様式 C-19

科学研究費補助金研究成果報告書

平成 22 年　5 月３０日現在

研究種目：基盤研究（C）
研究期間：2007～2009
課題番号：１９５００００９
研究課題名（和文）　暗号プリミティブの安全性検証の自動化への展開
研究課題名（英文）　Development on automations of security analysis for cryptographic primitives

研究代表者
太田　和夫（OHTA KAZUO）
電気通信大学・電気通信学部・教授
研究者番号：８０３３３４９１

研究成果の概要（和文）：暗号プロトコルの安全性自動検証手法 APSG，および T-PIOA の改良と事例研究の拡張を行い，各手法の性能を評価するとともに実用性を向上させた．また，低資源向き認証プロトコル GPS 方式と HB-PUF 方式の安全性解析を行い，既存方式の問題点を指摘するとともに，改良方式を提案した．

研究成果の概要（英文）：We improve utilities of frameworks for automated security analysis of cryptographic protocols (APSG and T-PIOA) by improving models, and introduce examples of analysis to evaluate performance of each framework. Also, we point out vulnerability of authentication protocols for low resource devices (GPS and HB-PUF) and introduce improved protocols.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,000,000 円	300,000 円	1,300,000 円
２００８年度	1,100,000 円	330,000 円	1,430,000 円
２００９年度	1,300,000 円	390,000 円	1,690,000 円
年度			
年度			
総　計	3,400,000 円	1,020,000 円	4,420,000 円

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：暗号系，フォーマルメソッド，安全性検証，低資源向き認証

１．研究開始当初の背景

(1) 複数の個別プリミティブを組み合わせた複合プロトコルや格子理論などの数学的構造を仮定した新たなプリミティブの発展に伴い，安全性証明を人手で行うのが困難になってきている．

(2) プリミティブによっては，計算能力が低い，メモリサイズが小さい，通信能力が限定されたような低資源な実装環境でも，状況に応じた安全性を保証できることが期待されている．暗号技術が広範に利用されるに従って低資源向きプロトコルのニーズは大きくなっている．

２．研究の目的

(1) 複合プロトコルや難解な数学的構造を仮定した安全性証明を自動で行うため，各種安全性自動検証手法の性能評価と改良を

行う.
(2) ニーズが大きい本人確認方式や認証つき鍵交換方式 (AKE) を対象とし，安全性の根拠とする数論問題レベルから見直すことで，実用的な低資源向きのプロトコルを提案する.

３．研究の方法
(1) いくつかの多面的な手段を用いて，自動検証手法 UCSA, APSG, T-PIOA の比較を行う．まず，共通したプリミティブへの適用範囲や攻撃モデルの記述能力の違いについて比較する．次に，両手法がどのように様々な攻撃法をモデルに取り込んでいるかを考察する．最後に，上記の比較で明らかになった問題点を解決し手法を拡張する.
(2) GPS 法の厳密な評価を行い，安全性に問題が見つかった場合には安全性を保証可能な改良方式を検討する．また，HB 方式の理論的な解析を行い，安全性の根拠となる問題の妥当性の評価を行い，中間者攻撃に対して安全な改良方式を検討する.

４．研究成果
(1-1) T-PIOA の解析能力を評価し，UCSA や APSG と比較することが可能となった．以下，比較を行った結果を示す．1. UCSA と T-PIOA はどちらも鍵交換プロトコルの解析能力を持っているが，T-PIOA の方がより高度な攻撃モデルで証明可能．2. APSG と T-PIOA はどちらも電子署名プロトコルの解析能力を持ち，かつ，もっとも高いレベルの安全性を証明可能．このように，3 つのアプローチの適用領域の解明に繋がる成果が得られた.

(1-2) 暗号プロトコルの安全性自動検証手法 APSG に基づく自動検証ツール CryptoVerif の問題点の指摘と改良を行った．鍵交換と GDH 署名の検証時に誤った検証結果を出力する場合が存在することを指摘し，ソースコードを変更することで問題点を解決した.

(1-3) CryptoVerif の証明能力を検証するために，ランダムオラクルからの情報漏洩をモデル化して，代表的な暗号プロトコル (FDH 署名，Bellare-Rogaway の公開鍵暗号方式，RSA-KEM 鍵配送方式) の安全性証明を試みた．本実験により，既存の項書換え規則の拡充が必要な箇所，検証系の機能拡張が必要な箇所等，新たな知見が得られた.

(2-1) GPS 方式の厳密な解析と拡張方式の提案をそれぞれ行い，従来の低資源向け認証プロトコルの (非) 実用性を明らかにし，また，実用的には問題無いレベルの安全性を持った効率的なプロトコルが得られた.

