様式 C-19

科学研究費補助金研究成果報告書

平成２２年６月１１日現在

研究種目：若手研究（B）
研究期間：2007～2009
課題番号：19700018
研究課題名（和文）　形式手法に基づくセキュリティプロトコルの匿名性検証法に関する研究

研究課題名（英文）　On Verifying Anonymity of Security Protocols with Formal Methods

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

研究成果の概要（和文）：本研究では，新たな匿名性の検証手法を提案した．この手法は，プログラム理論やソフトウェア工学の分野で注目を浴びる「形式手法」(数理的技法，フォーマルメソッドとも呼ばれる）を用いている．具体的には，匿名シミュレーション法と呼ばれる匿名性の証明法を，確率的匿名性や能動的攻撃者を許す場合にも扱えるように拡張した．さらに，Crowds と呼ばれる通信ルータの匿名性や Lee 電子投票の「無証拠性（匿名性の拡張)」を検証した．

研究成果の概要(英文)：This study proposed a new method to prove the anonymity of security protocols. We employ a formal method; specifically, we extended our “anonymous simulation method” to deal with probabilistic protocols and stronger adversaries. In this study, we demonstrated the anonymity verification for Crowds. Also, we proved the receipt-freeness property of an e-voting protocol.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1300000	0	1300000
２００８年度	900000	270000	1170000
２００９年度	700000	210000	910000
年度			
年度			
総　計	2900000	480000	3380000

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，セキュリティ検証

１．研究開始当初の背景

従来，プログラム理論やソフトウェア工学の分野において，プログラムに誤りが無いことを論理的に検証する手法（形式手法，数理的技法，フォーマルメソッドなどと呼ばれる）が研究され，当該分野の中心テーマの一つとなっている．なかでも近年，インターネット上の暗号プロトコル（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いる．

セキュリティ・プロトコルの検証では，「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」を表す性質（秘匿性）などが研究され，実際，クレジットカード決済プロトコルの安全性検証にも応用されていた．一方で，個人情報漏洩にかかわる性質として，「通信者が誰なのか，攻撃者に知られないこと」を表す性質（匿名性）が重要視されてきた．匿名性は，一般に，秘匿性よりも形式検証が難しい．たとえば，秘匿性を満たすプロトコル（すなわち，すべてのデータが暗号化されていて，盗聴してもその平文を知ることができないようなプロトコル）を扱う場合でも，「返信の有無」「メッセージの個数」「メッセージ発信のタイミング」などの送受信に関する情報を解析することで，通信者やその特徴を割り出せてしまう場合があった．

匿名性を保証するためには，通信パターンの正しさをコンピュータで検証する技術が必要である．しかし，それまでの匿名性の検証技術は小規模システムの場合に限られていたため，国内外の研究を考慮しても十分解明されているとは言えなかった．

２．研究の目的

研究代表者らは，状態遷移機械（具体的には，I/O-オートマトン）のトレース集合上の性質として匿名性（トレース匿名性）を定義し，セキュリティ・プロトコルの実行ステップ数に関する帰納法で匿名性を証明する手法（匿名シミュレーション法）を提案している．この研究により，無限状態システムなど大規模システムのための匿名性検証が可能となり，さらにコンピュータを使った匿名性検証の基本的な方法論が明らかとなった．しかし，この手法は「非決定的動作をするプロトコル」の「盗聴攻撃への耐性」を示す検証法であったため，より広い範囲のセキュリティ・プロトコルに対応できる検証法を構築するには，プロトコルの確率的振舞いやデータを送りつけてくる能動的攻撃者なども形式化し，匿名性を検証する必要があった．

そこで本研究では，従来の手法で直接扱うことのできなかった

（１）確率的動作をするプロトコル
（２）能動的攻撃者がいる場合

を扱い，匿名性を形式化することを目的とした．さらに匿名性・プライバシに関連した他の性質も扱えるように検証法を拡張し，応用範囲を広げることも視野に入れた．

３．研究の方法

確率的動作をするプロトコルと能動的攻撃者がいる場合の形式的な扱いについて，本研究では，従来の匿名シミュレーション法をそれぞれの目的にあう形で，拡張することにした．具体的な方法としては，以下の通りである．

（１）確率的匿名性の扱いについて：蓮尾らによる余代数理論に基づく“generic trace theory”（詳細は

Ichiro Hasuo, Bart Jacobs and Ana Sokolova, “Generic Trace Theory”, CMCS 2006, ENTCS 164, pp. 47-65. Elsevier Science, 2006.

