平成２４年度 委託研究
「軽量暗号プロトコルの省リソースデバイスに対する実装効率向上の研究開発」
研究計画書

独立行政法人
情報通信研究機構

１．研究開発課題

『軽量暗号プロトコルの省リソースデバイスに対する実装効率向上の研究開発』

２．研究開発の目的

現在、ネットワークに接続されるデバイスの種類が多様化しており、より高度なネットワーク利用への基盤が整いつつある。例えば、東日本大震災では、壊滅した情報収集基盤を他のインフラの普及に頼らないで短期に再構築することが期待され、それに際しては、配布した通信デバイスでの収集情報を、渡して良い、必要としている組織（人）に安全・確実に届ける通信網の構築の重要性がクローズアップされた。一方、中長期的には、省電力化、省資源化などのために、地産地消など流通距離、製造量、廃棄量などを抑えるための物流管理網の構築も期待されてきている。このような背景の下、モノを対象に、情報の収集や送信を安全・確実・簡単に実施できる情報収集基盤の構築を進める必要がある。この要請に応えるため、情報通信研究機構（以下、「機構」という。）の自主研究ではこれまで、RFID タグのような安価かつ広範囲で利用可能な情報デバイスでもセキュリティ確保とプライバシ保護を確立できる、軽量暗号プロトコルの研究開発を進めてきた［1］。

本研究開発では、軽量暗号プロトコルをベースとしたセキュアな情報収集基盤の構築に向け、例えば災害発生直後と一定期間経過後のように、アプリケーションや利用状況に応じて必要なプライバシ保護のレベルが異なるときに、省リソースデバイスで実行する軽量暗号プロトコルを切り替えられるような機能拡張を行った上で、軽量暗号プロトコルを利用したパッシブタグのセキュア化を可能とする１チップ搭載技術に関するフィージビリティ検証を目的とする。また、本研究開発の成果は、軽量暗号プロトコルの日本発の標準化推進に資することも目的とする。本研究開発成果に、機構の自主研究が実施するセキュリティ技術の標準化や実証実験を連携させることで、全てのネットワーク接続デバイスのライフサイクルにおける安全な情報流通、安全なネットワークの管理・運用に貢献することも視野に入れたものとする。

３．採択件数、研究開発期間及び予算

採択件数：１件

研究開発期間：契約締結日から平成 26 年度までの３年間。

予算：平成 24 年度は総額 65 百万円を上限とする。

提案の予算額の調整を行った上で採択する場合がある。

なお、平成 25 年度以降は対前年度比で 6%削減した金額を上限として提案を行うこと。

4. 研究開発の到達目標

1）アプリケーションを考慮した、普及促進に資する技術

＜前提条件＞

1 チップパッシブ RFID タグのアプリケーションによって必要なセキュリティレベルが異なることを前提に、アプリケーションや利用状況に応じて実現するプライバシ保護のレベルを切り替えることで、軽量暗号プロトコルの適用領域拡大に資する RFID タグ上の拡張機能の方式及びインターフェースであり、軽量暗号プロトコル処理部と合せてパッシブタグの１チップに搭載可能なプライバシ保護切り替えの実装方式、技術を確立すること。なお、アプリケーションのレベル、搭載機能によって、１チップに入りきらない場合は、それらに対する拡張機能を仕様変更も含めて提案すること。

＜実施要件＞

⑴アプリケーションに応じたセキュリティレベルの制御技術

- 1チップパッシブRFIDタグのセキュリティ確保を行うために、これらのタグに軽量暗号プロトコルを搭載する際のアプリケーションの検討と提案を行い、このアプリケーションに応じた効率の良いセキュリティレベル制御技術を確立すること。

⑵セキュリティレベルに応じた軽量暗号プロトコルへの普及促進に資する機能の搭載技術

- 軽量暗号プロトコルの適用領域拡大方式を支えるため、RFIDチップに搭載するプライバシ保護レベルの切り替えを実行するための機能、実装方式、プロトコル上のインターフェースを確立すること。なお、搭載機能も含め1チップに収まっていること。
- 軽量暗号プロトコルの暗号通信のセキュリティを保ちつつ、適用領域を拡大できる方式を確立すること。
- 1チップパッシブRFIDタグへの搭載における、回路規模や処理性能におけるフィージビリティ検証を行うこと。

2）１チップ実装技術

＜前提条件＞

軽量暗号プロトコルの論理設計について、暗号強度を保ちながら、実装に必要な回路規模ができるだけ小さい実装技術／方式であること。実装対象は 1 チップパッシブ RFID タグとすること。なお、アプリケーションのレベル、搭載機能によって、１チップに入りきらない場合は、それらに対する拡張機能を仕様変更も含めて提案すること。

