様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 ２２ 日現在

機関番号：８２６３６
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５００２７

研究課題名（和文）実装性を考慮した省リソースデバイス向け暗号プロトコル設計理論の研究

研究課題名（英文）A research on design theory of cryptographic protocols for resource constraint devices with considering implementation efficiency

研究代表者

松尾　真一郎（Matsuo, Shin'ichiro）

独立行政法人情報通信研究機構・社会還元促進部門・統括

研究者番号：２０５５３９６０

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：RFIDタグやセンサーなど計算能力やメモリが制限されていて、パソコンやサーバ向けに設計された暗号化や認証のための技術が利用できないデバイスにおいても、安全な通信や認証を行うために、安全性が証明されるとともに実際のデバイスにも実装可能な軽量な暗号プロトコルを設計し実装するための研究を行った。その成果として、PUFと呼ばれる、デバイスの製造時の物理的差異を用いた暗号プロトコルを設計し、その安全性を証明するとともに、実際のデバイスにおける安全性を統計学的に示した。また、RFID用の認証プロトコルを実装する際のハードウエア実装の性能評価を行い、実用に向けた技術的な目安を示した。

研究成果の概要（英文）：In this research, we conducted researches on design and implementation of feasible and security proven light-weight cryptographic protocols for low-power devices for authentication and secure communications. This protocol will be used in the devices which do not have enough memory and computational power like PC and servers, thus the existing cryptographic protocols can not be be executed. As results of this research, we designed cryptographic protocols using PUF, which is the difference of actual devices caused by production process, and then prove the security of the protocol from statistic analysis. We also evaluated efficiency in hardware implementation of RFID authentication protocols and show the technical estimations toward practical use.

研究分野：暗号プロトコル、暗号技術、安全性評価

キーワード：暗号プロトコル　暗号技術　省リソースデバイス　暗号実装

１．研究開始当初の背景

インターネットを通じた情報通信・情報処理の高度化により,インターネットに接続されるデバイスは,一般的なPCやサーバに限らず,スマートフォンなどの携帯機器,情報家電,スマートメーター,RFID タグからの情報など,幅広い種類のデバイスに広がっている．インターネットを通じた情報通信・情報処理においては,情報の守秘,通信主体や情報そのものの認証などのセキュリティを確保する必要があるが,上述のようにインターネットに接続するデバイスが多様になっても同様の要求が存在する．

現在 IETF 等で標準化されているこれらの機能を実現するプロトコルは,一般的なPCやサーバを前提に構築されている．一方で学術的には,RFID のような計算能力やメモリの限られたデバイスでも実行可能な認証プロトコルの研究が進められ，（A.Juels and R. Pappu, “ Squealing Euros: Privacy protection in RFID-enabled banknotes ”）など,2003 年から様々な方式が提案されている．これらの研究では,主に必要な計算量が少ない共通鍵暗号やハッシュ関数を組み合わせたプロトコルとして設計することにより実現されている．しかし,これらの研究は,暗号プロトコルの安全性理論からの視点のみで設計されており,安全な共通鍵暗号やハッシュ関数が存在すると仮定した場合に,理論的に安全なプロトコルが構築可能であることを示している．つまり,現実の共通鍵暗号やハッシュ関数（例えば AES や SHA-256 など）を用いた場合に,現実の RFID タグに実装可能であるかどうかの検証はされていない．実際に,現在外部から電力供給をされるパッシブ型の RFID タグで実装可能な回路規模は 4,000 ゲート程度とされ,今後実装技術が向上したとしても,電力消費の観点から 10,000 ゲートを超えることは困難であると考えられる．このゲート数は,暗号処理だけでなくRFID タグのアプリケーション全体で必要なものであり,暗号処理に使うことが出来るゲート数は,それよりも非常に限られることになる．そのため,現実のRFIDタグの回路規模,消費電力,処理性能,安全性要件を考慮した上で,現実的な暗号プロトコルの設計と評価を行うための理論体系を構築する必要がある．本研究実施者は,これまでに RFID 向けの認証プロトコルの研究,およびハッシュ関数のハードウェア実装における評価基準策定の研究を実施している．前者の研究は,RFID 認証プロトコルの理論的安全性実現のための研究であり,後者の研究はハッシュ関数単体の実装性能評価のための研究である．省リソースデバイス向けの暗号プロトコル全体として,実装の可能性と安全性の両方を追求した研究は,これまで世界的にも例がなく,十分な知見が得られていない．

