耐タンパー評価・対策技術

佐伯　稔*

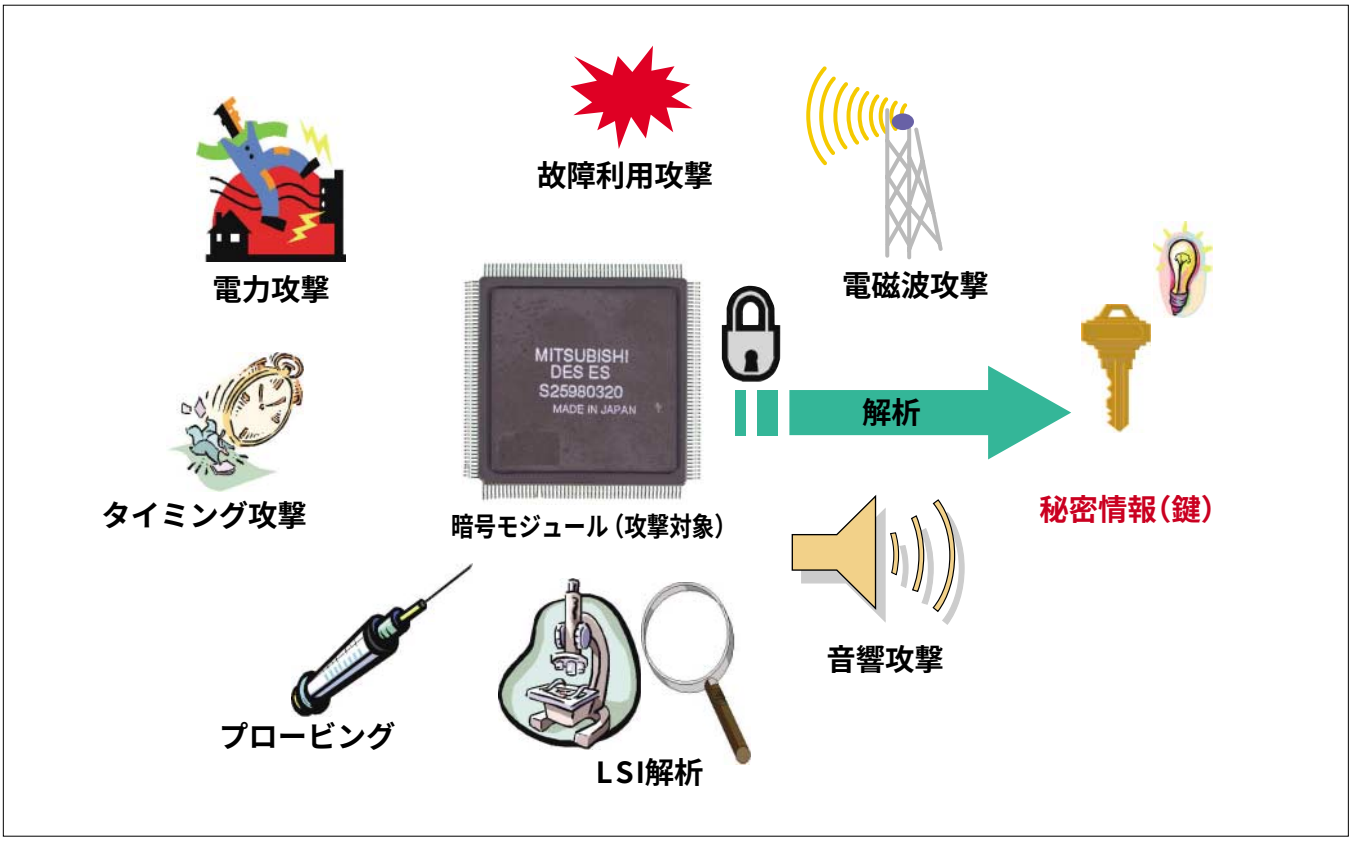
Tamper-resistance Evaluation and Countermeasure Technology

Minoru Saeki

要　旨

情報セキュリティ技術は，情報化社会を支える重要な技術であり，中でも暗号技術は最も重要な基盤技術の一つである。従来，現代暗号の安全性は主に暗号アルゴリズムの数学的(暗号学的)な安全性を根拠としており，暗号に対する攻撃(解読)も数学的な手法に基づくものが大半であった。一方，1990年代後半から，暗号アルゴリズムが実装された暗号モジュールに対する物理的・工学的な様々な攻撃法が登場し，情報セキュリティに対する新たな脅威となってきた。特に，暗号モジュールの処理時間や消費電力といったいわゆるサイドチャネル情報を解析する“サイドチャネル攻撃”と呼ばれる攻撃法は，強力な攻撃法として注目されている。暗号モジュールが，いかに数学的に安全な暗号アルゴリズムを用いても，その実装次第では，サイドチャネル攻撃によって，内部の秘密情報を簡単に解析されてしまう可能性がある。したがって，暗号モジュールには数学的な安全性だけでなく，実装面での安全性(耐タンパー性)も求められる。安全な実装を実現するためには，高度な耐タンパー評価・対策技術が不可欠である。

本稿では，サイドチャネル攻撃の中でも特に強力な攻撃法の一つである差分電力攻撃(Differential Power Analysis：DPA)を取り上げ，三菱電機が保有する評価技術や対策技術について述べる。また，暗号モジュールの耐タンパー性に関する国内の公的機関の取り組みや，国内外の標準化動向についても簡単に述べる。



暗号モジュールは様々な物理的攻撃にさらされる(イメージ)

数学的には事実上解読不能な暗号アルゴリズムを用いても，暗号モジュールの実装次第では，物理的な解析(攻撃)によって比較的簡単に解読されてしまう可能性がある。

*情報技術総合研究所