様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１５　日現在

機関番号：　３３９０３
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１６６

研究課題名（和文）セキュリティプロトコルの時間匿名性に対する形式検証法の研究

研究課題名（英文）Formal verification of anonymity for timed security protocols

研究代表者
河辺　義信（Kawabe, Yoshinobu）

愛知工業大学・情報科学部・教授

研究者番号：８０３９６１８４

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：近年，ＩＣＴ社会におけるプライバシ・匿名性保護の必要性が強く叫ばれている．とくに，スマートフォン，ロボット，車載ソフトウェア等の「実時間システム」がインターネットに接続され，個人情報を扱う時代が到来しつつあることから，実時間システムの匿名性（時間匿名性）をモデル化し効率的に検証できるようにする必要がある．しかし，時間を考慮しないシステムの匿名性にくらべ，実時間システムの匿名性には，モデル化などに特有の難しさがあった．本研究では，暗号プロトコルの時間匿名性を定式化し，さらに計算機で効率的に検証する技術を開発することで，この課題を解決した．

研究成果の概要（英文）：Recently, many real-time systems such as smartphones, intelligent robots, and vehicular software are connected to the Internet, and they are running security protocols that deal with privacy-related information. Hence, it is getting more important to establish the anonymity of real-time systems. In this study, we are interested in a formal verification for the anonymity of timed security protocols. Compared with the anonymity of untimed systems, the timed anonymity property was not investigated well, since there are some difficulties in modeling of timed anonymity. In this study, we provided a formalization of timed anonymity, and we developed a proof technique for the timed anonymity of security protocols. Our technique is based on I/O-automaton theory, and the theory provides computer-assisted theorem proving tools. With such tools, we can theorem-prove the timed anonymity of security protocols.

研究分野：　形式手法，セキュリティ検証

キーワード：　匿名性　実時間システム　形式手法　検証　定理証明　セキュリティプロトコル

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，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）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，匿名性が知られている．匿名性は，秘匿性よりも検証が難しいとされる．たとえば，太郎と花子の間でやりとりされる暗号文が解読できなくても，

「やりとりがある以上，
太郎と花子は知り合いに違いない」

との推測はできる．つまり，秘匿性（暗号文の中身がわからない）が成り立つ状況でも，匿名性（送受信者間の関係性がわからない）が成り立つとは限らないのである．

さらに近年，スマートフォン，ロボット，車載ソフトウェアなどの，数多くの「実時間システム」がインターネットに接続されつつあり，そうした実時間システムによって個人情報が扱われる時代の到来が予想される．しかしながら，そうした実時間システムの匿名性（時間匿名性）については，とくに扱うことが難しいと考えられる．たとえば，次のような「午後３時を投票期限とする，電子投票サーバ」の例を使って，その難しさを考えてみよう．

インターネット上に投票サーバがあり，午後３時まで投票を受け付けているとしよう．また，ネットワークには二人のユーザＡとＢが繋がっており，適宜，サーバに投票データを送るとする．票をあらわすデータは暗号を使って厳重に秘匿されていて，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とする．さて，ここで仮に，ユーザＡの送った投票データが２時５９分にサーバに届き，一方で，ユーザＢは票を４時過ぎに発出したとしよう．そして，それらのやりとりが盗聴されており，「ユーザＢの投票データは，午後４時過ぎにサーバに送られた」ことまで観測されたとする．いま，厳重に暗号化をしていることから，投票データの内容は外部には漏れないようになっている．しかしながら，盗聴者は「ユーザＢの投票は，受け付け期限の午後３時には間に合わなかった．だから，ユーザＢは，どの候補者にも投票できなかったはずだ．」という情報を得てしまう．つまり，観測によって直接得られる投票時間に関する情報のみならず，「誰にも投票できていない」という投票内容に関する情報まで，同時に漏れてしまうのである．

ここで述べた投票期限つき電子投票の例のように，全データが暗号化されていても，どのタイミングで処理がなされたかに関する，時間的な「非対称性（つまり，ユーザ A は午後 3 時前だが，ユーザ B は午後 3 時よりも後ということ）」から，「今回の投票で，ユーザ B は，誰にも投票していない」などの個人情報が漏れてしまうことがある．

これまでに，匿名性を検証するための研究としては，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行う文献

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.

などがあったが，従来の検証技術は時間を考慮しない場合のみを扱っており，国内外の研究を考慮しても，時間匿名性が十分に定式化され検証技術が確立しているとは言えなかった．

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”, Transactions on Data Privacy, Vol. 3 (3), pp. 177-198, 2010.