(2-2) 秘密情報の秘匿性を高めることにより，必要メモリ量を減らしたままで認証成功確率が 1 となる新たな改良方式 GPS++を提案した．これにより，RFID タグなどのより低資源なデバイス向けの認証方式を実現することに成功した.

(2-3) HB 方式と物理的複製困難関数を組み合わせた認証方式 (HB-PUF 法) の安全性を解析した．計算量を削減した HB 系の殆どの方式において具体的な攻撃手順を指摘した．計算量の僅かな増加を許容し，僅かなタンパなメモリ領域を用いることで，証明可能安全なアルゴリズム的耐タンパ認証装置を実現可能なことを示した.

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５件）

① Kazuki Yoneyama, Efficient and Strongly Secure Password-based Server Aided Key Exchange, Journal of Information Processing, 査読有り, vol.17,2009, pp.1046-1059

② Kazuki Yoneyama, Satoshi Miyagawa, Kazuo Ohta, Leaky Random Oracle, IEICE Trans. on Fundamentals, 査読有り, vol.E92.A(8), 2009, pp.1795-1807

③ Bagus Santoso, Kazuo Ohta, A New 'On the Fly' Identification Scheme: A Trade-off of Asymptoticity between ZK and Correctness, IEICE Trans. on Fundamentals, 査読有り, Vol. E92-A, No.1, 2009, pp.122-136

④ Kazuki Yoneyama, Does Secure Password-based Authenticated Key Exchange against Leakage of Internal States Exist?, IEICE Trans. on Fundamentals, 査読有り, Vol.E92.A, No.1, 2009, pp.113-121

⑤ 米山 一樹，太田 和夫，Task-Structured PIOA フレームワークを用いた適応的攻撃者に対する Diffie-Hellman 鍵交換の安全性解析，電子情報通信学会論文誌 D 分冊，査読有り，vol.J91-D, No.4, 2008, pp.859-872.

〔学会発表〕（計１８件）

① Yang Li, Kazuo Sakiyama, Lejla Batina, Daisuke Nakatsu, Kazuo Ohta, Power

Variance Analysis Breaks a Masked ASIC Implementation of AES, Design, Automation and Test in Europe (DATE 2010), 査読有り, 2010年3月10日, Dresden, Germany

② Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, Goichiro Hanaoka, Improving Efficiency of An 'On the Fly' Identification Scheme by Perfecting Zero-Knowledgeness, RSA Conference 2010, Cryptographer's Track (CT-RSA'10), 査読有り, 2010年3月1日, San Francisco, USA

③ 花谷嘉一，太田和夫, 情報を漏洩するランダムオラクルモデルにおける半自動証明, 暗号と情報セキュリティシンポジウム2010（SCIS2010），2010年1月20日，香川県

④ 長井 大地, 塙 知剛, 岩本 貢, 崎山 一男, 太田 和夫, PUF-HB 認証プロトコルに対する能動的な攻撃, 暗号と情報セキュリティシンポジウム2010 (SCIS2010)，2010年1月20日，香川県

⑤ Yusuke Naito, Kazuki Yoneyama, Lei Wang, Kazuo Ohta, How to Confirm Cryptosystems Security: The Original Merkle-Damgard is Still Alive!, ASIACRYPT 2009, 査読有り 2009年12月9日, Tokyo, Japan

⑥ 駒野 雄一, 太田 和夫, 三宅 秀享, 新保 淳, 証明可能安全なアルゴリズム的耐タンパ認証装置(3), Multimedia, Distributed, Cooperative, and Mobile Symposium 2009 (DICOMO2009), 査読あり, 2009年7月10日, 大分県

⑦ Kazuo Sakiyama, Tatsuya Yagi, Kazuo Ohta, Fault Analysis Attack against an AES Prototype Chip using RSL, RSA Conference 2009, Cryptographer's Track (CT-RSA'09), 査読有り, 2009年4月22日, San Francisco, USA

⑧ Kazuo Ohta, Cryptographic Applications of Indifferentiability via Leaking Random Oracle Models, Computational and Symbolic Proofs of Security (暗号の計算論的・記号的安全性証明に関するスプリングスクール＆ワークショップ)，招待講演, 2009年4月8日，静岡県

⑨ 花谷 嘉一, 角野 陽輔, 米山 一樹, 太田 和夫, CryptoVerifの証明能力の改良：誤った判定の回避, 日本応用数理学会 2009 年春の研究部会連合発表会, 2009年3月7日, 京都

