組込機器のセキュリティを脅かすレーザーフォールト攻撃

菅原 健, 崎山 一男

電気通信大学(〒182-8585 東京都調布市調布ヶ丘1-5-1)

An Introduction to Laser Fault Injection Attack against Secure Embedded Devices

Takeshi SUGAWARA and Kazuo SAKIYAMA

The University of Electro-Communications, Chofugaoka 1-5-1, Chofu, Tokyo 182-8585

(Received January 10, 2019)

Fault injection attack is a serious threat to the security of embedded devices. In fault injection attacks, an adversary applies physical stress to a target embedded device, causes a computational fault, and exploits the faulty computational result to break the system's security. A laser is an effective way of applying such physical stress, and laser fault injection attacks have been scrutinized over the last decade. This paper, which explains and describes laser fault injection attacks to researchers and practitioners in the laser field, covers the following three main topics: (i) general physical attacks on embedded systems, (ii) the mechanism through which a laser injection causes a computational fault, and (iii) sensor-based countermeasures that detect an attempt of fault injection attacks.

Key Words: Laser fault injection, Hardware security, Cryptography, Countermeasure

1. はじめに

近年、あらゆるものに情報技術が応用される中で、情報セキュリティ技術の重要性がますます高まっている。その中で、暗号技術は欠かすことのできない重要な構成要素である。暗号技術の中核は、通信の秘匿を維持したり、改ざんを検知したりすることを目的とする暗号アルゴリズムである。暗号アルゴリズムが安全性を実現するためには、大前提として、鍵と呼ばれる情報が秘密に保たれることが必要である。しかし、コピーが容易なデジタルデータである鍵を安全に保管することは容易ではない。

鍵を安全に保管するための手段として、暗号モジュールと呼ばれる機器が広く利用されている。暗号モジュールとは、暗号アルゴリズムを実行するための計算機やメモリー一式からなるモジュールである。モジュール内のメモリに封入された鍵を、論理的・物理的な攻撃から防御することが、暗号モジュールの使命である。

暗号モジュールは、日常生活においてとても身近なものである。ICカード(クレジットカードやプリペイドカードなど)は、代表的な暗号モジュールである。その他に、携帯電話の利用者認証に用いるSubscriber Identity Module(SIM)カード、車のスマートキーなども、暗号モジュールである。また、近年では、インターネットに接続する機能を搭載した組込機器が続々と市場に表れてい

る。そのような機器は、通信に暗号を使用するため、暗号モジュールの1つであると言える。

暗号モジュールでは、正規利用者が攻撃者になりうる。例えば、プリペイドカードの正規利用者は、カード内に記録された残高情報を書き換えて利益を得るために、自身が所有するカードを攻撃する動機がある。正規利用者=攻撃者は、暗号モジュールを物理的に所有しているため、物理的な方法を伴う攻撃(物理攻撃)を行うことができる。暗号モジュールは、そのような物理攻撃に耐えなくてはならない。

フォールト攻撃は、物理攻撃の一種である。暗号を実装した半導体チップ(IC)に物理的なストレスを加えて計算誤りを発生させ、その結果を用いて攻撃を行う点を特徴とする¹⁾。中でも、半導体チップにレーザーを照射することで計算誤り(フォールト)を発生させるレーザーフォールト攻撃は、数あるフォールト攻撃の中でも、最も防ぐのが難しい攻撃法として知られている。

本稿は、レーザーを専門とする研究者・技術者を対象に、レーザーフォールト攻撃の基礎と研究動向を紹介する。より具体的には、(i)物理攻撃の全体的な説明、(ii)レーザー照射により計算誤りが発生するメカニズム、(iii)センサーを用いてレーザー照射を検知する対策技術について述べる。

2. 暗号モジュールの物理攻撃

2.1 物理攻撃

暗号アルゴリズムの安全性は、通常、抽象化された理想的な計算モデルの元で議論される。それに対し、電子回路技術により実現される現実の計算機は、理想的な計算モデルとは異なる挙動を見せることがある。例えば、計算内容と相関を持つ電流や電磁波を発生させたり、誤った計算をしてしまったりすることがある。物理攻撃は、そのような計算機の物理的な側面を突いた攻撃である。

