別紙１

論文の内容の要旨

論文題目	Design Methodology of Secure RFID Tag Implementation （セキュアRFIDタグチップの設計論）
学位申請者	三　上　　修　吾

RFIDタグはハードウェアリソースが限られた小型機器であり，無線通信を利用してリーダにレスポンスを送る．従来のRFIDタグのレスポンスは固定値であることから，レスポンスを収集することでRFIDタグを追跡されるというプライバシ問題がある．この問題の解決策として，暗号プリミティブを用いた認証プロトコルが提案されている．このプロトコルを実行するためには，RFIDタグに暗号プリミティブと擬似乱数生成器を実装する必要がある．そのため実装負荷が高いと考えられており，RFIDタグへの実装と性能評価はされてこなかった．

本論文では暗号プリミティブを用いた認証プロトコルを実行可能な，セキュアなRFID タグの設計，実装と性能評価を行う．セキュアなRFID タグを実現するため，(A) 認証プロトコルの実装形態の決定，(B) 暗号プリミティブの選定，(C) 擬似乱数生成手法の確立，(D) RFID システムでのシリコンチップの性能評価，に分けて取り組んだ．本論文は，全８章から構成され，その内容の要旨は以下の通りである．

第１章では，本研究の目的と成果の概要を述べた後に，本論文の全体構造を説明する．従来のRFIDタグにおけるプライバシ問題の解決策として，ハッシュ関数と擬似乱数生成器を用いた認証プロトコル(OMHSOプロトコル)を紹介する．これまでに本プロトコルの実装評価はされておらず，実現可能性は分かっていなかった．そこで本研究では，OMHSO認証プロトコルを実行可能なRFIDタグの設計，実装と評価を行う．

第２章では，RFIDタグ，RFIDタグにおけるセキュリティおよびプライバシの問題，要求される機能について述べる．従来のRFIDタグには偽タグ生成とタグ追跡という脅威が存在するため，レスポンスが毎回異なるRFIDタグ認証が求められることを説明する．

第３章では，暗号プリミティブおよびハードウェア実装性能評価項目について述

べる．これまでに提案されている軽量暗号プリミティブの仕様を述べた後，RFIDタグでは，消費電力，回路面積とクロック数が重要な評価項目であることを説明する．

第４章では，(A)RFIDタグ向けの暗号プリミティブの実装形態について述べる．認証プロトコルを実行するには，認証の度，暗号プリミティブと擬似乱数生成器を複数回動作させる必要があるため，暗号処理にかかる時間の影響は大きいと考えられる．既存研究では回路面積が小さいことが求められてきたが，RFIDタグ向けには処理時間の観点から実装形態を検討する必要がある．そこで，認証プロトコルに適した実装形態を検討し，処理時間の評価を行う．ハッシュ関数は，１ブロック入出力を行うごとにラウンド関数を繰り返し適用するが，入出力ブロック長が短く設定されているため，入出力ブロック数は多い．主な実装形態として，パラレル実装形態，シリアル実装形態とシーケンシャル実装形態がある．ハッシュ関数の処理に必要な時間は，パラレル実装形態，シリアル実装形態，シーケンシャル実装形態の順に長くなり，シーケンシャル実装形態ではパラレル実装と比較して約600倍時間がかかる．本評価結果より，ハッシュ関数にはパラレル実装形態が適していることを述べる．また，ストリーム暗号にはいずれの実装形態も適していることを述べる．

第５章では，(B)暗号プリミティブのハードウェア実装性能評価結果を述べる．既存研究で多数の暗号プリミティブが提案されており，暗号プリミティブごとに回路単体の実装性能が評価されてきた．しかし，実装性能は評価環境によって異なるため，実装性能の比較評価が困難という問題があった．そこで，暗号プリミティブのハードウェア実装と，同一の実装評価環境を用いた実装性能の評価を行った．比較評価の結果，ハッシュ関数SPONGENTは少回路面積と低消費電力を達成しており，RFIDタグに適した暗号アルゴリズムであることを述べる．

第６章では，(C)RFID向けの軽量な擬似乱数生成方法を述べる．擬似乱数を生成する一方策として擬似乱数生成器の利用が考えられるが，擬似乱数生成用の回路を別途実装する必要ある．そこで，RFID認証プロトコルで使用されるハッシュ関数で構成される軽量な擬似乱数生成手法を提案し，乱数性の評価を行う．提案手法はハッシュ関数の出力を擬似乱数列として出力する部分と，次回の入力である秘密情報の部分に分割して使用する．乱数性検証用途で広く利用されるNISTテストスイートとDichardテストスイートを用いて，提案手法の出力バイナリデータを評価した結果，すべてのテスト項目に合格した．さらにハッシュ関数と擬似乱数生成器の両方を実装する場合と比較して，回路面積を約46%に削減可能となる．評価を通して，軽量な擬似乱数生成手法を確立し，本手法の有効性を述べる．

