科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１８　日現在

機関番号：　３３９０３
研究種目：　若手研究(B)
研究期間：　2011～2013
課題番号：　２３７０００２４

研究課題名（和文）形式手法に基づくプライバシ検証に関する研究

研究課題名（英文）On computer-assisted verification of privacy related properties

研究代表者
河辺　義信（Kawabe, Yoshinobu）

愛知工業大学・情報科学部・准教授

研究者番号：８０３９６１８４

交付決定額（研究期間全体）：（直接経費）　　2,900,000円、（間接経費）　　870,000円

研究成果の概要（和文）：近年ＩＣＴ社会において，プライバシ保護の必要性が強く叫ばれている．本研究では，従来より提案されていた「匿名性」の論理的な定義とその検証法を用いて，さまざまなプライバシ関連の性質を証明する手法を明らかにした．具体的には，「無証拠性」と呼ばれる，電子投票の秘密を守るための条件を匿名性として定式化し，Ｌｅｅらの電子投票プロトコルの無証拠性の証明に応用した．また，Ｃｒｏｗｄｓと呼ばれる秘密通信路の分散実装（および，その拡張）を形式的に記述し，その正しさを示した．さらには，プライバシを示す上で必要になるトレース一致と呼ぶ条件を，Ａｌｌｏｙと呼ばれる全自動の検証器を用いて検証する手法について明らかにした．

研究成果の概要（英文）：On the Internet, there are many services and protocols where privacy should be provided. By extending a computer-assisted proof technique for anonymity, this study developed a new method to prove privacy related properties. Specifically, we formalized the receipt-freeness property, which is a privacy-related property for electronic voting and is an extension of anonymity, and we proved that an electronic voting protocol by Lee et al. is receipt-free. Also, we described the Crowds protocol formally. Crowds is a communication system for a web access that preserves the sender's privacy. In this study, a computer-assisted proof for the sender's privacy is conducted, and an extension of Crowds which is for preserving the recipient's privacy is described in a formal specification language. Finally, this study described a sufficient condition for a trace equivalence of two systems in Alloy, which enables a fully automatic proof of privacy related properties.

研究分野：　情報学

科研費の分科・細目：　計算基盤・情報セキュリティ

キーワード：　プライバシ　形式手法　検証　定理証明　無証拠性　Crowds　セキュリティプロトコル

１．研究開始当初の背景

近年，プログラム理論やソフトウェア工学の分野において，ソフトウェアの正しさを論理的に検証する手法（形式手法と呼ばれる．また，「数理的技法」や「フォーマルメソッド」とも呼ばれる）が研究され，当該分野の中心テーマの一つとなっている．なかでも，暗号プロトコル（セキュリティプロトコルとも呼ばれる）を対象とした形式手法が世界的な注目を集めており，秘匿性（盗聴した暗号文をどのように組み合わせても平文を取り出せないこと）などが研究されてきた．

一方で，セキュリティの重要な性質として，プライバシが知られている．プライバシは秘匿性よりも検証が難しいとされる．たとえば，秘匿性を満たすプロトコルでもプライバシが満たされるとは限らない．

たとえば，ネット上で政党代表者選挙を行う，ある電子投票サーバを考えてみよう．この投票サーバは，「党員の投票のみを受け付け，それ以外には返信しない」という設計になっていて，かつ「すべての投票メッセージとそれに対する返信メッセージは厳重に暗号化されており，仮に第三者に盗聴されたとしても，票の内容が漏れることはない」ようにできているとしよう．さらに，ネットワーク上の二人のユーザ A と B が，投票サーバに投票データを送ったとする．ここでもし，両ユーザと投票サーバのやりとりが盗聴されていて，さらに「投票サーバはユーザ A に返信したが，ユーザ B には返信しなかった」という結果が観測されたとき，盗聴者に対して何か情報が漏れてしまうだろうか？ じつは，厳重な暗号化によって投票内容や返答メッセージの内容が全くわからないようになっているにもかかわらず，「ユーザ A には返信があったから A はこの政党の党員であり，一方ユーザ B には返信がなかったことから党員ではない」といったように，政党の所属に関する個人情報が盗聴者に漏れてしまう．

ここで述べた電子投票の例のように，全データを暗号化しても，通信パターン（具体的には，ユーザ A と B に対する返信パターン）の非対称性から，「A は党員である」という個人情報が漏れてしまうことがある．プライバシを保証するには，こうした通信パターンの正しさの検証が必要であるが，そのような技術は小規模な場合に限られていたり，あるいは手証明の場合に限られていた．たとえば，文献

J. Y. Halpern and K. R. O'Neill. “Anonymity and information hiding in multi-agent systems”. Journal of Computer Security, Vol. 13, No. 3, pp. 483-514, 2005.