物理攻撃には、大きく分けて2つのカテゴリがある。1つのカテゴリはサイドチャネル攻撃である。計算機が計算を行うと、処理するデータに応じて内部の電子回路が動作し、データに関する情報を含む過渡電流が生じる。そのような過渡電流は、計算機の消費電力や、計算機周辺に生じる電磁界として計測ができる。そのため、消費電力や電磁界を計測すると、さかのぼって、計算機内部でどのような計算が行われたかを伺い知ることができる。そのため、暗号アルゴリズムを実行する計算機の消費電力や漏洩電磁波を観察して解析すると、本来秘密にしなければならない鍵の情報を復元できることがある。そのように本来の通信チャネルとは別の物理的なチャネル(サイドチャネル)から漏えいする情報を用いる攻撃を、サイドチャネル攻撃と呼ぶ²⁾。

物理攻撃のもう1つのカテゴリは、本稿のテーマであるフォールト攻撃である。現実世界の計算機には、正常に動作する保証範囲がある。保証外の条件で計算機を動作させようとする、計算誤りを生じることがある。例えば、高温条件において計算機が誤動作すること(熱暴走)は良く知られている。逆に言えば、計算機に対して、電気・熱・光などの手段により物理的ストレスを与えると、計算誤りを意図的に発生させることができる。そのような計算誤りが生じると、正常状態では外部に露出すべきではない情報が、暗号モジュール外部に出てしまうことがある。そのような情報を用いて行う攻撃法をフォールト攻撃と呼ぶ。

2.2 学術界における物理攻撃

暗号を含む情報セキュリティの分野では、防御技術だけではなく、攻撃技術もまた研究対象である。新しい攻撃法が新しい対策法を生み、さらにその対策を破る新しい攻撃法が生むという研究サイクルが続けられている。そのようなサイクルを回すたびに、攻撃と防御の両方が高度化していく。攻撃が高度化することとは、すなわち、攻撃が成功するために必要なコスト(知識や機材)が増大する。攻撃が経済的に見合なくなるまで攻撃の難易度を上げることが、上記のサイクルの最終的な目標である。

物理攻撃も例外では無く、防御と攻撃の両面から研究がされている。物理攻撃についても、新しい攻撃と対策が生み出されてきた。特に、物理情報を用いる攻撃であることから、情報漏えいを取得する計測技術や、フォー

ルトを挿入する実験技術もまた、学術界においてオープンに議論がされている。そのような技術は、次節で述べるように、産業界における安全性評価として応用されている。

2.3 産業界における物理攻撃

物理攻撃は暗号モジュールへの現実的な脅威である。特に、ICカードにおける攻撃への脅威と対策へのニーズが、物理攻撃とその対策の発展を牽引してきた。中でも、特に高いセキュリティが求められる銀行やクレジットカード会社向けのICカードでは、物理攻撃への安全性を保証する認証(コモンクライテリア)の取得が、調達要件として課せられる。

メーカーが製品の認証を取得するには、評価機関のテストラボに製品を持ち込んで攻撃(貫通試験)を受け、それらの攻撃に耐性を持つことを確認してもらう必要がある。そのために、評価機関は、レーザー照射装置などの試験装置を持つとともに、最新の攻撃技術にキャッチアップする必要がある。

3. レーザーフォールト攻撃

3.1 レーザー照射でフォールトが生じるメカニズム

レーザー照射により、メモリに保存された1ビットのデータが1から0に書き換わるメカニズムを説明する。それは、宇宙線によってメモリが保持する値が化けてしまう現象(ソフトエラー)と同じである。

具体的な対象として、Fig. 1(a)に示すクロスカップルドインバータを例に説明する。クロスカップルドインバータは、2つのNOTゲートを環状に接続した回路である。片方のNOTゲートの出力をYと書く。この回路は、 $Y=0$ および $Y=1$ の2つの安定点を持つ。そのため、Yの値に応じて1ビットの値を保持することができる。実際、計算機中で使われるメモリ(フリップフロップおよびStatic RAM)は、クロスカップルドインバータを元に作られる。

Fig. 1(b)は、クロスカップルドインバータを構成するNOTゲートを、MOSトランジスタのレベルで記述したものである。NOTゲートは、PMOSトランジスタ M_p とNMOSトランジスタ M_n から構成する。NOTゲートの出力に応じて、いずれか一方のトランジスタのみが導通する。Fig. 1(b)は、 M_p はON(導通)、 M_n はOFF(非導通)の場合を図示している。この場合、出力Yは電源電圧 V_{DD} と接続されている。これは、Yが論理値1を表すことに対応する。

攻撃者が、NMOSトランジスタ M_n にレーザーを照射する場合を考える。その際に生じる現象を、Fig. 1(c)に示す M_n の断面図を用いて説明する。 $Y=1$ の時、N型半導体であるドレーン(n+)と、P型半導体であるP基板は逆バイアスとなり、その界面には空乏層が形成される。空乏層のシリコン原子にレーザーが当たると、原子が励起され、電子正孔対が生じる。逆バイアスがかかっているため、電子と正孔は、PN接合の異なる極に引き寄せら

Fig. 1 Mechanism of a laser-induced bit-flip in a cross-coupled inverter.