第７章では，(D)RFIDタグチップの実装性能評価を述べる．暗号プリミティブを用いた認証プロトコルは提案されてきたが，RFIDタグへの実装と性能評価はされてこなかった．そこで，認証プロトコルを実行可能なシリコンチップを作製した．また，暗号回路がRFIDタグの実装性能に与える影響を評価するため，第５章の検討結果であるSPONGENTに加えて，比較対象として実装性能が大きく異なるNIST標準暗号のKeccakもチップに実装した．RFIDタグの実装性能評価を行った結果，通信距離10cmでRFIDタグが動作することを確認した．さらに，いずれの暗号プリミティブを利用しても，消費電力と最大通信可能距離の観点で差はないことが分かった．評価を通して，暗号プリミティブを用いた認証プロトコルは実現可能であることを実証し，RFIDタグにおいて暗号回路はボトルネックになっていないことを述べる．

第８章では，本論文で得られた知見を体系化し，結論を述べる．さらにRFID向けハードウェアセキュリティ実装技術に関する研究の展望を述べる．

別紙２

論文審査の結果の要旨

学位申請者氏名　　三上　修吾

審査委員主査　　崎山　一男

委員　　太田　和夫

委員　　吉浦　裕

委員　　石橋　孝一郎

委員　　岩本　貢

本論文は，暗号応用として，ハードウェアリソースの限られたRFIDタグ向けの暗号回路の設計，実装から性能評価までを一貫して行い，従来のRFIDタグ設計フローにはなかった暗号関連箇所の設計論を提案するものである．

第１章では，本論文の背景としてRFIDシステムの一般的な構成について述べ，RFIDタグに対する脅威を，セキュリティ面の脅威とプライバシ面の脅威に体系化している．さらにこれらの脅威への対策を，デバイス特性を利用する方式(PUF)と暗号プリミティブを用いた認証プロトコルに分類することで，対策全体の中で，暗号プリミティブを用いた対策手法であるという位置づけを明確にしている．

第２章では，既存のRFIDタグが使用する無線通信の通信帯域によって，RFIDタグを分類している．また，RFIDタグにおけるセキュリティ面及びプライバシ面での脅威を網羅的に抽出し，これらの脅威へ対応するための要件を明確化している．第１章で記載の認証プロトコル(OMHSOプロトコル)はこれらの要件を満たしており，本研究で対象とする認証プロトコルの位置づけを明確にしている．

第３章では，認証プロトコルで用いる既存の暗号プリミティブと，その実装性能評価項目を議論している．本章で述べた技術は，第５章で述べる暗号プリミティブのハードウェア実装性能評価のベースとなるものである．

第４章では，RFIDタグ向けの暗号プリミティブの実装形態を評価している．これまでRFIDタグでの利用を念頭においた処理時間の観点からの評価は報告されておらず，本論文の評価結果は１つのケーススタディとして，学術的観点のみならず，実用的観点からも有益であると考えられる．

第５章では，異なる評価環境で評価された暗号プリミティブのハードウェア実装性能を比較することは困難であることを指摘し，ハッシュ関数と擬似乱数生成器のハードウェア実装を行い，同一環境でハードウェア実装性能の比較評価を行っている．本研究では，RFIDタグでの利用を想定して設計した暗号回路のインターフェースを行いて評価しており，様々なトレードオフを考慮して暗号プリミテ

ィブを選択する上で，学術的・実用的観点の両面で価値が高いといえる．

第６章では，従来の擬似乱数生成手法では，暗号回路とは別に擬似乱数生成用の付加回路が必要なことを指摘し，ハッシュ関数で構成する軽量な擬似乱数生成方法を提案している．RFIDタグの認証プロトコルでは，短い擬似乱数列が要求されることから，ハッシュ関数の出力を擬似乱数と更新用シードとに分割して使用する工夫をすることで，付加回路の不要な軽量擬似乱数生成方式が構成可能であることを述べている．本提案手法はOMHSOプロトコルに限らず，ハッシュ関数を用いる認証プロトコルにも応用できることが期待される．

第７章では，従来の研究では，OMHSOプロトコルの実現可能性が検証されていないことを指摘し，OMHSOプロトコルの処理を実行可能なシリコンチップを作製し，実装性能を評価している．さらに，暗号回路がRFIDタグ実装性能に与える影響を評価するため，シリコンチップには，実装性能の大きく異なる2種類の暗号プリミティブを実装している．シリコンチップの実装においては，消費電力を抑えるためにデジタル処理部とアナログフロントエンド部をシングルチップで実装しており，このような実装例は今までになく，学術的・実用的観点の両面で価値が高いといえる．また，軽量暗号と標準暗号を用いる場合で，RFIDタグの消費電力と通信距離の観点で差がないという本章の議論は，標準暗号も組み込みシステムのセキュリティ向上に有用な候補であることを示した点で，将来の新たな応用研究につながる成果といえる．

第８章では，本論文で得られた知見を体系化し，結論を述べるとともに，RFIDタグのセキュアな実装技術に関する研究の展望を述べている．

以上のように，本論文はRFIDタグのセキュリティとプライバシの向上が可能な技術として期待されている，暗号を用いた認証プロトコルを対象に，暗号回路の設計，実装と評価までを一貫して実施し，RFIDタグの設計フローにおける暗号関連箇所の設計方法を提案した．本研究はOMHSOプロトコルの実現可能性を示すことに貢献するとともに，RFIDタグのセキュリティを向上させることに寄与するものである．よって，本論文は博士（工学）の学位論文として十分な価値を有するものと認める．