＜実施要件＞

⑴軽量暗号プロトコルの実装技術

- 軽量暗号プロトコルの論理設計を基に、他の必須機能も含めた1チップへの搭載を可能とする軽量化実装設計技術を確立すること。
- 軽量暗号プロトコルを1チップパッシブRFIDタグに実装し、回路規模、処理性能における評価を実施し、実装技術の妥当性を確認すること。

⑵暗号化方式の選定と実装技術

- 軽量暗号プロトコルとの親和性が高く、軽量化に耐える暗号化方式を選定するとともに、1チップへの搭載を可能とする実装技術を確立すること。
- 選定した暗号化方式について、1チップパッシブRFIDタグ上における実装を行い、回路規模や処理性能における評価を実施し、実装技術の妥当性を確認すること。

注意点

（１） 本研究開発においてフィージビリティ検証を行うデバイスについては、フィージビリティに関するデータを導出するとともに、平成 27 年度の自主研究における実証実験に提供すること。

（２） 軽量暗号プロトコルの標準化と普及に資するため、研究対象となる軽量暗号プロトコルの国際標準化の推進に必要な、処理性能、実装面積などの実装におけるフィージビリティ、および優位性を示すデータを導出すること。また、本研究開発で確立した軽量暗号プロトコル仕様に関しては、機構と連携して国際標準化に資するため、実装観点での改善提案を機構の自主研究に対して行うこと。

5. 研究開発の運営管理及び評価について

研究開発に当たっては、機構の自主研究との連携を図ること。なお、平成 26 年度に終了評価を行う。

6. 参考

（１）研究課題の設定の背景及びその必要性

現在、機構の自主研究では、情報セキュリティ技術に関して、「サイバーセキュリティ」、「セキュリティアーキテクチャ」、「セキュリティ基盤」の３つの研究開発を柱に、三位一体として国民誰もが安心・安全に情報通信を行うことができるように、社会が必要とする研究開発を進めている。

特に、「セキュリティアーキテクチャ」の研究開発では、モバイル、クラウド、新世代ネットワークを含めた、セキュアネットワークの最適構成技術と設計・評価技術を確立し、安全なネットワークを提供することを目指している。この実現に向けて、圧倒的な数量となる端末側（新世代ネットワークでは数十兆の端末からの情報を想定）でもセキュリティ確保に向けた応分の責任を持つことで、より強固で安全なネットワークを構築可能とすることを目指している。その要となる暗号化プロトコル、及びその軽量実装は、必要不可欠な技術要素である。

これからのネットワーク利用環境では、端末側の装置として、センサーネットワーク、スマートメーター、交通系カード、NFC（Near Field Communication）向けチップ、そして RFID タグなど、認証や情報収集を安価かつ手軽に行う手段として、計算

能力やメモリが少ない代わりに安価で大量に組み込みや配布が可能な省リソースデバイスがより広く普及することが予想されている。省リソースデバイスは、回路規模、処理能力が大幅に制限されているため、PC などに比べてセキュリティ・プライバシ上の大きな課題が存在する。例えば、無線アンテナを通じてリーダーを用意すれば誰でも情報の取得を試みることが可能であり、取得した情報から所有している物の情報の把握や行動の追跡など、市民のプライバシ情報を取得することが可能である。また、取得された情報はクラウドに蓄積されることが想定されるが、蓄積された情報からも同様のプライバシ情報を取得することができる。そのため、最近発生したスマートフォンによる位置情報収集問題のような、省リソースデバイスからの意図しない情報収集や、蓄積された情報からのプライバシ侵害が大きな課題となりうる。例えば、2011 年 2 月に行われた NFC Congress では、NFC チップとポスターを用いてモバイル機器から情報収集を行う事例が示されている。特に、数年内に爆発的に機器数が増加することが見込まれるスマートメーターでは、プライバシ保護技術の導入が急務である。

機構では、第三期中期計画において、セキュリティアーキテクチャに関する研究として、省リソースデバイスを含めたプロトコルを開発する予定となっている。現実にシステムを構築する際には、回路規模が限られたこれらのデバイスの中で、システムに必要なアプリケーションの回路から実装されるため、プライバシ保護のための回路を実装するゲート数はさらに限定される。現在のシステムで標準的なブロック暗号である AES のためのゲート数（数 1000 ゲート）程度で省リソースデバイスにプライバシ保護機能を付加する手段として暗号プロトコルの研究が進められている。しかし、これらの研究には 2 つの課題があり実用化に至っていない。1 点は、暗号プロトコルの研究が理論的なものに留まっていることであり、もう 1 点は省リソースデバイスへの実装技術の観点で暗号プロトコルへの応用を考慮したフィージビリティスタディがなされていないことである。