I. Hasuo, Y. Kawabe, and H. Sakurada, “Probabilistic anomymity via coalgebraic simulations”, Theoretical Computer Science, Vol. 411, No. 22-24, pp. 2239-2259, 2010.

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，Vol. 52(9), 2011, pp. 2549-2561.

など）において，通信システムの匿名性やその拡張に対するフォーマルな定義と，数学的帰納法による匿名性の検証技術を提案してきた．これらの予備研究により，さまざまな分散システムや通信プロトコルなどの匿名性を，定理証明ソフトウェアを用いて，計算機で検証することが可能となっている．しかしこれらの手法は，時間を考慮しない場合において構築された手法であった．

そこで本研究では，第１節で述べたような実時間システムの持つ問題を考慮した匿名性の定義や証明手法を検討し，「超大規模実時間システムのための時間匿名性の自動検証技術」を構築することを目的とした．

３．研究の方法

研究開始当初の時点では，上記の目的を達する方法として，すくなくとも，二通りの方法が考えられた．

予備研究では，I/O-オートマトンと呼ばれる，分散アルゴリズムの記述・解析のための理論を用いて，匿名性検証手法を構築している．この理論に対して，Kaynar らは，通常の I/O-オートマトンの拡張として「時間 I/O-オートマトン」を定義している．さらに，通常の I/O-オートマトンで開発されたトレース包含のための証明手法を，時間 I/O-オートマトンにまで拡張している．時間匿名性を扱うためのひとつめの考え方は，通常の I/O-オートマトンで議論された「匿名性の定義」や「証明手法」を時間 I/O-オートマトン上で展開することで，時間匿名性の検証理論を得るという方法である．ただし，このアプローチでは，時間 I/O-オートマトン特有の概念や前提条件があるため（たとえば，通常の I/O-オートマトンと時間 I/O-オートマトンでは，匿名性の定義に必須の「トレース」と呼ばれる概念に相違点がある），実際には，それら条件等に対応するように匿名性の定義をうまく拡張せねばならない．

もうひとつの方法は，従来型の I/O-オートマトンモデルに基づき，これに時間パラメータを加えた形で実時間システムをモデル化して時間匿名性を検証するという考え方である．こちらのアプローチでは，上記の「時間 I/O-オートマトン特有の概念や前提条件」を検証者が直接扱う必要があるが，さまざまな暗号プロトコルを IOA 言語（I/O-オートマトン理論に基づく仕様記述言語）でモデル化し，さらに IOA 言語のための既存の定理証明ソフトウェア（半自動での検証が可能となる技術）もしくはモデル検査器（「しらみつぶし」に基づく全自動の検証が可能となる技術）の適用が可能になると期待される．

本研究では，上記のどちらのアプローチをとるか検討するため，まずは実時間システムのモデル化に関する事例研究を行っている．その結果として，本研究では後者のアプローチを採用した．また，作成する時間匿名性の検証ツールとして，定理証明ソフトウェアに基づく，「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，実時間システムの記述例として直噴ガソリンエンジンの制御部を題材として選び，通常の I/O-オートマトン（実際には，IOA 言語）でその動作を記述した．動作記述については，抽象版と具体版の 2 種類を記述した．さらに，両者のトレース集合の包含関係を，I/O-オートマトンのよく知られた証明技法（シミュレーション技法）で示せることを確認した．これにより，従来型の I/O-オートマトンモデルに基づき，これに時間パラメータを加えた形で，無限状態システムとして実時間システムをモデル化・検証できることを確認した．I/O-オートマトンモデルは，もともと，状態数の有限性を仮定しない．そのため，検証ツール（定理証明ソフトウェア）も無限状態システムに対応しており，時間システムを扱うことができる．本研究では上記のほか，関連して，定理証明ソフトウェアを用いた数学問題の証明実験や，IOA 言語で記述されたシステムの実装方法についても検討を行った．さらに，SCRAM と呼ばれるロボットの移動経路決定アルゴリズムの拡張や AI ミニ四駆の制御（いずれも，実時間システムの典型例）についても，検討を行なっている．

