公開

戦略的創造研究推進事業　AIP 加速課題
研究課題「小型 IoT エッジデバイスの軽量暗号アーキテクチャ設計」

研究終了報告書

研究期間　2020年4月～2023年3月

研究代表者：原　祐子
（東京工業大学　工学院情報通信系、准教授）

§1 研究実施の概要

(1) 実施概要

Internet of Things (IoT) のエッジコンピューティングの普及に伴い、小型エッジデバイスの台数、および、センシングデータ量が増大し、それらのセキュリティ強化は重要な課題となっている。そのため、近年、アメリカ国立標準技術研究所 (National Institute of Standards and Technology; NIST) や国際標準化機構 (International Organization for Standardization; ISO) において、小型デバイスを想定した軽量暗号の標準化が進められている。本研究では、NIST/ISO 等で標準化された軽量暗号に対象に、サイドチャネル攻撃(特に電力解析攻撃)に対して堅牢な小型・低電力プロセッサ、および、最新の攻撃技術に対するセキュリティ評価プラットフォーム開発を目指し、東京工業大学の原グループ、および、電気通信大学の李グループの 2 チーム体制で研究開発を行った。

原グループ

- **軽量暗号システムのサイドチャネル攻撃への対策を施した小型プロセッサの開発**:軽量暗号システムのアルゴリズム、および、その対策手法であるマスキングをソフトウェア実装する際の主要演算に着目し、小型組込みプロセッサのための命令セットアーキテクチャの最小セットを新たに定義した。さらに、軽量暗号アルゴリズムを処理する際に発生する消費電力から秘密情報が漏洩することを防ぐため、プロセッサ中の主要モジュールに漏洩対策設計を施し、マスキングした暗号ソフトウェアを意図通りに(漏洩無く)処理できる小型プロセッサを開発した。FPGA 実機評価を行い、既存プロセッサに比べて処理性能オーバヘッドを抑えつつ、大幅な回路面積・電力削減を達成し、より高い安全性を実現できることを実証した。
- **セキュリティを考慮していないハードウェア設計ツールを活用した軽量暗号専用回路の耐タンパ設計手法の確立**: IoT 機器上で効率的な暗号処理を行うためには、プロセッサの他、専用回路を設計して搭載することも考えられる。しかしながら、現在の回路設計ツールは、回路面積やレイテンシ削減を主眼として最適化を行う結果、それらの最適化が情報漏洩の要因になっている。本研究では、回路設計ツールの内、上流設計を行える高位合成ツールに対して調査・評価した結果、特に高速化のために頻繁に使用される最適化が電力解析攻撃に対して極めて脆弱であることを明らかにした。さらに、セキュリティ未考慮の回路設計ツールを活用したまま、耐タンパ設計を行う方法を確立した。

李グループ

- **軽量暗号アルゴリズムの調査・実装**:現在、NIST で軽量暗号アルゴリズムの標準化活動が進められている。本研究で開発した上記の小型プロセッサと同等の処理性能を持つ ARM Cortex-M0 を対象に、10 個の NIST ファイナリストを定量的に評価し、特に効率良く処理できたアルゴリズムに共通した特徴を明らかにした。さらに、既に ISO 等によって標準化されているアルゴリズムの内それらの特徴を持つものを対象に、様々なマスキング手法をソフトウェア実装した。
- **電力解析攻撃における鍵復元の効率化**:攻撃側の課題として、段階的に部分鍵を復元する際、予測鍵の評価に関わる冗長な計算が攻撃の非効率さを招いていた。言い換えれば、この課題を解決することで攻撃がより一層高度化するため、耐タンパ性を設計から見直す必要がある。本研究では、復元済みの部分鍵情報を活用し、システムノイズ(他の部分鍵の影響)を抑えることで、遺伝的アルゴリズムを活用した最新研究成果の僅か 1~5%の計算量で鍵復元を可能にする、より強力な攻撃手法を構築した。
- **機械学習モデルに対するサイドチャネル攻撃手法**:これまでは暗号システムの秘密鍵がサイドチャネル攻撃の主な対象であったが、IoT と AI の発展により AI を搭載した IoT 機器への攻撃も深刻な問題になっている。本研究では、暗号システムに対するサイドチャネル攻撃手法を応用し、AI アプリケーションの主要な構成要素である活性化関数 8 種を識別する攻撃手法を開発した。さらに評価結果より、AI アプリケーション設計者がサイド

