P-16

サイドチャネル攻撃に対する情報理論的解析

水野 弘章[*1]　田中 秀磨[*2]

アピールポイント

- 装備品の選定の際に、使用する暗号技術及び暗号プロトコルに対して適切な実装手法、達成する安全性に関する客観的な評価及び相互評価を可能とする。

研究のねらい

暗号アルゴリズムが実装された FPGA(field-programmable gate array：書き換え可能な集積回路)や LSI チップなどのモジュールは、駆動時に生ずる消費電力波形や電磁波を元に秘密鍵を暴露するサイドチャネル攻撃が知られている。対策技術は性能低下を起こす上に、その効果は実際に攻撃が成功するか否かでしか評価できないとされている。本研究では、装備品のモジュールの安全性を数値的に評価することで、利便性と安全性のバランスを確保することを目的とする。

研究内容

サイドチャネル攻撃の評価は、モジュールの駆動に伴う消費電力波形などの物理現象の観測数で論じられている。我が国の電子政府用暗号モジュールでは 10 万観測数未満で攻撃不能であれば安全と判断されている(CRYPTREC)。しかし、測定機器の性能や安全性評価の理論的根拠に乏しく、評価環境や評価時間などの物理的拘束に加え異なる対策技術間の相互評価が不能という問題もある。本研究では、シャノン-ハートレーの定理を応用し、モジュールが単位観測毎に漏洩する情報量を定量的に算出した。実際の暗号モジュールに対し実験を行い、評価手法の妥当性を確認した。

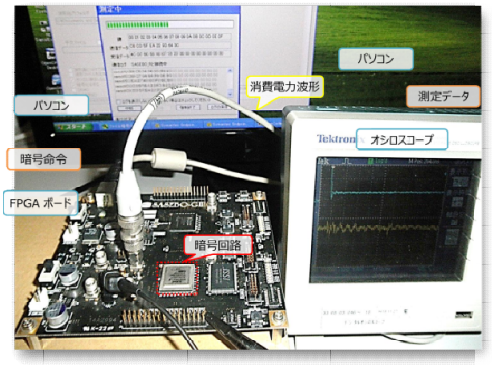

図 1 実験の様子

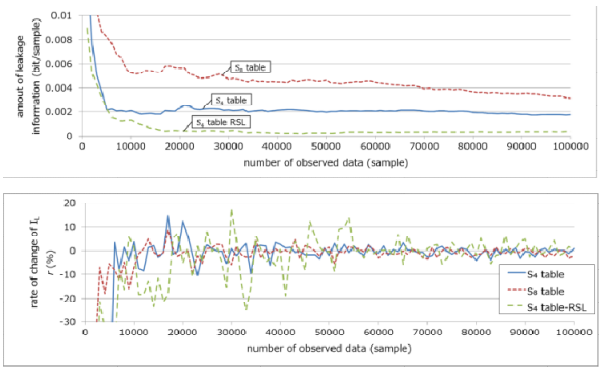

図 2 評価結果の例

[*1] 防衛大学校 理工学研究科 情報数理専攻 コンピュータ工学研究室 2 陸尉
[*2] 防衛大学校 電気情報学群 情報工学科 准教授