必要がある．これは，両モデルの差や，検証法の検証能力の限界から生じる問題であり，一般に記述は自明ではない．

すなわち，新たな暗号プロトコルを開発した場合に，迅速かつ効果的に検証することが非常に困難となっている．

２．研究の目的

本研究では，UC 安全性あるいはそれ以上の強さをもつ計算論的安全性を検証するため，多様な機能に柔軟に対応可能かつ計算論的モデルと違和感なく利用可能な検証基盤の創出を目的とする．

３．研究の方法

研究目的を達成するために，以下の(1)～(3)を遂行した．

(1)新たな記号論的モデルの定義：まず，UC 安全性の基本モデルとその拡張モデルを検討し，多様な機能を実現可能かつ実用的な計算論的モデルを選択する．次に，選択した計算論的モデルの下での定式化において統一的な特徴を調べる．そして，その特徴を活かし，記述対象についての多様性を有する記号論的モデルを定義する．さらに，定義した記号論的モデルの下で，記号論的安全性を定式化する．

(2)計算論的に健全な記号論的検証法の開発：記号論的安全性は計算論的安全性よりも抽象化された形となるが，一般にその安全性を判定する問題は決定不能であることが知られている．よって，決定可能となるための十分条件を導出し，その条件の下での安全性判定法（すなわち安全性検証法）を設計する．記号論的モデルは計算論的モデルよりも抽象度が高いため，一般に記号論的安全性は計算論的安全性と等価ではない．すなわち，検証法が記号論的に安全と出力しても，計算論的に安全とは限らない．よって，設計した記号論的安全性の検証法が計算論的安全性を保証すること（計算論的健全性）を証明する．

(3)再設計支援のための攻撃導出法の開発：検証によって安全でないことがわかった場合に攻撃法を導出できれば，安全でないことの証拠となるだけでなく，その攻撃法が無効になるように修正でき，暗号プロトコルの再設計に貢献すると期待できる．よって，効果的な再設計を可能とする攻撃法を検討し，複数の方針と各方針に従った攻撃導出法を設計する．

４．研究成果

本研究の主要な成果を示す．

(1)新たな記号論的モデルの定義：まず UC 安全性のモデルとその拡張，等価な安全性の計算論的モデルを調査し，より多様な機能を実現可能で，多くの暗号プロトコルの機能の安全性の定式化に利用されているモデルを選択した．具体的には，UC 安全性のモデルのうち，多くの暗号プロトコルの機能の定式化に利用されている最初に提案された UC モデルを対象とした．そして，暗号技術と暗号プロトコルが目標とする理想的な機能（理想機能）の具体的な定式化を調査した．調査によって，理想機能と参加者間の通信の一連の流れを分割することで，いくつかの共通の特徴（通信パターンと呼ぶ）が見出された．よって，通信パターンに基づき，機能を分類し，それぞれに対する記号論的モデルを定義した．さらに，UC 安全性の拡張の中で，最も現実的なモデルである GUC モデルも対象とした．ただし，GUC 安全性をそのまま扱う場合はモデルが非常に複雑となるため，等価な単純化である EUC 安全性に対して，記号論的モデルを定義した．

UC モデルおよび GUC/EUC モデルから記号論的モデルを定義する際，暗号設計者が違和感なく利用可能とするために，元の計算論的モデルにおける記述ポリシーを可能な限り反映した（明確に記述が分けられる概念は，記号論的モデルにおいても対応する形で分けられるように定義するなど）．これにより，UC モデルと GUC/EUC モデルにおける既存の各種概念を記号論的に対応する形で定義できた．これによって，暗号プロプロトコルと UC/GUC 安全性の記号論的定義を結びつけることができたこととなる．

さらに，定義した記号論的モデルにおいて，UC 安全性と GUC/EUC 安全性を定義した．

(2)計算論的に健全な記号論的検証法の開発：まず UC 安全性を対象に，安全性を判定する問題が決定可能となる十分条件を導出し，その十分条件の下での検証法を設計し，計算論的健全性を証明した．計算論的健全性の証明では，検証対象の暗号プロトコルに対して，計算論的モデルで現実的に起こりうる実行状況（高い確率，実行可能な時間内）が，記号論的モデルでも起きること（一対一に対応すること）を証明する．一般に，十分条件が緩い場合は抽象度の低い計算論的モデルでは様々な実行状況が起こり，記号論的モデルとの差が大きくなる．そこで，まず比較的