上記の実時間システムのモデル化・検証実験を進めるなかで，時間匿名性を扱う際には，時間 I/O-オートマトン特有の前提条件を必ずしもすべて扱う必要はないことが明らかとなった．たとえば，時間 I/O-オートマトンの理論では「時間経過を表す状態遷移ばかりが発生して，計算本体を行うための状態遷移がいつまでたっても発生しない，という状況（アンフェアな実行と呼ぶ）は起こらない」という仮定が設けられている．この仮定は，実時間システムのさまざまな性質を検証する際には必須である．しかしながら，時間匿名性を扱う際には，この仮定は必ずしも必要ない．なぜなら，仮にユーザ A に関するアンフェアな実行が存在したとしても，それに対応するようなユーザ B の（アンフェアな）実行が存在すれば，「ユーザ A とユーザ B は，アンフェアな実行までも含めた意味で，全く同じ実行をしうる（したがって，外部観測者は両者の実行を区別できず，そのシステムは時間匿名性を満たす）」という議論ができるからである．このことも，時間匿名性の検証手段として，通常の I/O-オートマトンを用いることにした，大きな理由である．

時間匿名性のモデル化は，盗聴よりも強い攻撃者を扱うシステムにおける匿名性検証に関する研究

> Y. Kawabe and H. Sakurada, “An adversary model for simulation-based anonymity proof”, IEICE Trans., volume E91-A, No. 4, pages 1112-1120, 2008.

の考え方を参考にして行った．この先行研究は，プロトコル本体のほか，盗聴よりも強い攻撃者に関する動作（攻撃部）を別途モデル化し，匿名性を検証するというものである．この検証法では，2 ステップの手続きを経て匿名性を証明する．まず第 1 段階では，プロトコル本体の（盗聴者に対する）匿名性を示す．その後，第 2 段階で，攻撃部を加えたシステムが，第 1 段階での匿名性の結果を保存することを証明する．これにより検証者は，攻撃者を考慮する，より複雑な場合の匿名性

を，より簡便に検証することができる．本研究では，この「攻撃部」を，時間をあらわすタイマー変数を保持・管理するプロセスに変更することで，時間経過の形式化を行った．その結果，先行研究と同様の，2 ステップの手続きを経るような時間匿名性の検証が可能となった．具体的には，まず第 1 段階で，プロトコルの時間制約を考えない，通信などの処理のみを考慮したシステム（制御部と呼ぶ）の匿名性を証明する．さらに第 2 段階で，その制御部の匿名性を，時間を考慮する場合にまで拡張する．以上より，時間匿名性が示される．一般に，通信などの処理と時間経過の制約を同時にモデル化・検証することは，検証者の大きな負担になると考えられる．しかし本研究の手法では，それらを分けて段階的に時間匿名性を扱うことができる．これにより，検証者は証明すべき問題の本質に注力できるようになった．

時間を考慮しない場合の匿名性検証手法としては，これまで，I/O-オートマトン理論に基づき，「フォワード型」と「バックワード型」と呼ばれる 2 種類の手法が考案されている．最後に本研究では，簡単な例に対してそれぞれの証明法を適用し，時間匿名性の段階的検証を行った．用いた例は，「ユーザ A または B が 10 ドルを支払うが，支払うユーザの手持ち金額によって，支払いまでの時間が変わる」というものである．どちらか一方のユーザが「10 ドルを支払う」のは変わらないが，支払い開始時間の違いを観測することで，どちらのユーザが支払ったかがわかってしまう．こうしたシステムの時間匿名性を保証するには，支払い時間を揃える変更を施すことが必要である．こうした事例研究を通じた記述・検証実験を通じて，フォワード型の証明手法はバックワード型に比べて補題の利用がより容易という利点があり，一方でバックワード型については，計算結果が処理の終了時まで確定しないような場合にモデルを簡素にできるという利点があることを，明らかにできた．本研究で扱った検証手法は，定理証明技術をベースとしている．そのため，原理的に，大規模なシステムを直接的に扱うことが可能である．さまざまな大規模システムに対する事例研究は，残された課題である．これについては，順次進めてゆきたい．

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　0　件）

〔学会発表〕（計　16　件）

[1] Y. Kawabe, and N. Ito, “On Computer-Assisted Verification of Timed Anonymity of Multi-Agent Systems”, Proc. of ACIS CSII 2016, 2016 年 12 月 12 日～2016 年 12 月 14 日，ラスベガス（米国）.

[2] S. Jaishy, N. Ito, and Y. Kawabe, “Problem Solving with Interactive Theorem-Proving - A Case Study”, Proc. of ACIS CSII 2016, 2016 年 12 月 12 日～2016 年 12 月 14 日，ラスベガス（米国）.