チャネル攻撃に対して有効な実装手法を提案した。

FPGA 実機評価においては、暗号システム毎の専用回路設計と比較した場合のプロセッサの柔軟性や有用性を評価できた。また、セキュリティを考慮せずに構築されてきた回路設計ツールを使って、漏洩を抑えた回路設計ができること、今後の課題を明らかにした。現在、提案プロセッサの LSI チップを試作段階であり、完成し次第、新たに構築した電力解析攻撃を適用し、最新の強力な攻撃手法に対する堅牢性を評価する。暗号システム以外のアプリケーション（AI アプリケーションなど）を処理する場合の有用性や課題も評価できると考えている。

（2）顕著な成果

＜優れた基礎研究としての成果＞

1. 軽量暗号アルゴリズム指向の小型プロセッサの最小命令セットアーキテクチャ
概要：軽量暗号を効率良く処理するための最小の命令セットアーキテクチャを定義した。現在実用化されているプロセッサは、アプリケーションの大規模・複雑化に伴い、命令セットに定義されている命令の種類は非常に多く、多くの命令を使用しない。様々な構成の暗号アルゴリズムを命令レベルで解析し、処理性能に大きな影響を与えない、最小の命令セットを定義することで、それをサポートするプロセッサの小型化に貢献できる。

2. 機械学習モデルに対する電力解析攻撃手法
概要：これまでは暗号システムの秘密鍵がサイドチャネル攻撃の主な対象であったが、IoT と AI の発展により AI を搭載した IoT 機器への攻撃も深刻な問題になっている。本研究では、暗号システムに対するサイドチャネル攻撃手法を応用し、AI アプリケーションの主要な構成要素である活性化関数 8 種を識別する攻撃手法を開発した。さらに評価結果より、AI アプリケーション設計者がサイドチャネル攻撃に対して有効な実装手法を提案した。

3. 回路設計ツールの脆弱性解析
概要：現行の回路設計ツールは、回路面積やレイテンシ削減を主眼として最適化を行う結果、それらの最適化が情報漏洩の要因になっている。本研究では、回路設計ツールの内、上流設計を行える高位合成ツールに対して調査・評価した結果、特に高速化のために頻繁に使用される最適化（ループや配列を展開して高速化する最適化）が電力解析攻撃に対して極めて脆弱であることを明らかにした。

＜科学技術イノベーションに大きく寄与する成果＞

1.小型・低消費電力・セキュアな組込みプロセッサ
概要：軽量暗号アルゴリズムとそのソフトウェアマスキング指向の最小命令セットアーキテクチャによって定義されたプロセッサを開発した。既存手法（小型プロセッサのセキュア設計）と比べて、複数の軽量暗号アルゴリズムに対して処理性能は 2~17%のオーバヘッドに抑えつつ、1/4 以下の回路面積、1/10 以下の電力消費量、より高い安全性を実現できることを実証した。

2. 電力解析攻撃における鍵復元の効率化手法
概要： 攻撃側の課題として、段階的に部分鍵を復元する際、予測鍵の評価に関わる冗長な計算が攻撃の非効率さを招いていた。言い換えれば、この課題を解決できると攻撃がより一層高度化し、システム開発者はより高度な耐タンパ設計によって対策を施す必要がある。本研究では、復元済みの部分鍵情報を活用し、システムノイズ（他の部分鍵の影響）を抑えることで、最新研究成果の僅か 1~5%の計算量で鍵復元を可能にする、より強力な攻撃手法を構築した。

3. 軽量暗号の専用回路の耐タンパ設計手法
概要：FPGA を対象とした高位合成ツールは、研究や製品開発に広く活用されるようになったが、

安全性を考慮していないため、それらのツールを使って開発した FPGA アクセラレータはサイドチャネル攻撃に対して脆弱である。本研究では通常の（安全性を考慮していない）ツールを用いて耐タンパ性向上に応用し、サイドチャネル情報の漏洩（特に消費電力に起因する情報漏洩）を抑える回路設計手法を確立した。

＜代表的な論文＞

1. Go Takatoi, Takeshi Sugawara, Kazuo Sakiyama, Yuko Hara-Azumi, and Yang Li, “The Limits of Timing Analysis and SEMA on Distinguishing Similar Activation Functions of Embedded Deep Neural Networks,” Applied Sciences, 2022.