自明な強い十分条件を見出し，検証法を設計することから始めて，より実用的な十分条件の下での検証法となるように改善していった．対象とするプロトコルは，インターネット上での安全な通信に必要不可欠な鍵交換プロトコルと認証プロトコルとした．

そして，UC 安全性検証法を EUC 安全性向けに拡張した．EUC 安全性では，攻撃者の能力がより高くなるため，検証法の拡張ではそれを反映するようにした．安全性判定問題が決定可能となるための十分条件の導出と検証法の設計のため，最初は，送受信者間での通信が 1 回の one-message プロトコルを対象とした．その上で，2 回以上の multi-message プロトコルを対象とした決定可能となるための十分条件を導出し，検証法を設計した．

(3)再設計支援のための攻撃導出法の開発：暗号プロトコルの計算量的安全性の根拠として，様々な数学問題の困難性が仮定されている．安全性を保証するためには，基となる数学的構造を理想化した Generic model (GM) において困難性仮定に対する攻撃の有無を判定する必要がある．そこで，GM における攻撃の有無判定・導出法を設計した．また暗号プロトコルそのものに対する攻撃の導出も検討した．安全でない場合は，まず攻撃の容易さ，あるいは困難さを把握することが重要である．最も実行しやすい攻撃の困難さを把握することができれば，その暗号プロトコルへの攻撃が現実的に可能か否かの判断の目安となる．よって第一の方針として，攻撃者にとって最も実行しやすい攻撃の一つとその困難さを求めるという方針を検討した．また，安全でない暗号プロトコルを再設計する場合，無効化すべき攻撃の見落としを減らすことが重要である．無効化対策が互いに異なる可能性がある攻撃を多く導出することができれば，まとめて無効化する修正を考えることができ，少ない修正で安全なプロトコルを得ることができる．よって第二の方針として，無効化対策が互いに異なる可能性のある攻撃を可能な限り求めるという方針を検討した．具体的には，第一の方針のために，攻撃の困難さの尺度として妥当な定義を検討し，その定義の下で攻撃導出法を設計する．さらに第二の方針のために，無効化対策が互いに異なる可能性がある攻撃法とはどのような攻撃法かを検討し，その極大集合を求める攻撃導出法を設計した．

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）

〔雑誌論文〕（計 10 件）

① Maki Yoshida and Toru Fujiwara, ``Toward Digital Watermarking for Cryptographic Data,'' IEICE Transactions on Fundamentals, Vol.E94-A, No.1, pp.270-272 (2011-01), 査読あり.

② 山中 広明, 岡村 真吾, 藤原 融, 吉田 真紀, 石原 靖哲, 秋山 豊和, 加藤 精一, 下條 真司, ``評価者間類似度計算の改善による汚染コンテンツダウンロード抑制効果向上,'' 情報処理学会論文誌, Vol.51 No.8, pp.1428--1442 (2010-08), 査読あり.

③ Maki Yoshida and Toru Fujiwara, ``All-or-nothing Property for Efficient Symbolic Analysis,'' Computational and Symbolic Proofs of Security (2010-04), 査読あり.

④ Maki Yoshida and Toru Fujiwara, ``Expiration Dated Fingerprinting,'' IJICIC, Vol.6, No.3, pp.1271--1278 (2010-03), 査読あり.

⑤ 鈴木 斎輝, 吉田 真紀, 藤原 融, ``公理的安全性の枠組みにおける汎用的結合可能な相互認証と鍵交換の記号的安全性,'' 日本応用数理学会論文誌, 第 20 巻, 第 1 号, pp.11-32 (2010-03), 査読あり.

⑥ Maki Yoshida, Shigeo Mitsunari, and Toru Fujiwara, ``The Vector Decomposition Problem,'' IEICE Transactions on Fundamentals, Vol.E93-A, No.1, pp.188--193 (2010-01), 査読あり. Best paper award.

⑦ Maki Yoshida and Toru Fujiwara, ``Watermarking Cryptographic Data,'' the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2009), A02-02 (CD-ROM) (2009-09), 査読あり.