ではマルチエージェント系を用いて通信パターンの正しさの検証を試みているが，その証明は基本的に手作業であり，計算機を使った証明は困難であった．

２．研究の目的

研究代表者らは，本研究の開始以前から，予備研究（たとえば，文献

Y. Tsukada, K. Mano, H. Sakurada and Y. Kawabe. “Anonymity, privacy, onymity and identity: a modal logic approach”. In IEEE PASSAT-09, pp. 42-51. IEEE CS Press, 2009.

Y. Kawabe et al. “Theorem-proving anonymity of infinite state systems”. Information Processing Letters, Vol. 101, No. 1, pp. 46-51, 2007.

など）において，匿名性（「誰がやっているか」の情報が漏れないこと）の論理的な定義と，数学的帰納法による匿名性の自動検証技術を提案してきた．プライバシに属する様々な性質（たとえば，電子投票システムを扱うユーザが，自分の投票内容を秘密のままにしておける「無証拠性」と呼ばれる性質）は広い意味では匿名性とみなせるため，上記の予備研究により，原理的には計算機でプライバシを検証できるようになったと言える．しかしながら，無証拠性などの性質には，攻撃者の有無や能力などに関する条件の違いがあるため，実際にプライバシを匿名性検証技術で扱えるようにするには，こうした前提条件を明らかにし，論理式として記述する必要があった．

そこで本研究では，プライバシを匿名性検証技術で扱うための各種の「前提条件」を明らかにし，その前提条件を匿名性検証技術に組み込むことで，超大規模システムのための「プライバシの自動検証技術」を構築することを目的とした．

３．研究の方法

上記の目的を達する方法として，具体的には，「電子投票（FOO プロトコルや Lee らのプロトコルが知られている）」や「匿名通信路（Mixnet, Crowds, Tor（Onion Routing）などが有名）」などの主要な暗号プロトコルを IOA 言語（分散アルゴリズムの記述・解析の理論である「I/O-オートマトン」に基づく仕様記述言語）でモデル化し，さらに無証拠性などの性質を計算機で検証する実験を繰り返しながら，プライバシの自動検証に必要な各種の条件を明らかにすることにした．検証実験を短期間で効率的に行うため，既存のモデル検査器（「しらみつぶし」に基づく全自動の検証技術）や定理証明器（半自動の検証技術）などを活用することとした．最終的に

はモデル検査（もしくは，SAT ソルバと呼ばれる全自働の検証ツールでも良い）による全自動化を目指すが，困難なことも予想されたため，その場合は，定理証明による実装に切り替え，「ユーザ（検証者）をアシストするツール」を目指すこととした．

４．研究成果

本研究では，まず，電子投票プロトコルのプライバシに関する重要な性質として知られる「無証拠性」を題材に，計算機を用いた検証実験を行った．電子投票プロトコルが無証拠性を満たすというのは，そのプロトコルが匿名性を満たし，なおかつ，以下の条件を満たすことを言う．

(1) 攻撃者は，投票終了後，脅迫などによって「どの候補者に投票したのか」を投票者から聞き出すことができる（聞き出した情報を「レシート」と呼ぶ）．ただし投票者は，せめてもの抵抗として，攻撃者に対し，嘘の情報(嘘のレシート)を渡すことができる．
(2) 投票者は，どの候補者に投票したかを証明できない．つまり，攻撃者が投票結果を検証する際，投票者が正直に白状した場合でも，嘘をついている場合でも，どちらの場合でも検証が成功してしまう．

つまり，上記の二つの条件が，無証拠性に必要な「前提条件」であると言える．これらの条件を論理式として記述し，匿名性とともに検証ツールで証明すれば，無証拠性を計算機で自働検証できたことになる．本研究では，Lee らの電子投票プロトコル（このプロトコルの詳細は，文献

B. Lee et al.
“Providing receipt-freeness in mixnet-based voting protocols”.
In 6th International Conference on Information Security and Cryptology (ICISC 2003), LNCS 2971, pp. 245-258, Springer-Verlag, 2004.