上記から,現実的な RFID なデバイスの実装状況を制約として考えながら,暗号プロトコルの観点で必要な暗号アルゴリズムの要件を,回路規模,消費電力,処理性能,安全性の 4 つの観点でバランスを取る形で追求し,暗号アルゴリズム設計理論,安全性・実装性の評価理論を構築することは,学術的に非常に価値があるテーマであると言える．

２．研究の目的

本研究の 3 年の期間内においては,以下を達成することを目標とし,実用的な省リソースデバイス向け暗号プロトコルの設計・評価に関する知見を得ることを目的とした．

(1) これまでに提案されている省リソースデバイス向け暗号プロトコルについて,暗号処理だけではなくて,デバイスとして必要とされるアプリケーション全体としての実装規模の評価を行い,実アプリケーションを考慮した際の暗号プロトコル設計のための指針を得る．

(2) (1)の指針に沿うような,暗号プロトコルの実装性と安全性の評価理論と評価手法を確立する．この評価理論は,実アプリケーションに本当に必要とされる安全性と,制約された実装規模の両方をパラメータとしたものとする．

(3) 利用する暗号アルゴリズムとして,近年開発されている軽量暗号アルゴリズムを利用した場合の,現実的な RFID タグにおける回路規模と処理速度のトレードオフを評価し,課題の洗い出しをするとともに,暗号プロトコル設計手法にフィードバックする．

３．研究の方法

本研究は,暗号プロトコルの安全性理論と暗号実装性の両方を考慮する研究であるため,前者において研究業績がある独立行政法人情報通信研究機構と,後者において研究業績がある国立大学法人電気通信大学で研究を分担する．平成 24 年度は,既存の省リソースデバイス向けの暗号プロトコルの実装規模の評価を行うとともに,評価理論の構築を行う．平成 25 年度以降は,現実の RFID タグをターゲットに,実際の軽量暗号アルゴリズムを用いた暗号プロトコルの設計と評価を行い,性能,安全性,回路規模などの実装性を考慮した設計理論を構築する．

本研究は,(1)既存の省リソースデバイス向け暗号プロトコルの実装性の評価,(2)回路規模などの実装性を考慮した安全性評価理論,評価手法の確立,(3)現実的な RFID タグを想定した暗号プロトコルの設計,(4)設計した暗号プロトコルの安全性評価,(5)性能,安全性,回路規模などトレードオフを考慮した暗号プロトコルの設計ガイドラインの構築,の 5 つのフェーズで実施する．

(1)においては,省リソースデバイス向けの

暗号プロトコルに利用可能なコンポーネントとして近年注目されている PUF（物理的複製困難関数）を用いた暗号プロトコルの評価に関する検証を進めた. PUF は,認証や暗号処理のための鍵の生成などの応用に対して個々のデバイスの物理的性質の製造上の再により生じる出力の乱数性などを用いる技術であるが,これまでに理論的に提案されている複数の PUF の実現方式に対して,FPGA に対して実装を行い,その実装性を実機で評価するとともに,安全性の評価としてその乱数性などについて実際の評価を行い,SRAM PUF を用いた認証プロトコルについてその安全性の確認と,安全な運用条件の導出を行った. また,これらの結果について,既存の RFID タグ向け認証プロトコルに応用した際の評価手法の確立を行った.

(2)においては,RFID 認証プロトコルの安全性評価理論において,近年注目されている,複数の暗号プロトコルの組み合わせの安全性も保証可能な Universal Composability（UC:汎用結合可能性）フレームワークにおける RFID タグの安全性評価モデルを改良するとともに,その他のモデルとの関係性を示した. また,PUF を使った RFID 用の認証プロトコルについて,その安全性評価モデルと評価手法を確立の確立を行った.

また,RFID タグに実装する共通鍵暗号,あるいはハッシュ関数を軽量暗号アルゴリズム１つに限定し,利用モードを処理する回路を加えることで,仮想的に複数の暗号アルゴリズムを組み合わせて安全な暗号プロトコルを想定し,このような仮想的な暗号アルゴリズムの組み合わせ方について,実装回路の実現方法を考慮して攻撃者の攻撃モデルについても検討を加え,新たな安全性の定義や,安全性評価方法についても確立した.

