修士論文

微細素子のパラメータばらつきによる耐タンパーLSIの劣化と対策

山内 裕史

東京大学大学院 工学系研究科 電子工学専攻

学籍番号 46413

指導教官 浅田 邦博 教授

提出日 平成18年2月3日

目次

図目次

表目次

第1章

序論

1.1 研究の背景

近年、コンピュータやIT（Information Technology）技術、電子商取引の急速な発展に伴ってユビキタス時代が到来している。ユビキタスとは、人々が社会の中でその場所や存在を感じることなくコンピュータやネットワークと接しているような状況を表している言葉である。このユビキタス時代において、IT技術を安全に利用するための暗号技術、耐タンパーデバイスが非常に重要となってきている。

耐タンパーデバイスとは外部からの攻撃に対して保護対象となるデバイス内の暗号鍵などの秘密情報や秘密情報の処理メカニズムを守秘し、さらにその秘密情報の改変を困難とする性質（耐タンパー性）を実現するデバイスであり、情報セキュリティ社会を支える重要な技術となっている。

これら耐タンパーデバイスの中で代表的なものとされているのが、ICカード・スマートカードである。一般に、ICカードはIC内にデータを記憶する機能を持ったカード、スマートカードはICカードのうちで記憶機能の他に処理機能を持っているものと定義されている。これらICカード・スマートカード（以下、スマートカードで名称を統一）はキャッシュカードほどの大きさのカードの中にCPU、RAM、ROM、EEPROMなどで構成されたLSIチップが搭載されており（図1.1）、従来の磁気カードでは実現できない複雑な演算機能や判断機能、大きな記憶容量を実現している。このため、高度な暗号・認証処理を実現することができ、高度なセキュリティを実現している。これらは、社員証などの個人認証や電子マネーなどの多岐にわたる分野において実用化されており（図1.2）、今後も利用範囲が広がってくると考えられる。

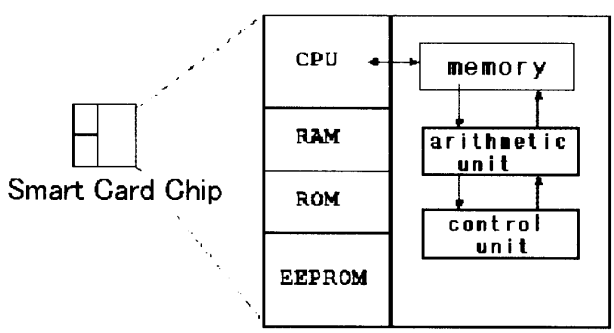

図1.1 スマートカード内のチップの概要

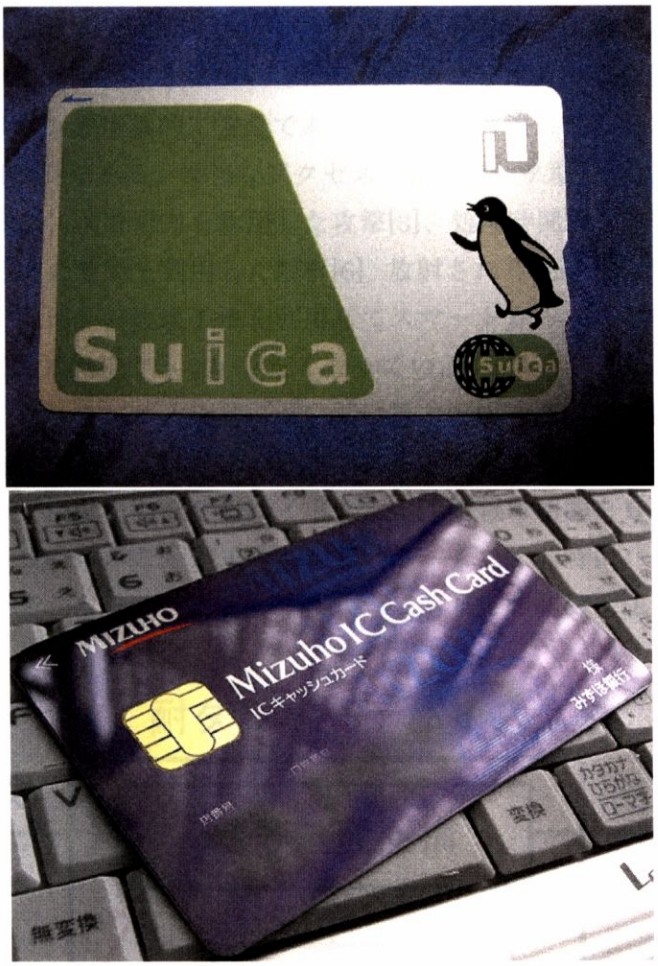

図 1.2 スマートカードの例
上：スマートカードを利用した電子マネー（Suica：JR 東日本）
下：スマートカードを利用した銀行キャッシュカード

このように、スマートカードなどの耐タンパーデバイスに対して重要性が高まってくるのと同時に、これら耐タンパーデバイスの耐タンパー性自身に対しての攻撃に対して関心が高まっている。

これらの耐タンパー性に対しての攻撃は主に耐タンパーデバイス自身を破壊して内部の秘密情報を得る破壊攻撃（Invasive attack）と耐タンパーデバイス自身には被害を与えずに秘密情報を得る非破壊攻撃（Non-invasive attack）に分類される。一般に非破壊攻撃において攻撃に用いられる消費電力や処理時間、放射される電磁波のような、設計者の予想しなかった暗号デバイス固有の付加情報を用いた解析はサイドチャネル攻撃と呼ばれている[1]。