[3] S. Jaishy, Y. Fukushige, K. Iwata, N. Ito, and Y. Kawabe, “An Evaluation of BAR: Breakdown Agent Replacement algorithm for SCRAM”, Proc. of ACIS CSII 2016, 2016 年 12 月 12 日～2016 年 12 月 14 日，ラスベガス（米国）.

[4] Y. Kawabe, and N. Ito, “On Backward-Style Verification for Timed Anonymity of Security Protocols”, Proc. of 5th IEEE Global Conference on Consumer Electronics (GCCE 2016), 2016 年 10 月 11 日～2016 年 10 月 14 日, メルパルク京都（京都府）.

[5] Y. Kawabe, and N. Ito, “Proving Anonymity for Timed Systems”, Proc. of International Workshop on Informatics (IWIN 2016), 2016 年 8 月 28 日～2016 年 8 月 31 日，リガ（ラトビア）.

[6] Y. Kawabe, and N. Ito, “Toward Formal Analysis of Timed Anonymous Systems”, Proc. of 31st International Technical Conference ITC-CSCC 2016, 2016 年 7 月 10 日～2016 年 7 月 13 日，沖縄自治会館（沖縄県）.

[7] 河辺 義信，“匿名性・プライバシの定式化とシミュレーション技法による証明法”，2015 年 電子情報通信学会ソサイエティ大会（招待講演），2015 年 9 月 8 日～2015 年 9 月 11 日, 東北大学川内北キャンパス（宮城県）.

[8] 磯部 輝，伊藤 暢浩，河辺 義信，“数学入試問題に対する定理自動証明の適用の試み”，電子情報通信学会 第 28 回 回路とシステムワークショップ, 2015 年 8 月 3 日～2015 年 8 月 4 日, 淡路夢舞台国際会議場（兵庫県）.

[9] S. Jaishy, N. Ito, and Y. Kawabe, “Agent Breakdown in SCRAM”, Proc. of 2nd ACIS International Conference on Computational Science and Intelligence (CSI 2015), 2015 年 7 月 12 日～2015 年 7 月 16 日，岡山コンベンションセンター（岡山県）.

[10] Y. Kato, M. Ozaki, J. Kani, N. Ito, and Y. Kawabe, “Developing Compiler for

Nihongo Programming Language PEN”, Proc. of CSI 2015, 2015 年 7 月 12 日～2015 年 7 月 16 日, 岡山コンベンションセンター (岡山県).

[11] M. Yamamoto, K. Suzuki, R. Ogawa, N. Ito, and Y. Kawabe, “Robust Location Tracking Method for Mixed Reality Robots using a Rotation Search Method”, Proc. of 14th IEEE International Conference on Computer and Information Science (ICIS 2015), 2015 年 6 月 28 日～2015 年 7 月 1 日, ラスベガス (米国).

[12] M. Yamauchi, N. Ito, and Y. Kawabe, “Verifying Ignition Timing of Gasoline Direct Injection Engine's PCM”, Proc. of ICIS 2015, 2015 年 6 月 28 日～2015 年 7 月 1 日, ラスベガス (米国).

[13] 吉政 徳晃, 河辺 義信, “IOA に基づく実行可能仕様のための変換系の試作”, 第 12 回情報学ワークショップ (WiNF 2014), 2014 年 11 月 29 日, 静岡大学浜松キャンパス (静岡県).

[14] 岡島 侑大, 菅谷 晃宏, 河辺 義信, “センサーと無線モジュールを使ったデータ取得とデータ解析によるコースレイアウトの導出”, 人工知能学会 社会における AI 第 20 回 研究会, 2014 年 11 月 8 日～2014 年 11 月 9 日, 愛知工業大学自由ヶ丘キャンパス (愛知県).

[15] M. Yamauchi, N. Ito, and Y. Kawabe, “Toward Formal Verification of ECU for Gasoline Direct Injection Engines”, Proc. of IIAI CSI 2014, 2014 年 8 月 31 日～2014 年 9 月 4 日, 北九州国際会議場 (福岡県).

[16] 吉政 徳晃, 河辺 義信, “IOA 仕様から関数型言語 Erlang への自動変換”, 日本知能情報ファジィ学会 第 37 回東海ファジィ研究会 (蒲研 2014), 2014 年 8 月 3 日～2014 年 8 月 4 日, 蒲郡市生命の海科学館・蒲郡情報ネットワークセンター (愛知県).

〔その他〕
ホームページ等
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・教授
研究者番号：80396184

(2)研究分担者
伊藤　暢浩（ITO, Nobuhiro）
愛知工業大学・情報科学部・教授
研究者番号：40314075