⑩ 花谷 嘉一, 太田 和夫, 米山 一樹, 角野 陽輔, CryptoVerifを用いたFDH署名の緊密な安全性証明の検討, 暗号と情報セキュリティシンポジウム2009年1月23日，滋賀

⑪ 角野 陽輔, 花谷 嘉一, 米山 一樹, 太田 和夫, 安全性検証ツール CryptoVerif の改良：異常終了に対する一対策, 暗号と情報セキュリティシンポジウム 2009 年 1 月 23 日，滋賀

⑫ Bagus Santoso, Kazuo Sakiyama, Kazuo Ohta, Yet Another New 'On the Fly' Identification Scheme: Reducing Memory Cost by Improving Zero-Knowledgeness, 暗号と情報セキュリティシンポジウム 2009年1月23日，滋賀

⑬ Kazuki Yoneyama, Masayuki Terada, Sadayuki Hongo, Kazuo Ohta, Universally Composable Fair Voucher Exchange, 暗号と情報セキュリティシンポジウム 2009年1月22日，滋賀

⑭ Kazuki Yoneyama, Efficient and Strongly Secure Password-based Server Aided Key Exchange, International Conference on Cryptology in India, 査読有り, 2008年12月16日，カラグプル（インド）

⑮ Kazuki Yoneyama, Security Analyses on Cryptographic Protocols against Strong Adversaries using Task-structured PIOA Framework, The 4th Franco-Japanese Computer Security Workshop, 査読有り, 2008年12月6日，東京

⑯ Kazuki Yoneyama, Satoshi Miyagawa, Kazuo Ohta, Leaky Random Oracle, International Conference on Provable Security, 査読有り, 2008年10月31日，上海（中国）

⑰ Kazuki Yoneyama, Anonymous Message Authentication: Universally Composable Definition and Construction, International Conference on Security and Cryptography 査読有り, 2008年7月28日，ポルト（ポルトガル）

⑱ サントソ バグス, 太田 和夫, A New 'On the Fly' Identification Scheme: A Trade-off of Asymptoticity between ZK and Correctness, 暗号と情報セキュリティシンポジウム2008年1月23日，宮崎シーガイア

〔図書〕（計７件）

① 花谷嘉一，太田 和夫（分担執筆者），共立出版，**数理的技法による情報セキュリティ**，第3章「ゲーム列による安全性証明の基礎」，2010，37-64 ページ

② 米山 一樹，太田 和夫 （分担執筆者），共立出版，**数理的技法による情報セキュリティ**，第 5 章「タスク構造確率 I/O オートマトンを用いた安全性証明」，2010，87-110 ページ

③ Lejla Batina，Kazuo Sakiyama，Ingrid Verbauwhede （分担執筆者），Springer，"Compact Public-key Implementations for RFID and Sensor Nodes," Chapter in I. Verbauwhede editor，Secure Integrated Circuits and Systems，2010，179-196 ページ

④ 太田 和夫（分担執筆者），丸善株式会社書，現代数理科学事典，（編集代表 広中 平祐），VIII 情報の理論，3. 暗号理論の数理，3.4 デジタル署名方式 執筆担当，2009，932-935 ページ

⑤ Michael Sipser （著），太田和夫（監訳），共立出版，計算理論の基礎（原著第２版）１オートマトンと言語，2008，232 ページ

⑥ Michael Sipser （著），太田和夫（監訳），共立出版，計算理論の基礎（原著第２版）２計算可能性の理論，2008，208 ページ

⑦ Michael Sipser （著），太田和夫（監訳），共立出版，計算理論の基礎（原著第２版）３複雑さの理論，2008，290 ページ

〔産業財産権〕
○出願状況（計１件）
① 名称：本人確認システム
発明者：Bagus Santoso，崎山一男，太田和夫
権利者：電気通信大学
種類：特許出願
番号：2008-289266
出願年月日：2008 年 11 月 11 日
国内外の別：国内

〔その他〕
ホームページ等
http://www.oslab.ice.uec.ac.jp

６．研究組織
(1)研究代表者
太田　和夫（OHTA KAZUO）
電気通信大学・電気通信学部・教授
研究者番号：８０３３３４９１

(2)研究分担者
西野　哲朗（NISHINO TETSURO）
電気通信大学・電気通信学部・教授
研究者番号：１０１９８４８４

崎山 一男（SAKIYAMA KAZUO）
電気通信大学・電気通信学部・准教授
研究者番号：８０５０８８３８

(3)連携研究者
國廣　昇（KUNIHIRO NOBORU）
東京大学・新領域創成科学研究科・准教授
研究者番号：６０３４５４３６