(3)においては,(1)において研究した PUF を利用した認証プロトコルにおいて,サイドチャネル攻撃などを用いたデバイス内の一部の秘密情報の漏洩という,現実的に流通するタグにおいて想定される攻撃を考慮した暗号プロトコルを構築した. この方式では,PUF で利用する不揮発性メモリの領域の全部が漏洩したとしても,なりすましの防止と通信データの累積によるプライバシ情報の漏洩の防止が可能となっている.

また,RFID タグに実装する共通鍵暗号,あるいはハッシュ関数を軽量暗号アルゴリズム 1 つに限定し,利用モードを処理する回路を加えることで,仮想的に複数の暗号アルゴリズムを組み合わせて安全な暗号プロトコルを設計する.

(4)としては,(3)で設計した暗号プロトコルについて,ゲーム列を利用した安全性証明手法を用いて,必要な安全性要件を満たしているどうかの証明を行った.

また,RFID が許容できる実装回路の規模を考慮し，暗号回路を無線通信機能として利用する実装方法を考案し，認証性能と安全性の評価を行った. 実験では，RFID タグとして FPGA 上に実装された AES ブロック暗号を用い,ID とチャレンジを含む入力データを暗号化処理する際に漏洩するサイドチャネル情報を，認証者がレスポンスとして解析した. 今回は，基本的なチャレンジーレスポンス認証プロトコルを用いたが，既存の暗号プロトコルに広く活用できるものである.

(5) については,(1)から(4)で得られた安全性評価に関する知見,およびプロトコル実装に関する知見をまとめるとともに,理論的なプロトコルの安全性を損なわずに動作可能なプログラムに変換可能か考察した.

４．研究成果

本研究により,以下の 5 つの研究成果を得た.

(1)PUF を用いて,暗号処理や認証に用い鍵の生成や再現を行う手法（PMKG-RT）を題材とし,この手法に既存の PUF の実現手法である Arbiter PUF と S-RAM PUF を実装し,その有効性を統計的に評価した. 実装においては,100 台の SASEBO GII を用い,統計的にも十分なサンプルを元に評価を実施した. その結果,Arbiter PUF は PMKG-RT の 仕様に合うように,任意にチャレンジのビット長を拡張できる点で優れていることが確認できた.一方，SRAM PUF は実装する際に専用の回路が必要なく,また PUF 間のレスポンス差分が大きいことより鍵 再現フェイズで第二種誤り(False Acceptance)が発生しにくいことを実験より確認できた.評価結果は,SCIS2013 において発表した（学会発表(5)）.

(2) PUF を用いたプライバシ保護付きの認証プロトコルとして,デバイス内の秘密情報が漏洩したとしても,プライバシと認証の安全性を保つ方式を確立した. この成果は,SCIS2014 おいて発表した(学会発表(4)). この方式では,PUF で利用する不揮発性メモリの領域の全部が漏洩したとしても,なりすましの防止と,通信データの累積によるプライバシ情報の漏洩の防止が可能になっている. また,この方式について,ゲーム列を利用した安全性証明手法を用いて,所期の目的通りの安全性を有していることを示した.

(3)UHF 帯無線通信を用いた RFID パッシブタグへの暗号実装を考慮し，電力や通信距離に関する既存研究の調査を行った. 現実の RFID 環境における実装に対する制約条件を明らかとするとともに，UHF 帯無線通信の業界標準である EPC Global 仕様と研究レベルで論じられているプロトコルとの整合性について明らかにした.

特に，相互認証型のプロトコルにおいて，リーダーとタグが情報を相互に交換する際に生じる時間差により，タグの電力不足が発生する可能性があるため，次のいずれかの方法で解決することが必要であることが分かっ

た．タグを実装する際に不揮発性メモリを使用する．リーダーから発する電波を工夫タグの電力不足が生じないようにする．PUF 等の新しい暗号技術を用いたプロトコルを構築する．

(4)基礎的な実験を通じて，サイドチャネル情報を用いた RFID 認証が可能であることを確認できた．研究成果は ISEC 研究会で発表した(学会発表(3))．この研究成果は,「サイドチャネル認証」という新たな研究テーマに繋がるものであり，暗号回路の実装方法だけでなく,RFID タグ全体のアーキテクチャにまで踏み込んだ実装性を議論する研究テーマを発掘することができたと考える．また,安全性・プライバシ保護のある RFID 認証プロトコルを物理的な端末に実装するため,どのような形で書く暗号学的な構成要素に落とし込み,理論的なプロトコルの安全性を損なわずに動作可能なプログラムに変換可能か考察した．回路規模の制約から耐タンパ性を有する RFID タグを想定することが現実的ではないことから,PUF を利用した RFID 認証プロトコルを構築し,マイクロコントローラーとネイティブなハードウエア実装において必要な計算時間（サイクル数）を検討した．