本研究開発では、省リソースデバイスを用いる具体的なアプリケーションを設定した上で、FPGA 実装により現実の省リソースデバイスにおける実装性能の検証を行うとともに、現実の省リソースデバイスに対して暗号プロトコルの処理ロジックを実装することにより、現在研究されている省リソースデバイス向け暗号プロトコルの実用性と課題を明らかにするとともに、その課題を暗号プロトコル設計にフィードバックするスパイラルアップ型の研究により、より実用的な暗号プロトコルと、実装を実現することが求められる。

（2）本研究開発による省リソースデバイスにおけるセキュリティ強度向上

従来のセキュリティ確保のための暗号プロトコルは、サーバや PC、携帯端末など、ヒューマンインターフェースなどの搭載が必須のCPUを対象としており、それらCPUがセキュリティ確保の十分な情報処理能力を有していることを前提としている。一方、前述のとおり、RFID タグなどの省リソースデバイスは直接的なヒューマンインターフェースがなく、またセキュリティ機構のための計算リソースが不足しているため、セキュリティ機能の実現には限界があった。

本研究開発により、軽量暗号プロトコルの 1 チップ搭載を可能とすることで、今後ますます増大する RFID タグもセキュアなネットワーク接続が可能となることから、ネットワーク全体でのセキュリティレベルを飛躍的に向上できる可能性がある。飛躍的な向上の可能性の背景は、セキュリティが最も弱いところのセキュリティレベルが、ネットワーク全体のセキュリティレベルと等価となると考えられるため、RFID タグにおけるセキュリティ向上が、ネットワーク全体のセキュリティのベースラインを向上させることが期待できるからである。

（3）本課題と機構の自主研究の関係

「セキュリティアーキテクチャ」における機構の自主研究では、省リソースデバイスにおいて効率的にセキュリティ確保やプライバシ保護を行うための暗号プロトコルを設計するとともに、その有効性を StarBED や JGN-X などの大規模テストベッドにおけるシミュレーションを通じて検証する予定である。

一方、現実のデバイスを用いた際のフィージビリティや有効性については、その実装性に関する知見を本研究開発によって得た上で、上記シミュレーションにフィードバックしないと検証することができない。そこで、本研究開発で実証された技術を元に、これらの成果を踏まえて、機構の自主研究で軽量暗号プロトコルの国際標準化を行っていく他、ここで得られた技術をセキュアなアーキテクチャ技術や新世代ネットワークのセキュリティスライスの中に利用していくなど、本研究開発と自主研究が補完することで、セキュリティアーキテクチャ全体の実用化が促進できるものである。

具体的には、機構の自主研究では、平成 27 年度に上記テストベッドにおけるセキュリティアーキテクチャの実証実験を行う予定である。その実証実験においては、本研究開発で暗号プロトコルを実装した実際の RFID タグを、テストベッド上の機器と連携させて動作させることを予定している。そのため、本研究開発においてフィージビリティ検証を行うデバイスについては、平成 26 年度に実装を完了し、フィージビリティに関するデータを導出するとともに、平成 27 年度の自主研究における実証実験に利用可能な RFID タグを試作する必要がある。本研究開発では、この実証実験を視野に入れ、自主研究との連携が求められる。

また、本研究を実施するにあたっては、実装方式の改良を検討する際、暗号プロトコルそのものの修正が必要となる場合もあるため、必要に応じて機構が実施する軽量暗号プロトコル設計の研究開発と連携をすることが求められる。

（4）本課題と過去の委託研究課題との関係

暗号技術とその情報通信システムへの実装については、過去、「次世代ハッシュ関数の研究開発」（平成 19～21 年度）など、多くの研究テーマを委託研究として実施している。ただし、「次世代ハッシュ関数の研究開発」では一般的なハッシュ関数の研究を行っており、特定のプラットフォームへの実装に絞った研究は行っていない。それに対し、本研究で対象とする軽量暗号プロトコルでは、軽量のハッシュ関数を用いることが想定されており、過去の委託研究の成果を含めて、最近の世界的な軽量暗

号プリミティブの研究成果を活用することが期待される。

参考文献

[1] Yoshikazu Hanatani, Miyako Ohkubo, Shin'ichiro Matsuo, Kazuo Sakiyama and Kazuo Ohta: ″A Study on Computational Formal Verification for Practical Cryptographic Protocol: The Case of Synchronous RFID Authentication,″ In Proceedings of RLCPS 2011.