れる。その結果、PN接合に光電流が生じる。そのようにして、本来は非導通であるはずのNMOSトランジスタ M_N が導通する。

レーザー照射によって生じる光電流が、クロスカップルドインバータに与える影響を説明する。レーザー照射によって生じる光電流は、Fig. 1(b)に示すように電流源でモデル化できる。今、 M_P が導通状態であるため、電流源は電源電圧とグランドをショートする。その結果、NOTゲートの出力 Y の電圧が低下する。もし出力電圧が、しきい値電圧を下回ると、クロスカップルドインバータはもう1つの安定状態に遷移する。すなわち、 $Y=0$ となり、その状態で安定する。これは、メモリに保存された値が1から0に化けたことを表している。

3.2 フォールトを用いた攻撃

前節で述べた方法を用いると、攻撃者は、ある狙った1ビットの値を書き換えることができる。たった1ビットのデータ改変であっても、深刻なセキュリティ上の問題を生じる可能性がある。たとえば、あるデータにアクセスできるかどうかを司る情報(アクセスフラグ)は、メモリ上では1ビットの情報として記録される。そのため、ビットが反転すると、本来想定されていなかった情報へのアクセスが可能になる可能性がある。

フラグではなく、演算中の中間データが書き換わった場合も、攻撃につながる可能性がある。暗号演算の中間値の1ビットが反転してしまった場合を考える。暗号を実装した計算機はそのことに気づかず、誤ったまま計算を続け、誤った値を出力する。そのような誤った出力値を用いて、1ビット誤りがどのように伝搬したか逆算することで、演算で用いた秘密鍵を復元する暗号解読法が知られている。

さらに、フォールトにより、メモリに格納されたプログラムが書き換わってしまう可能性もある。その場合、実行すべき命令や、プログラムの実行フローが変わってしまう。それもまた、データが書き換わった時と同様に、アクセス違反などのセキュリティ上の問題を引き起

こす可能性がある。

3.3 レーザーフォールトに用いられる装置

2.3節で述べた通り、評価機関は、暗号モジュールがレーザーフォールト攻撃に対して安全であるかどうかを試験するための能力を持っている。そのために、レーザーフォールト攻撃の評価を目的としたレーザー装置が販売されている^{†1,†2}。以下では、レーザーフォールト攻撃にかかる重要なパラメータについて述べる。

波長: チップの表面と裏面のどちらから照射するかによって、レーザーの波長を決める。ICの表面から照射する時は、可視光レーザーを用いることが一般的である。表面に照射したレーザーは、シリコン基板に到達するまでに、チップの上層を占める金属配線層により反射・回折される。それにより表面からの照射が困難な時は、シリコン基板の裏面にレーザーを照射する。その場合は、シリコン基板を透過する近赤外光(例: 1064 nm^{†1})が用いられる。

時間分解能: レーザー照射の対象になるメモリなどのデータは絶えず更新されている。そのため、特定の間値へフォールトを挿入することを望む攻撃者は、ある特定のクロック周期の間にフォールト挿入を完了しなくてはならない。そのため、対象のクロック周期(10 ns~100 ns)の間に、その周期よりも短いレーザーパルス照射する必要がある。さらに高度な攻撃では、異なるクロック周期に、連続してレーザーパルスを照射することが求められることがある(タイミングダブルレーザー)。そのためには、繰り返し時間(Repetition Rate)が短いレーザーを用いる必要がある。

空間分解能: 3.1節で述べたように、攻撃者は、小領域に対し選択的にレーザー照射を行う。そのために、光学顕微鏡による集光を行うことが一般的である。また、照射位置を網羅的にスキャンして問題が無いか試験をする

^{†1} Riscure, "Laser Station 2: A Security Test Tool for Laser Attacks on Smartcards," <https://www.riscure.com>

^{†2} ALPhANOV, "Laser solutions for IC evaluation", <http://www.alphanov.com>

ために、プログラム制御ができるXYZステージが必要である。そのため、レーザー・光学顕微鏡・ステージからなるレーザー・ステーションがよく用いられる^{1,2}。さらに高度な攻撃では、2箇所以上の座標に同時にレーザーを照射することが求められる(空間ダブルレーザー)。そのために、顕微鏡に加えて、レーザーを導くための光ファイバを備えたレーザー・ステーションも存在する。

