【基盤研究（S）】

大区分Ｊ

研究課題名　暗号技術による IoT エコシステムのレジリエンス向上

電気通信大学・大学院理工学研究科・教授　崎山（さきやま）　一男（かずお）

研究課題番号：18H05289　研究者番号：80508838
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

【研究の背景・目的】【研究の背景・目的】

本研究の目的は、IoT (Internet of Things) 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。IoT 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、回路内部のデータを直接読み出すプロービング攻撃を想定しなければならない。そこで本研究では、暗号デバイスの鍵の安全性状態を測るために、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、鍵の一部がリークした場合でも、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。

【研究の方法】

取り組むべき具体的課題として、二つの課題を設定する。一つ目の課題は、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、物理攻撃による鍵のリークに耐えるリーク耐性暗号技術を構築する。

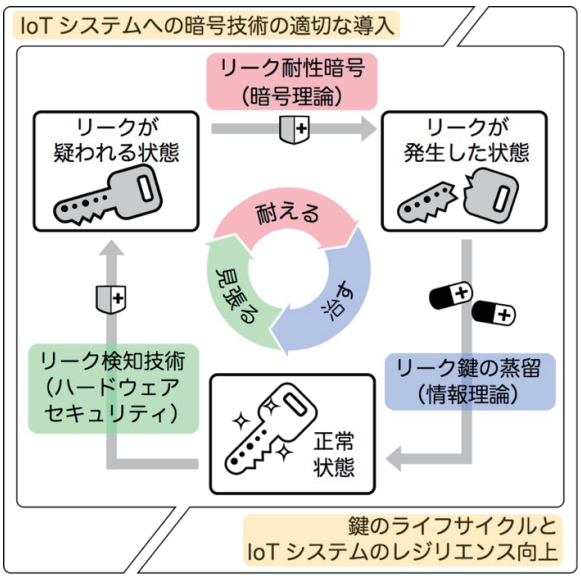

図１　暗号デバイスの安全性状態の循環と対策技術

二つ目は、鍵のライフサイクルと IoT エコ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でも、物理攻撃に耐えるリーク耐性暗号の拡張を検討し、情報の一部が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向けた研究との連携を図る。

本研究におけるコア技術は、暗号とリーケージセンサである。H31 年度に、光センサと電磁波センサを応用した最初のリーケージセンサを設計し、動作検証と安全性評価を行う。H33 年度には、リーケージセンサを搭載した暗号デバイスを開発し、リーク耐性暗号、リーク鍵の蒸留及びリーク検知技術に関する研究と協働を進める。

【期待される成果と意義】

センサと暗号技術の融合による新たな物理攻撃対策つき IoT デバイスの創生が期待できる。理論的研究では、物理パラメータを取り入れた安全性証明技法の確立や、漏れた鍵情報を排除できる情報蒸留といった発展課題につながる。実践研究と理論研究の成果を合わせることで、IoT エコシステムの一面として、鍵の安全性状態の循環が実現できると考える。

本研究で開発するリーケージセンサは、プロービング攻撃の検知を軸に、物理（もの）と数理（こと）を橋渡しする技術であり、異なる研究分野間の協働を可能にする新しい概念ともいえる。つまり、本研究課題は、物理攻撃対策に関連する学術的知識創生の源泉として機能することが期待できる。

【当該研究課題と関連の深い論文・著書】

・K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, N. Miura, “A 286F²/cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack,” ISSCC 2018: 352-354 (2018).
・K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, “Information-Theoretic Approach to Optimal Differential Fault Analysis,” IEEE Trans. Inf. Forensic Secur., 7(1): 109-120, (2012).

【研究期間と研究経費】

平成 30 年度－34 年度
149,500 千円

【ホームページ等】

http://sakiyama-lab.jp/study