で述べられている）を題材とし，I/O-オートマトンモデル（IOA 言語）でこの電子投票プロトコルの設計図を記述した．さらに，上記の無証拠性の条件（および匿名性のための条件）を一階述語論理式として記述した上で，Lee らの電子投票プロトコルの設計図がこの論理式を満たすことを，Larch 定理証明器（Larch Prover）と呼ばれる半自動の検証ソフトウェアを用いて証明した．この結果，Lee らの電子投票プロトコルが匿名性を満たしており，なおかつ票の買収行為が事実上無意味になる意味でプライバシがきちんと守られることを，論理的に保証した（第５節の雑誌論文[1]が対応）．

もともと無証拠性は電子投票プロトコルの性質として考案されたが，上記の検証実験から整理し，より一般的に考えると，セキュリティプロトコルの無証拠性とは，匿名性を満たし，なおかつ「そのプロトコルを観測して得られる情報に加えて，別の付加的な情報を通信者が外部に与えたとしても，ある結果をもたらす通信パターンと(結果が同じとなるような)別の通信パターンが区別できない」という性質だと言える．本研究の検証実験を通じて，この知見を得ることができた．また，これにより，電子投票プロトコル以外の様々なプロトコル（たとえば，インターネットオークションプロトコルなど）に対しても，無証拠性を計算機で形式的に検証するための見通しがついた．

本研究ではさらに，アクセス者の情報を隠しながらウェブアクセスを実現するためのシステムである「Crowds」を対象としたプライバシの検証を行った．Crowds はよく知られた匿名ウェブアクセスシステムであるが，そのシステムはルータの集合体から成る．本研究の検証実験では，「コラプト（corrpupt)」と呼ばれる，コンピュータウィルスに感染した状態に陥った Crowds ルータの存在する場合までも考慮し，どのような条件のときに送信元ユーザを隠せるのかを，I/O-オートマトン理論の立場から明らかにした（第５節の学会発表[8][13]が対応）．さらに本研究では，河野らにより提案された Crowds の拡張に対しても，IOA 言語によるモデル化とプライバシ検証を実施した（学会発表[12]が対応）．この拡張されたプロトコルは，文献

K. Kono, Y. Ito, and N. Babaguchi.
“Anonymous communication system using probabilistic choice of actions and multiple loopbacks”, Proc. Information Assurance and Security (IAS), pp. 210-215, 2010.

で示されたものであるが，「メッセージの目的地を一時的に変更してルータ間で交換しあうような拡張」をすることで，（送信者を隠すだけでなく）受信者が誰なのかも隠すことができる．河野らの文献では送信者に関するプライバシのみを分析していたが，本研究では，これに加えて，受信者の匿名性までも扱った．

上記の 2 種類の実験は，Lee らの電子投票プロトコルに対する検証実験と同じく，Larch 定理証明器を用いて行った．なお，河野らの上記文献での分析は，プロトコルの確率的動作を考慮したものであるが，本研究では，それよりも少し単純化された，非決定的な状況における動作の解析を行っている．そのため，研究代表者らが行ってきた確率的匿名性の理論

I. Hasuo, Y. Kawabe and H. Sakurada,

“Probabilistic anomymity via coalgebraic simulations”, Theoretical Computer Science, Vol. 411, No. 22-24, pp. 2239-2259, 2010.

に基づき，確率的動作までも考慮してプライバシ検証を行っていくことが，今後は必要である．

上記のいくつかの検証実験を通じて，どのような論理式をプライバシの前提条件として記述すればよいのかが明らかになった．しかし，これまでにも述べた通り，これらの検証実験は，Larch 定理証明器を用いて，半自動で行われている．そこで本研究では，プライバシの全自働検証に向けての試みも行った．プライバシの重要な前提条件である匿名性を示すには，セキュリティプロトコルとそれに対応する自明に匿名的なプロトコルの間に「トレース集合の一致」と呼ばれる条件が成り立つことを示す必要がある．具体的にこれを I/O-オートマトン理論の中で示すには，フォワードシミュレーションと呼ばれる状態集合上の二項関係の存在を証明すればよい（注：システム A からシステム B へのフォワードシミュレーションを示すことで，A と B のトレース集合の包含が示される．よって，A と B のトレース集合の一致を示すには，A から B へのフォワードシミュレーションだけでなく，B から A へのフォワードシミュレーションも示す必要がある）．本研究では，Larch 定理証明器上で半自動により行われてきたふたつのシステムの間のフォワードシミュレーションの存在証明を，Alloy Analyzer と呼ばれる SAT ソルバを用いて全自動で行うことができた．この検証は，文献

山本 匠，加藤 岳久，西垣 正勝，“振り込め詐欺への現実的な対策についての検討”，情報処理学会 第 13 回コンピュータセキュリティシンポジウム，pp. 621 - 626, 2010.