⑧ Kazuya Ohkita, Maki Yoshida, Itaru Kitamura, and Toru Fujiwara, ``Improving Capability of Locating Tampered Pixels of Statistical Fragile Watermarking,'' the 8th International Workshop on Digital Watermarking (IWDW 2009), LNCS 5703, pp.279-293 (2009-08), 査読あり.

⑨ Itsuki Suzuki, Yoshiki Kamano, Maki Yoshida, and Toru Fujiwara, ``Development of a Verification Tool for Composable Security,'' Computational and Symbolic Proofs of Security (2009-04), 査読あり.

⑩ Maki Yoshida and Toru Fujiwara, ``Flexible Timed-release Encryption,'' IEICE Transactions on Fundamentals, Vol.E92-A, No.1, pp.222--225 (2009-01), 査読あり.

〔学会発表〕(計 11 件)

① Itsuki Suzuki, Maki Yoshida, Toru Fujiwara, “Generic Construction of GUC Secure Commitment Protocol in the PKI Model,” Proceedings of the 2012 Symposium on Cryptography and Information Security, 1D2-5E (2012-01).

② 池田成吾, 吉田真紀, 藤原融, “画質劣化を抑えた加法と乗法のハイブリッド電子透かし,” 2012 年暗号と情報セキュリティシンポジウム予稿集, 3E2-3 (2012-02).

③ 鈴木斎輝, 吉田真紀, 藤原融, “EUC 安全なメッセージ認証のための multi-message プロトコルに対する記号的基準,” IEICE Tech. Rep., vol.111, no.285, ISEC2011-57, pp.155-162, Nov. 2011 (2011-11).

④ Maki Yoshida, Kazuya Ohkita, Toru Fujiwara, “Recovery of Tampered Pixels for Statistical Fragile Watermarking,” IEICE Tech. Rep., vol.111, no.126, EMM2011-9, pp.7-12, June 2011 (2011-07).

⑤ Maki Yoshida, Toru Fujiwara, “On the Impossibility of d-Multiplicative Non-perfect Secret Sharing,” IEICE Tech. Rep., Vol.111, No.34, ISEC2011-5, pp. 31-36, May 2011 (2011-05).

⑥ Itsuki Suzuki, Maki Yoshida, Toru Fujiwara, “ Computationally Sound Symbolic Analysis for EUC Security of Key Exchange,” 日本応用数理学会 2010 年度年会, pp.63-64, 2010 (2010-09).

⑦ 雲嶋健太, 吉田真紀, 阿部正幸, 大久保美也子, 藤原融, “Generic Model における困難性仮定への攻撃の数式処理を用いた導出,” 電子情報通信学会技術研究報告 (ISEC2010-58), Vol.110, No.281, pp.57-64 (2010-11).

⑧ 岡前直由, 吉田真紀, 雲嶋健太, 阿部正幸, 大久保美也子, 藤原 融, “Bilinear Group に関する困難性仮定への攻撃導出 - Cryptology ePrint Archive 上の仮定に攻撃は存在するか？ -,” 2011 年暗号と情報セキュリティシンポジウム予稿集, 4F1-1 (2011-01).

⑨鈴木斎輝, 吉田真紀, 藤原融, “Static Adversary に対して EUC 安全な認証の記号的基準について,” 電子情報通信学会技術研究報告, Vol.110, No.443, ISEC2010-133, pp.403-410 (2011-3).

⑩鈴木斎輝, 吉田真紀, 藤原融, “汎用的結合可能な相互認証に対する記号的識別不可能性を用いた記号的基準,” 2010 年暗号と情報セキュリティシンポジウム予稿集 (SCIS2010), 2C4-1, CD-ROM (2010-01).

⑪鈴木斎輝, 吉田真紀, 藤原融, “汎用的結合可能な安全性の形式的検証のための pattern 拡張に関する一考察,” 日本応用数理学会 2009 年度年会, 数理的技法による情報セキュリティ(FAIS), (2009-09).

６．研究組織

(1)研究代表者

吉田　真紀 (YOSHIDA MAKI)

大阪大学・大学院情報科学研究科・助教

研究者番号：50335387

(2)研究分担者

なし

(3)連携研究者

なし