(5)RFID タグに対する認証プロトコルを構築する際,回路規模を考慮して共通鍵暗号系を利用した認証プロトコルに対象を絞った場合に達成できるプライバシの要件を精査し既存研究では捉えられていない安全性モデルの構築およびプロトコルの例を示した．研究成果は翌年の WISTP2013 にて発表した（学会発表(1)）．本安全性モデルを多くの RFID 認証プロトコルに適応することで,プロトコルが高い安全性を有しているかを判別することができるため今後の RFID 認証の発展に寄与したと考える．

(6)RFID タグが実際には一度に大量に処理されることを想定し,通信時の情報を基に事後に認証プロセスが動作する grouping-proof に対して暗号学的な安全性モデルを確立した．安全性のレベルは,攻撃者が正規の RFID タグになりすます攻撃と任意の通信データを改ざんする中間者攻撃の 2 つを定義し,具体的な証明可能安全なプロトコルを例示することで通信データ量や計算量にトレードオフがあることを示した．研究成果は翌年の RFID-TA2014 にて発表した（学会発表(2)）．当該分野において証明可能安全性を具体的に議論したのは初めてであり,今後の安全なプロトコル構築が期待できる．

(7)本研究において構築した安全性・プライバシ保護のある RFID 認証プロトコルを物理的な端末に実装するため,どのような形で各暗号学的な構成要素へ落とし込み,理論的なプロトコルの安全性を損なわずに動作可能なプログラムに変換できるかを考察した．
回路規模の制約から耐タンパー性を有する RFID タグを想定することが現実的でないことから,物理的複製困難関数を利用した RFID 認証プロトコルを構築し,マイクロコントローラ（MSP430）によるソフトウェア実装を想定した場合と,ネイティブなハードウェア実装を想定した場合でどの程度の計算時間（サイクル数）が必要かを検討した．

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　0 件）

〔学会発表〕（計　5 件）
(1)Daisuke Moriyama, "Provably Secure Two-Round RFID Grouping Proof Protocols", RFID-TA 2014, pp.272-276, 2014 年 9 月 9 日，タンペレ，フィンランド

(2)松原有沙，李陽，林優一，崎山一男，“サイドチャネル認証に向けた基礎的考察，” ISEC2014-10, pp.1-8, 2014 年 7 月 3 日，サンリフレ函館，北海道，函館市

(3)森山大輔，松尾真一郎，Moti Yung,“メモリ漏洩に対して安全性とプライバシを満たす PUF ベース RFID 認証プロトコル，”SCIS2014, 3B2-1, 2014 年 1 月 23 日，城山観光ホテル，鹿児島県，鹿児島市

(4)Daisuke Moriyama, Miyako Ohkubo, and Shin’ichiro Matsuo,
"A Forward Privacy Model for RFID Authentication Protocols",
WISTP 2013, pp. 98-111,2013 年 5 月 29 日，イラクリオン，ギリシャ

(5)岩井祐樹，福島崇文，森山大輔，松尾真一郎，駒野雄一，岩本貢，太田和夫，崎山一男，“巡回シフトを用いた PUF に基づくパターン照合鍵生成システムの実装評価，” SCIS 2013, 2E3-3, 2013 年 1 月 23 日，ウェスティン都ホテル京都，京都府，京都市

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0件）

〔その他〕
ホームページ等
６．研究組織
(1)研究代表者
松尾　真一郎　（MATSUO, Shin’ichiro）
独立行政法人 情報通信研究機構・社会還元促進部門・
統括
研究者番号：20553960

(2)研究分担者
森山　大輔（MORIYAMA, Daisuke）
独立行政法人 情報通信研究機構・ネットワークセキュリティ研究所セキュリティアーキテクチャ研究室・研究員
研究者番号： 10613987

崎山　一男（SAKIYAMA, Kazuo）
電気通信大学大学院・情報理工学研究科・教授
研究者番号： 80508838

(3)連携研究者