科学研究費助成事業（基盤研究（Ｓ））公表用資料
〔令和２(2020)年度 中間評価用〕

平成３０年度採択分
令和２年３月３１日現在

暗号技術による IoT エコシステムのレジリエンス向上

Resilience Enhancement of IoT Ecosystem by Cryptographic Technologies

課題番号：18H05289

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

研究の概要（４行以内）
IoT (Internet of Things)時代のあらゆる機器は、次々と登場する攻撃の脅威に直面している。本研究では、IoT 機器の安全性状態をモニタするリーケージセンサを新たに開発し、暗号プリミティブ、暗号アルゴリズム及び暗号プロトコルの各レイヤーにおいて、たとえ、鍵の情報がリークしても、しなやかに IoT システムを正常状態に回復させるレジリエンスの向上を狙う。

研　究　分　野：情報学

キ　ー　ワ　ー　ド：情報セキュリティ、暗号理論、情報理論、ハードウェアセキュリティ、集積回路工学

１．研究開始当初の背景

IoT (Internet of Things)時代の暗号デバイスは、次々と登場する新たな物理攻撃の脅威に直面している。レーザーフォールト攻撃は、暗号回路に対する最も深刻な物理攻撃として知られているが、攻撃者の能力がさらに高くなった場合には、それを凌駕するプロービング攻撃を想定しなければならない。社会に新しい技術が普及することで、暗号技術に対する攻撃の脅威は増すばかりである。

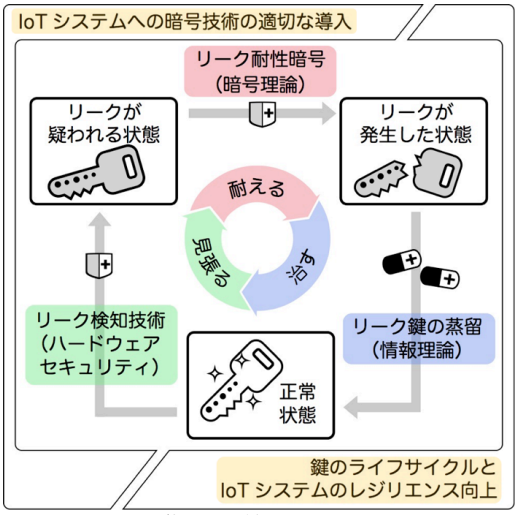
２．研究の目的

本研究の目的は、IoT デバイスへの物理攻撃によって遷移する安全性状態の循環を IoT のエコシステムの機能とみなし、システム全体のレジリエンスを向上させることにある。アナログ回路技術により IoT デバイスの暗号鍵の安全性状態を測るリーケージセンサを新たに開発し、暗号プリミティブ、暗号アルゴリズム及び暗号プロトコルの各レイヤーにおいて、たとえ、鍵のリークが生じた場合でも、しなやかに IoT システムを正常状態に回復させるレジリエンスの向上を狙う。

３．研究の方法

本研究課題を以下の２つの課題に分け、リーク耐性暗号、リーク鍵の蒸留及びリーク検知技術の３つの研究テーマを進める。

【IoT システムへの暗号技術の適切な導入】
物理攻撃対策を念頭に置いた IoT システムへの暗号技術の適切な導入である。暗号鍵が正常な状態であるかを見張るリーク検知技術と、物理攻撃に耐え、鍵のリークを防ぐリーク耐性暗号技術を構築する。



【鍵のライフサイクルと IoT システムのレジリエンス向上】鍵のライフサイクルと IoT システムのレジリエンス向上である。鍵のリークは不可避との立場を取り、リークが疑われる状態となった場合にでも、攻撃に耐えるリーク耐性暗号の拡張を検討するとともに、リークした鍵からセキュアな鍵を抽出する鍵の蒸留技術の構築に取り組む。

４．これまでの成果

リーク耐性暗号

リーケージレジリエント暗号の実現に向け、検索可能暗号を対象として研究を進めた。情報検索時に重要なフォワード安全性について、強フォワード安全性の定式化を行うとともに、従来の最も効率の良いとされていた