概要：これまでは暗号システムの秘密鍵がサイドチャネル攻撃の主な対象であったが、IoTとAIの発展によりAIを搭載したIoT機器への攻撃も深刻な問題になっている。本研究では、暗号システムに対するサイドチャネル攻撃手法を応用し、AIアプリケーションの主要な構成要素である活性化関数 8 種を識別する攻撃手法を開発した。さらに評価結果より、AIアプリケーション設計者がサイドチャネル攻撃に対して有効な実装手法を提案した。

2. Saya Inagaki, Mingyu Yang, Yang Li, Kazuo Sakiyama and Yuko Hara-Azumi, "Power Side-channel Countermeasures for ARX Ciphers using High-level Synthesis," International Symposium on Field-Programmable Gate Arrays (ISFPGA), 2023.

概要：現在の回路設計ツールは、回路面積やレイテンシ削減を主眼として最適化を行う結果、それらの最適化が暗号回路設計において情報漏洩の要因になっている。本研究では、回路設計ツールの内、上流設計を行える高位合成ツールを用いて情報漏洩のない暗号回路設計を行う方法、それによって発生する回路面積や遅延のオーバヘッド、さらには漏洩の原因になっている高位合成の最適化を明らかにした。

3. Rei Kudo, Takeshi Sugawara, Kazuo Sakiyama, Yuko Hara-Azumi, and Yang Li, “Revisiting System Noise in Side-Channel Attacks: Mutual Assistant SCA vs. Genetic Algorithm,” Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 2021.

概要： 攻撃側の課題として、段階的に部分鍵を復元する際、予測鍵の評価に関わる冗長な計算が攻撃の非効率さを招いていた。言い換えれば、この課題を解決できると攻撃がより一層高度化し、システム開発者はより高度な耐タンパ設計によって対策を施す必要がある。本研究では、復元済みの部分鍵情報を活用し、システムノイズ（他の部分鍵の影響）を抑えることで、最新研究成果の僅か 1~5%の計算量で鍵復元を可能にする、より強力な攻撃手法を構築した。

§2 研究実施体制

(1)研究チームの体制について

① 原グループ
研究代表者:原　祐子(東京工業大学工学院情報通信系　准教授)
・ 軽量暗号システムのサイドチャネル攻撃への対策を施した小型プロセッサの開発
・ 現行のハードウェア設計ツールを活用した軽量暗号専用回路の耐タンパ設計手法の確立

②李グループ
主たる共同研究者:李　陽(電気通信大学大学院情報理工学研究科　准教授)
・ 軽量暗号アルゴリズムの調査・実装
・ 電力解析攻撃における鍵復元の効率化
・ 機械学習モデルに対する電力解析攻撃手法の開発

(2)国内外の研究者や産業界等との連携によるネットワーク形成の状況について

- KU ルーベンとの連携
  マスキング理論の 1 つである Threshold Implementation 考案者の Nikova 博士、および、AES 暗号の発明者の一人である Rijmen 教授と連携し、本研究におけるマスキング理論の実応用とその物理評価(電力消費からの情報漏洩)を行った。2022 年夏には電気通信大学の学生が KU ルーベンに留学し、連携強化と本研究課題の促進を行った。
- アーヘン工科大学との連携
  ハードウェア設計は重要な知的財産 (IP) であり、本研究成果も権利化を進めていく予定である。特に物理情報を狙うサイドチャネル攻撃に対する設計手法は、高度な設計技術の結集であるため、設計情報を公開する場合でも IP 保護の仕組みを導入する必要があると考えられる。ハードウェア IP の保護とその攻撃について世界的な権威の一人である Leupers 教授と共同研究を開始し、その成果を本研究に応用・活用することを検討している。2021 年秋～冬に東工大の学生が留学し、Leupers 教授の研究グループと密な研究連携基盤を構築した。
- 大阪大学との連携
  暗号回路の下流設計技術において、国内外で卓越した成果を得ている三浦教授と連携し、本研究成果の小型・低消費電力・セキュアなプロセッサの LSI 試作やその評価方法について適宜助言をいただいたと共に、共同研究の基盤を強化した。