で示されている振込め詐欺防止用に拡張された電話システムに対して行われている（学会発表[1][3][7][11]が対応）．

最後に本研究では，プライバシの検証を行った分散システム仕様の実装に向けた試みとして，I/O-オートマトンモデルで記述されたシステム仕様を直接分散環境下で実装する手法についても検討を行った（学会発表[2][6]が対応）．また，組み込みシステムを実装するための言語処理系についての試作を行った（学会発表[4][5][9]が対応）．

上記を通じて，研究目的に示した課題を解決することができた．

５．主な発表論文等

〔雑誌論文〕（計　１　件）

[1] 河辺 義信，真野 健，櫻田 英樹，塚田 恭章，“電子投票プロトコルに対する無証拠性の定理証明”，情報処理学会論文誌，査読有，Vol. 52(9)，2011，pp. 2549-2561.

〔学会発表〕（計　13　件）

[1] N. Yoshimasa, J. Sakoh, and Y. Kawabe, “SAT-Solving Trace Equivalence of I/O-Automata with Alloy Analyzer: A Case Study”, 28th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2013), 2013 年 6 月 30 日～2013 年 7 月 3 日，麗水（韓国）.

[2] N. Yoshimasa, and Y. Kawabe, “An Implementation of IOA with A Functional Programming Language”, 28th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2013), 2013 年 6 月 30 日～2013 年 7 月 3 日，麗水（韓国）.

[3] J. Sakoh, N. Yoshimasa, and Y. Kawabe, “Automated Proof for Equivalence of Telephone Systems”, 12th IEEE International Conference on Computer and Information Science (ICIS 2013), 2013 年 6 月 16 日～2013 年 6 月 20 日，朱鷺メッセ（新潟県）.

[4] M. Osawa, N. Yoshimasa, and Y. Kawabe, “On Embedded Programming Education with A Tiny Lisp”, 12th IEEE International Conference on Computer and Information Science (ICIS 2013), 2013 年 6 月 16 日～2013 年 6 月 20 日，朱鷺メッセ（新潟県）.

[5] Y. Kozuka, N. Ito, K. Iwata, T. Mori, and Y. Kawabe, “A Development Framework for Humanoid Robots Simulation Systems”, IIAI International Conference on Advanced Information Technologies 2013 (IIAI-AIT 2013), 2013 年 11 月 28 日～2013 年 11 月 30 日.

[6]吉政 徳晃，河辺 義信，“関数型言語を用いた IOA 仕様の実装について”，電子情報通信学会 第 26 回 回路とシステムワークショップ，2013 年 7 月 29 日～2013 年 7 月 30 日，淡路夢舞台国際会議場（兵庫県）.

[7] Y. Kawabe, K. Kurono and A. Maeda, “Formal verification of a telephone system with a concierge server”, 27th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2012), 2012 年 7 月 15 日～2012 年 7 月 18 日，札幌コンベンションセンター（北海道）.

[8] Y. Kawabe, “Formalizing and verifying anonymity of Crowds-based communication protocols with IOA”, First Workshop on Information Hiding Techniques for Internet Anonymity and Privacy (IHTIAP 2012), in the proceedings of the Fourth International Conference on Evolving Internet (INTERNET 2012), 2012 年 6 月 24 日～2012 年 6 月 29 日, ベニス (イタリア).

[9] 大澤 愛美, 河辺 義信, “KED-SH101 を用いた組み込みプログラミングのための Lisp 言語”, 第 10 回 情報学ワークショップ (WiNF 2012), 2012 年 12 月 8 日～2012 年 12 月 9 日, 豊橋技術科学大学 (愛知県).

[10] 河辺 義信, “Larch Prover による論理パズルの解法”, 電子情報通信学会 2012 年ソサイエティ大会 (招待講演), 2012 年 9 月 11 日～2012 年 9 月 14 日, 富山大学五福キャンパス (富山県).

[11] 黒野 恵人, 前田 彩, 河辺 義信, “コンシェルジュサーバを持つ電話システムの形式的検証”, 電子情報通信学会 システム数理と応用研究会, 2012 年 3 月 9 日, JAIST 東京キャンパス (東京都).

[12] 河辺 義信, “多重ループバックを持つ Crowds プロトコルに対する匿名性の形式検証”, 電子情報通信学会 2012 年 暗号と情報セキュリティシンポジウム, 2012年2月2日, 金沢エクセルホテル東急 (石川県).

[13] 河辺 義信, “Crowds 型通信システムに対する形式検証について”, 第 9 回 情報学ワークショップ (WiNF 2011), 2011 年 11 月 25 日, 豊橋技術科学大学 (愛知県).

〔その他〕
http://aitech.ac.jp/~kawabe

６．研究組織
(1)研究代表者
河辺　義信（KAWABE, Yoshinobu）
愛知工業大学・情報科学部・准教授
研究者番号：80396184