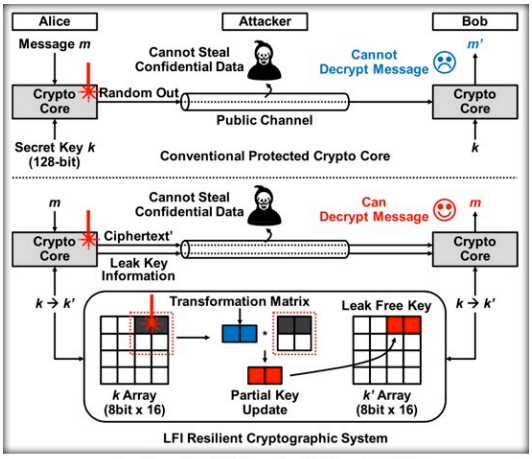
手法を本質的に改善した。暗号利用モードの研究では、機密性と改竄検知を同時に提供する認証暗号について、誤用と物理的な情報漏洩を防ぐ方式を設計した。また、サイドチャネル攻撃による情報漏洩に対する耐性を有する方式を設計した。物理的情報漏洩メカニズムの解明のための実験・評価環境を構築し、形式的モデルを理論研究にフィードバックした。プロービング攻撃における物理的情報漏洩メカニズムの理解も進んでおり、本研究の後半で研究するリーケージレジリエント回路の基本仕様を策定することができた。

リーク鍵の蒸留

リーク鍵の理解に繋がる理論的研究として、トランプのカードを用いた暗号（カードベース暗号）やキャンディーのペッツを用いたマルチーパーティ計算について研究を進め、先行研究の実装効率を上回るプロトコルを考案した。また、実践的研究では、最終目的のひとつである鍵のライフサイクルの理解に向けて、リーケージセンサと暗号鍵の情報漏洩の関係を定量的に評価することができた。暗号利用モードの安全性証明に関しては、模倣可能性と呼ばれる物理的な情報漏洩の形式的モデルについて、その簡略化を検討した。また、リークした暗号鍵の更新に必要となるリキー方式を新規に設計した。

リーク検知技術

計画を前倒しして、レーザープロービング攻撃箇所を高精度に計測するリーケージセンサを作製し、検知精度と必要センサ数のトレードオフを明らかにすることができた。さらに、このリーケージセンサを利用して漏洩のリスク下にある鍵を部分的に更新するレジリエント暗号システムの基本構成を考案することができた。本研究の後半で作製するリーケージセンサの仕様に反映することができた。物理的に複製困難なデバイス（PUF）を用いて、暗号鍵を生成する新たな手法を構築することができた。実証実験に向けて、SRAM PUF を搭載した評価基板を作製することができた。攻撃シナリオや考えうる脅威



リーケージレジリエント暗号システム[2]

に関するリスク分析を予定通り進め、プロービング攻撃対策の安全性評価に向け、理想的な攻撃耐性を有する暗号アルゴリズムのモデル化ができた。今後、あらゆる攻撃における情報漏洩の評価に利用する。

当初の研究計画にはなかった新たな展開として、ベルギーKU Leuven 大の Rijmen 教授と Nikova 博士との国際共同研究があげられる。Mask and Macs (M&M)とよばれる理論的な安全性に基づく物理攻撃耐性技術の安全性評価を共同で進めることになった。

５．今後の計画

【IoT システムへの暗号技術の適切な導入】における対策技術の実現性については、これまでに作製した評価基板を研究の中心に置き、適切な鍵の更新を考慮した暗号プロトコルの構築を進める。【鍵のライフサイクルと IoT システムのレジリエンス向上】では、レジリエンス向上に繋がる理論的な対策案を、実際の IoT システムに適用し、実証実験による安全性評価を行う。また、システムのレジリエンスを評価することで、境界領域における研究分野の創出と各分野の発展を目指す。

６．これまでの発表論文等（受賞等も含む）

[1] K. Sakiyama, T. Fujii, K. Matsuda, and N. Miura, “Flush Code Eraser: Fast Attack Response Invalidating Cryptographic Sensitive Data,” IEEE Embedded Syst. Lett., 4 pages, 2019.

[2] K. Matsuda, S. Tada, M. Nagata, Y. Komano, Y. Li, T. Sugawara, M. Iwamoto, K. Ohta, K. Sakiyama, and N. Miura, “An IC-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density,” JJAP, Volume 59, Number SGGL02, 12 pages, 2020.

[3] T. Sugawara, N. Shoji, K. Sakiyama, K. Matsuda, N. Miura, and M. Nagata, “Side-channel leakage from sensor-based countermeasures against fault injection attack,” Microelectron. J., Vol.90, pp.63-71, 2019.

[4] Y. Komano and S. Hirose, “Re-Keying Scheme Revisited: Security Model and Instantiations,” Appl. Sci., Vol.9(5), 1002, pp.1-15, 2019.

[5] Y. Abe, M. Iwamoto, and K. Ohta, “Efficient Private PEZ Protocols for Symmetric Functions,” Proc. TCC, LNCS11891, pp.372-392, 2019.

7．ホームページ等

http://sakiyama-lab.jp/study