論 文 内 容 の 要 旨

博士論文題目

真性乱数生成器の物理攻撃に対する乱数性評価に関する研究

A Study on Randomness Evaluation for True Random Number Generators against Physical Attacks

氏　　名　　大須賀 彩希

（論文内容の要旨）

True Random Number Generator（TRNG）はランダムな物理現象を使用して乱数を生成し、この乱数によりセキュアな秘密鍵を作ることができる。オシレータを使用して乱数を生成する TRNG は、チップ上に安価に組み込めることからローエンドの機器に使用され、広く普及している。しかし、TRNG に脆弱性が生じた場合、秘密鍵の安全性が保障されなくなり、情報セキュリティに対する現実的な脅威となる。これまで、こうした TRNG に対して外乱を与えることで乱数性を低下させる攻撃が提案されてきた。一方、セキュリティで使用される乱数が満たすべき性質である、一様性・再現不可能性・予測不可能性に対して物理攻撃が与える影響については十分に議論されていない。

本研究では、オシレータをエントロピー源として使用した TRNG に対して、一様性・再現不可能性・予測不可能性に対する物理攻撃による乱数性への影響を評価した。なかでも、電気的外乱を使用した物理攻撃は暗号モジュールに対して非侵襲かつ強力な攻撃手法として知られていることから、電気的外乱が TRNG に与える影響について評価を行った。

一様性・再現不可能性の低下は、TRNG の出力の偏りや外乱による出力ビットの操作によって生ずる。このことから、TRNG に対する外乱の印加手法と印加した外乱による出力ビットの評価手法について提案した。実験により、TRNG のエントロピーを抑制する周波数を探索し、外乱を与えることで TRNG の出力ビットの一様性・再現不可能性が統計的に有意に低下することを示した。続いて、TRNG から生じる電磁放射から TRNG のエントロピーと TRNG の出力ビットを推定可能であるかについて評価を行った。これにより、出力ビットに依存した回路動作の変化を反映した電磁放射から TRNG の出力ビットを予測可能であることを示した。

以上の結果から、本研究は TRNG に対する物理攻撃による乱数性評価手法として、電気的な外乱の印加による一様性・再現不可能性への影響の評価手法、機器内部からの出力ビットを反映した情報漏えいによる予測不可能性への影響評価を提案し、電気的な外乱が TRNG に与える乱数性への影響の評価が可能であることを示した。

氏　名	大須賀　彩希

（論文審査結果の要旨）

本研究では、セキュリティの基盤技術の一つとして、秘密鍵生成等に使用される乱数を生成する真性乱数生成器（TRNG: True Random Number Generator）の中でも多種多様な情報機器で利用されているオシレータをエントロピー源として使用したTRNG に対して、一様性・再現不可能性・予測不可能性に対する物理攻撃による乱数性への影響評価を行った。

本論文の主な成果は以下に要約される。

1. 電気的外乱によるエントロピー源への影響の評価を行うために、機器外部から非侵襲に電気的外乱を与えることで、一様性を統計的有意に低下させることが可能であることを実証した。
2. エントロピー源に対して、電気的外乱は時間方向に高い分解能で影響を与えることから、TRNG の出力ビットを操作可能な外乱を一時的に与えることで一様性・再現不可能性を低下させることが可能であることを示した。
3. オシレータのエントロピー低下を評価する技術について検討を行い、振幅確率分布の測定によって、周波数領域においてもエントロピーを評価できることを示した。
4. 出力ビットに応じた回路動作の変化に着目した漏えいモデルを提案し、実験によりTRNG から放射される電磁を観測することで出力ビットを推定可能であることを示した。

以上の様に、本論文は一様性・再現不可能性・予測不可能性をハードウェアレベルで確保するための知見を与えており、堅牢なセキュリティ基盤の確立に貢献している。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。