4. レーザーフォールトにおけるトピックス

4.1 チップの微細化と空間分解能

脅威の程度を見積もったり、攻撃者の能力に合わせた効率的な対策を行ったりするには、攻撃者がどこまで精密に攻撃を行うかを知る必要がある。3.1節で述べたように、攻撃者が行う攻撃の正確さは、レーザー照射の空間分解能により決まる。そのため、半導体技術の進展により、トランジスタのサイズが微細化すると、特定のトランジスタを狙い撃ちするような攻撃は難しくなっていくと考えられている。そのため、どこまで微細なチップに対してレーザーフォールトが可能かということは、重要な研究上の問いである。そこで、研究者達が競って実験を行っている。

著者が知る最新の成果は、Dutertreらによる28 nm CMOSテクノロジーで製造された専用回路(Application Specific Integrated Circuit: ASIC)への攻撃例である³。半導体はさらなる微細化を続けているものの、暗号モジュールを始めとする組込機器では、28 nm以上より大きい半導体製造技術によるチップが、10年以上は利用され続けると考えられる。そのため、少なくともしばらくの間は、トランジスタ1個を狙い撃ちにするようなレーザーフォールト攻撃を想定して暗号モジュールを設計する必要がある。

4.2 対策法

フォールト攻撃対策の基本的なことは、フォールトを検知することである。検知後に暗号モジュールを停止・リセットすることで、フォールトに由来する攻撃を防ぐことができる。特に、フォールトを誘発する物理現象を、センサで検出することは、フォールト攻撃への有効な対策法である。電圧や温度の変化によるフォールト挿入に対しては、電圧センサや温度センサを用いることができる。

レーザーフォールトを検出するためのセンサとして、従来は光センサ(フォトディテクタ)を用いる方法が知られている⁴。しかし、光センサは、受光面に当たった光しか検出することができない。そのため、カバレッジを向上させるためには、受光面を増やすしかないため、高コストである点が問題となる。

以上の背景より、レーザー照射を検出する別の方式として、レーザー照射に伴って二次的に生じる電気現象を検出するセンサが注目を集め、活発に研究がされている。3.1節で述べたように、レーザー照射は、短期的なショートを生じる。そのようなショートに伴う電気現象

は、グラウンドなどを介してチップ中を容易に伝搬するため、センサ辺りのカバー範囲を広げることができる。

ショートを検出するセンサとして有名なものに、NetoらによるBulk Built-In Current Sensor (BBICS)がある⁵。ショートが生じると、通常ではほとんど電流が流れない経路(P基板およびNウェル)に大きな電流が生じる(Fig. 2を参照)。BBICSは、そのような電流を検出することを目的とした、トランジスタ埋込み型の電流計である。BBICSそのものの改良だけではなく、システム化やチューニングについても研究が進められている。著者らも、分散配置したBBICSと、検出時に電源を遮断する回路をシステム化したアーキテクチャを提案している⁶。

4.3 さらに新しい攻撃

機能の追加は、新しい攻撃につながる副作用を持つことがある。著者らは、4.3節で述べた対策法にそのような問題が無いかを調べ、実際に新しい攻撃が存在することを発見した⁷。これは、2.2節で述べた、防御と攻撃の研究サイクルにより技術を洗練させる事例となっている。

3.1節では、クロスカップルドインバータを対象に、レーザー照射によりフォールトが生じるメカニズムを説明した。より具体的には、Fig. 1(b)において、 $Y=0$ の時にレーザーを照射すると、ビット反転が生じると述べた。その時は考慮しなかったもう1つの場合、すなわち $Y=1$ の時にレーザーを照射すると何が起きるだろうか? 実は何も起きないのである。 $Y=1$ の時、トランジスタ M_N はすでに導通状態であるため、たとえレーザー照射によって電子正孔対が生じたとしても、即座に再結合して消滅するのである。よって、 M_N にレーザーを照射してセンサが反応するのは、 $Y=0$ の時に限られる。

以上の性質を利用すると、メモリ内のデータを不正に読み取る攻撃ができる。攻撃者はトランジスタ M_N にレーザーを照射する。もしセンサが反応したら、攻撃者は $Y=0$ であると知ることができる。一方、もしセンサが反応しなかったら、攻撃者は $Y=1$ であると知ることができる。以上のようにして、攻撃者は、本来は知られてはいけなはずの Y の値を入手することができる。そのような1ビットの値の漏洩は、暗号解読などの攻撃に直結する。この攻撃は、 Y の値に応じて、センサの反応

