シーズ技術名

IoT デバイス向け軽量暗号の耐タンパ技術

技術分野分類	情報学 計算基盤　1106 情報セキュリティ
技術キーワード	暗号・セキュリティ、認証　耐タンパー技術
産 業 分 類	G－39：情報サービス業

内容

概　要

【概要】

Internet of Things（IoT）では，様々な機器がネットワークに接続されるため，外部の攻撃の脅威から安全性を確保するために暗号技術の利用が必須である。この暗号技術について，IoT で利用される組込機器では利用可能な回路規模等に制約があるため，小回路規模・低消費電力・低レイテンシで利用可能な軽量暗号が注目されている。一方で，暗号回路動作時に生じる消費電力や電磁波などを利用して内部の秘密鍵情報を解析するサイドチャネル攻撃の脅威が報告されている。そのため，IoT 機器の安全性を確保するためにはサイドチャネル攻撃への対策を施すことが必要とされている。

本研究では，様々な軽量暗号を対象に，暗号利用時に脅威となるサイドチャネル攻撃とその対策技術（耐タンパ技術）を開発した。

従来技術・競合技術との比較（優位性）

【これまでの研究事例】

- 小回路規模実装指向の軽量暗号 Simeck に対する電力・電磁波・フォールト解析とその対策
- 低消費電力指向の軽量暗号 Midori に対する電力・電磁波・フォールト解析とその対策
- 低レイテンシー指向の軽量暗号 PRINCE に対する電力・電磁波・フォールト解析とその対策

本技術の有用性

参考論文

[1] 野崎，吉川，“軽量認証暗号 TWINE-OTR に対する 2 段階電力解析とその評価，”電子情報通信学会論文誌 D，vol.J101-D，no. 3，pp. 512-521，2018 年 3 月

[2] 野崎，竹本，池崎，吉川，“RSM をベースとした Midori128 の耐タンパ実装とその評価，”電子情報通信学会論文誌 B，vol. J106-B，no. 3，2023 年 3 月（掲載予定）

関連情報（図・表・写真等）

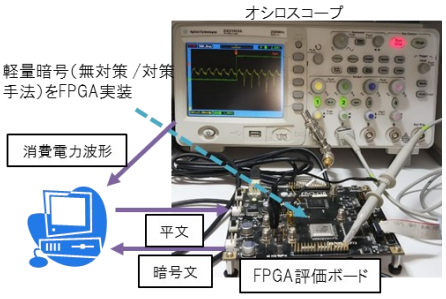

図 1　実験環境

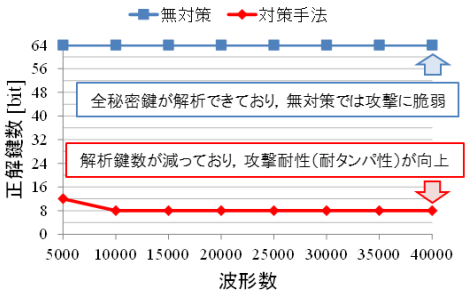

図 2　サイドチャネル攻撃に対する安全性（耐タンパ性）の評価結果

適用可能製品

技術シーズ保有者

氏名	野崎　佑典　助教
所属・役職	名城大学　情報工学部　情報工学科

技術シーズ照会先

窓口	名城大学　学術研究支援センター
TEL/FAX	TEL 052-838-2036　FAX 052-833-7200
e-mail	sangaku@ccml.meijo-u.ac.jp

■知 的 財 産

■試作品状況　無　提示可　提供可

作成日 2023 年　2 月　10 日