Ichiro Hasuo, “Generic Forward and Backward Simulations”, CONCUR 2006, LNCS 4137, pp. 406-420, 2006.

など）を応用する方法を用いた．すなわち，トレース匿名性と匿名シミュレーションの手法を蓮尾らの枠組みの上で記述することで，従来の（非決定的）トレース匿名性の定義や（非決定的）匿名シミュレーション法を，確率的トレース匿名性や確率的匿名シミュレーション法に拡張する．さらに，匿名通信路を実現する通信ルータとして注目されている Crowds システム などを対象に検証実験を行うこととした．

（２）能動的攻撃者の扱いについて：以下の方法で取り組んだ．まず最初に，I/O-オートマトンのトレース集合に基づく匿名性である「トレース匿名性」を，攻撃者がいる場合に拡張する．あわせて，匿名シミュレーション関係に基づく証明技法も，攻撃者のいる場合に拡張する．さらに本研究では，この新しい匿名性検証法を用いて，Crowds システムの（非決定的な意味での）匿名性を証明する事例研究を試みた．一方で，本研究では，能動的攻撃者に関連した電子投票システムの性質を上記の枠組みで記述することにした．無証拠性と呼ばれる電子投票の性質が知られており，これは，盗聴よりも強い攻撃者がいる環境での匿名性に対応

する．無証拠性を「拡張されたトレース匿名性」に含まれる性質として扱うことで，新しい匿名シミュレーション技法を用いて無証拠性を証明する．

４．研究成果

「確率的匿名性」の扱いについては，雑誌論文①において，以下の結果を得た．まず，確率的匿名性を形式的に定義し，さらに確率的匿名性を検証するための手法を構築した．これを行う上で，本研究では，蓮尾らの“generic trace theory”を用いた．具体的には，トレース匿名性と匿名シミュレーションの手法を蓮尾らの枠組みの上で記述することで，従来の（非決定的）トレース匿名性の定義や（非決定的）匿名シミュレーション法を，確率的トレース匿名性や確率的匿名シミュレーション法に拡張することを行っている．また，確率的匿名シミュレーション法の健全性（すなわち，検証法の正しさ）は，蓮尾らの理論により自動的に導かれる．さらに，モデル検査器や定理証明器（コンピュータ上で数学の問題を解くツール）で確率的匿名性を示すための，具体的な条件を明らかにすることができた．上記に加えて，我々は，匿名通信路を実現する通信ルータとして注目されている Crowds システムを対象とした確率的匿名性の証明を行った．ところで，従来のトレース匿名性は，「strong anonymity」と呼ばれる匿名性を（非決定的な）I/O-オートマトンの理論で定義したものである．これに対して，上記の Crowds の証明では，「probable innocence」と呼ばれる少し条件の弱い匿名性まで扱い，形式化することができた．さらに，probable innocence のためのシミュレーション関係を導いている．

「能動的攻撃者がいる場合」の扱いについては，雑誌論文③および学会発表⑤⑥⑦において，以下の結果を得た．まず，攻撃者がいる場合の匿名性を，I/O-オートマトンのトレース集合を用いて定義し，さらに匿名性の証明法を導入した．この証明法は，ある条件を満たす「良い種類の」匿名シミュレーションの存在を示すというものである．我々は，この新しいシミュレーション関係が成り立つとき，攻撃者のいない場合の匿名性が攻撃者のいる場合にまで拡張できることを示した．これにより，セキュリティ・プロトコルに対して，

１．まず，盗聴者のみの場合の匿名性を証明する
２．次に，１．の証明で見つけた匿名シミュレーションから作られる「拡張された匿名シミュレーション関係」が，攻撃者のアクションによって保存されることを示す

というステップを踏むことで，段階的に攻撃者がいる場合の匿名性を示せるようになった．また，本研究では，この新しいシミュレーション関係による匿名性検証法を用いて，Crowds システムの（非決定的な意味での）匿名性を証明する事例研究を試みた．とくにこの事例研究を通じて，「攻撃者がいる場合に，ツールを用いてどのように匿名性を検証すればよいか」について，方法論を具体化することができた．

さらに本研究では，盗聴者よりも強い攻撃者に関連した電子投票システムの性質を，上記の枠組みで記述した（学会発表①③）．無証拠性と呼ばれる電子投票の性質が知られており，これは，「盗聴よりも強い攻撃者がいる環境での匿名性」に含まれる性質である．Jonker らは，文献

H. L. Jonker and W. Pieters, “Receipt-freeness as a special case of anonymity in epistemic logic”, Proc. of the IAVoSS Workshop On Trustworthy Elections (WOTE 2006), pp. 29-30, 2006.