従来は、暗号デバイスから秘密鍵などの秘密情報を取り出す攻撃手法としては、総当たりで鍵を検索したり、暗号アルゴリズムの脆弱性をつくことで強度を下げる方法がとられていた。これら従来の暗号デバイスに対しての攻撃に対しての安全性の検討としては、鍵

長の検討などといった暗号アルゴリズム自身に対しての安全性に対するものが殆どであった。しかし、サイドチャネル攻撃については暗号アルゴリズムの安全性だけでは不十分であり、暗号アルゴリズムが理論的に安全であっても実装方法によってはより短時間で秘密情報を抽出できる可能性がある。不当なアクセス・秘密データ取得手法（図 1.3）としてはプローブによる攻撃[2]、消費電力を利用した攻撃[3]、処理時間のタイミングを利用した攻撃[4][5]、意図的に与えた故障を利用した解析[6]、放射される電磁波を用いた攻撃[7]等が挙げられる。実際に、これらの攻撃手法を利用してスマートカードなどを対象とした攻撃の成功例も報告されており無視できない状況となっている。

そのため、現在の暗号デバイス設計においては電力解析・電磁界解析などのサイドチャネル攻撃に対して耐性のある設計が求められており、暗号デバイスの設計者には、暗号デバイス内の秘密情報が消費電力などのサイドチャネル情報に相関をもって現れないように注意深くデバイスを設計することが求められている。また、同時にハードウェア、ソフトウェアの両面においてこれらサイドチャネル攻撃に対しての防御手法が多数提案されている。

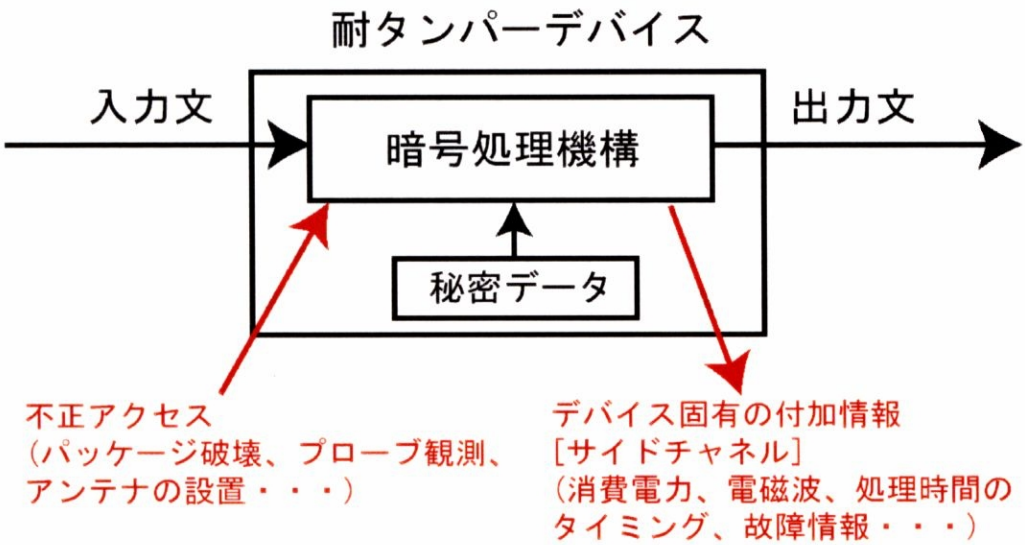

図 1.3 耐タンパー性についての攻撃

1.2 研究の目的

本研究では、これら耐タンパー性に対しての攻撃の中のうち、消費電力やデバイスから放射される電磁波を利用した解析について特に着目する。

これらの攻撃に対しての防御例としてハードウェア、特に LSI 回路のレベルからのアプローチとしては 2 線式回路などを利用した電力消費変動が発生しにくい耐タンパーLSI 回路方式が提案されている。しかし、これらの固有電力消費を図った耐タンパーLSI 回路方式についてもさらに隠された脆弱性が存在するかどうか検討する。

特に、本研究では、LSIの素子ばらつきに着目し、レイアウト的に完全に双補的に構成された固有電力消費電力回路であっても、しきい値ばらつきが電流波形、さらに外部に放射される電磁波に対して与える影響を考慮することで、ばらつきによるアンバランスが隠されたサイドチャネルとなり、LSI自身の耐タンパー性が劣化しないか検討し、解析シミュレーションを行う。さらに、十分に攻撃が行えるための解析手法の提案や攻撃に必要な素子ばらつきのレベルを調査する。また、これらの素子ばらつきを利用した解析手法に対しての防御策も検討し、提案する。

1.3 本論文の構成

本論文の構成を説明する。第2章では、電力解析と電磁界解析について説明を行い、標準1線式CMOS回路に対しての差分電磁界解析シミュレーションを行い差分電磁界解析シミュレータの有効性を示した上で解析結果を示す。さらに、差分電磁界解析への対策手法を提案し、有効性をシミュレーションによって確認する。第3章では、差分電磁界解析に耐性を持つとされる固有電力消費アーキテクチャを持ったWDDL回路に対して、素子ばらつきを考慮した上で差分電磁界解析を適応させた解析を行うことで暗号鍵の解析を行うことが可能であることを提案し、シミュレーションによって解析の有効性を確認する。第4章では、素子ばらつきを考慮した電磁界解析を行うことを防ぐための対策手法を複数提案して、シミュレーションにより有効性を確認する。第5章では、素子ばらつきを考慮した電磁界解析のシミュレーションにデバイススケーリングを適応して、今後の製造プロセスの進化と素子ばらつきを考慮した電磁界解析への脆弱性の関連を調べる。最後に第6章で結論を述べる。