Fig. 2 Detection of laser-induced current using bulk built-in current sensors

の有無が変化するために起こる。その性質は、ショートに由来する電気現象を検知するというセンシング方式に由来する根本的なものである。

以上の攻撃は、どうやったら防げるだろうか?この攻撃は、手段としてレーザーを照射するものの、フォールトそのものを利用するのでは無く、フォールトの有無から得られる1ビットの情報漏えいを利用する。そのため、2.1節で述べたサイドチャネル攻撃に近い性質を持っている。そのため、サイドチャネル攻撃への対策法により防ぐことができる⁸⁾。すなわち、その弱点をサイドチャネル攻撃への対策法を用いて補うことで、4.2節で述べた効率的なレーザーフォールト攻撃対策法を利用することができるようになる。

5. まとめとその他の話題

本稿では、レーザーフォールト攻撃の基礎と研究動向を紹介した。レーザーフォールト攻撃は、暗号実装の研究コミュニティを中心に研究が進められてきた。しかし、本研究課題のより深い理解と、それに基づく対策法の開発には、レーザーを専門とする研究コミュニティの知見が必要になると考えられる。本稿が、これまで希薄であった両コミュニティをつなぐ助けになれば幸いである。

本稿は、特にレーザーフォールト攻撃と、それを検出するセンサーによる対策について述べた。それに限らず、レーザーを用いた計測・通信技術にかかる物理セキュリティは、近年注目を集めている非常に重要な研究課題である。特に、自動運転などで必須となるレーザーを用いた測距技術(LiDARなど)において、誤った計測値を意図的に挿入するような攻撃の脅威が指摘されている^{9,10)}。また、脅威に対抗するための対策法として、特殊なレーザー変調技術が提案されている^{10,11)}。それらの課題についても、今後の研究の発展が期待される。

謝 辞

本論文の一部は、科研費JP18K18047およびJP18H05289の助成を受けた。また、本論文で述べた内容は、文献6), 7)において、永田 真, 三浦 典之, 松田 航平(神戸大学), 林 優一(奈良先端科学技術大学院大学), 藤井 達哉, 庄司 奈津(電気通信大学)らと共同で行った研究に基づく。

参考文献

- 1) M. Joye and M. Tunstall: *Fault Analysis in Cryptography* (Springer-Verlag, Berlin, 2012).
- 2) S. Mangard, E. Oswald, and T. Popp: *Power Analysis Attacks - Revealing the Secrets of Smart Card* (Springer-Verlag, Berlin, 2007).
- 3) J.-M. Dutertre, V. Beroulle, P. Candelier, S. De Castro, L.-B. Faber, M.-L. Flottes, P. Gendrier, D. Hely, R. Leveugle, P. Maistri, G. Di Natale, A. Papadimitriou, and B. Rouzeyre: *Proc. 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography* (2018) p. 1.
- 4) Renesas Technology Corporation: *IC Card System Using Photo-Detectors for Protection* (US Patent US7042752, 2003).
- 5) E. H. Neto, I. Ribeiro, M. G. Vieira, G. I. Wirth, and F. L. Kastensmidt: *IEEE Micro* **26** (2006) 10.
- 6) K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, and N. Miura: *IEEE J. Solid-State Circuits* **53** (2018) 3174.
- 7) T. Sugawara, N. Shoji, K. Sakiyama, K. Matsuda, N. Miura, and M. Nagata: *Proc. 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography* (2017) p. 49.
- 8) Y. Ishai, A. Sahai, and D. A. Wagner: *Proc. CRYPTO 2003* (Lecture Notes in Computer Science **2719** (2003), Springer-Verlag, Berlin) p. 463.
- 9) 中澤 祐希, 中野 将志, 汐崎 充, 久保田 貴也, 白畑 正芳, 藤野 毅, 菅原 健, 鈴木 大輔, 小林 信博: 2016年暗号と情報セキュリティシンポジウム予稿集4F1-1.
- 10) H. Shin, D. Kim, Y. Kwon, and Y. Kim: *Proc. Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science **10529** (2017), Springer-Verlag, Berlin) p. 445.
- 11) R. Matsumura, T. Sugawara, and K. Sakiyama: *Proc. 6th International Symposium on Computing and Networking Workshops* (2018) p. 479.