において，無証拠性を

> 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投票者が外部に与えたとしても，ある投票パターンと別の(内訳の同じ)投票パターンが区別できないこと

と考え，知識論理を用いた匿名性の形式化に基づく無証拠性の定義を述べている．Jonker らと同様の考え方に基づいて，拡張されたトレース匿名性の形式化のもとで無証拠性を匿名性として形式化すれば，匿名性の定理証明手法を無証拠性にも適用できると考えた．実際，本研究ではこの考え方に基づき，無証拠性を I/O-オートマトンのトレース集合を用いて形式化した．さらに，Lee 電子投票プロトコルを題材に形式化を行い，定理証明器による無証拠性の検証を行っている（検証時に作られた定理証明器の

「証明スクリプト」は，研究代表者のウェブページで公開している）．

そのほか，本研究の一部として，「能動的攻撃者がいる場合」の基礎となる新たな匿名シミュレーション法（バックワード型匿名シミュレーション法）を，雑誌論文②において示した．さらに関連して，学会発表②④では匿名性を知識論理（さきの Jonker の道具立てと同様のもの）を用いて分類している．

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３件）

① Ichiro Hasuo, Yoshinobu Kawabe and Hideki Sakurada, “Probabilistic anomymity via coalgebraic simulations”, Theoretical Computer Science, 査読有, volume 411, No. 22-24, pages 2239-2259, 2010.

② Yoshinobu Kawabe, Ken Mano, Hideki Sakurada and Yasuyuki Tsukada, “On backward-style anonymity verification”, IEICE Transactions, 査読有, volume E91-A, No. 9, pages 2597-2606, 2008.

③ Yoshinobu Kawabe and Hideki Sakurada, “An adversary model for simulation-based anonymity proof”, IEICE Transactions, 査読有, volume E91-A, No. 4, pages 1112-1120, 2008.

〔学会発表〕（計７件）

① 河辺 義信,“無証拠的プロトコルのフォーマルな記述について”, 第 21 回 電気関係学会東海支部連合大会, 2009.（2009 年 9 月 11 日, 於：愛知県豊田市）

② Yasuyuki Tsukada, Ken Mano, Hideki Sakurada and Yoshinobu Kawabe,“Anonymity, privacy, onymity and identity: a modal logic approach”, IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT-09), pages 42-51. IEEE Computer Society Press, 2009.（2009 年 8 月 29 日, 於：カナダ・バンクーバー市）

③ 河辺 義信, 真野 健, 櫻田 英樹, 塚田 恭章,“I/O-オートマトンによる無証拠性の形式化について”, 電子情報通信学会 2009 年 暗号と情報セキュリティシンポジウム, page 346（アブストラクト, 論文本体は CD-ROM で配布）,2009.（2009 年 1 月 23 日, 於：滋賀県大津市）

④ 塚田 恭章, 真野 健, 櫻田 英樹, 河辺 義信,“匿名性・プライバシ・顕名性・アイデンティティへの知識論理的アプローチ”, 情報処理学会 第 11 回 コンピュータセキュリティシンポジウム, pages 599-604, 2008.（2008 年 10 月 8 日, 於：沖縄県宜野湾市）

⑤ 河辺 義信, 真野 健, 櫻田 英樹, 塚田 恭章,“能動的な攻撃者が存在するシステムに対する匿名性の検証について”, 電子情報通信学会 2008 年 暗号と情報セキュリティシンポジウム, page 119（アブストラクト, 論文本体は CD-ROM で配布）,2008.（2008 年 1 月 23 日, 於：宮崎県宮崎市）

⑥ Yoshinobu Kawabe and Hideki Sakurada, “A formal approach to designing anonymous software”, 5th International Conference on Software Engineering Research, Management and Applications (SERA '07), pages 203-212. IEEE Computer Society Press, 2007.（2007 年 8 月 21 日, 於：韓国釜山市）

⑦ 河辺 義信, 櫻田 英樹,“攻撃者を考慮した匿名性検証法”, 電子情報通信学会 第 20 回 回路とシステム軽井沢ワークショップ, pages 367-372, 2007.（2007 年 4 月 23 日, 於：長野県軽井沢町）

〔その他〕
ホームページ等
http://aitech.ac.jp/~kawabe/
研究代表者のウェブページ．ここでは，Lee 電子投票の無証拠性の証明スクリプト（バッチファイルのようなもの）を公開している．用いた定理証明器は，LP（Larch Prover）である．

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