計測自動制御学会東北支部 第249回研究集会
資料番号 249-4

情報機器からの漏洩電磁界に関する基礎的計測

Fundamental Measurement of Electromagnetic Field radiated from Information Devices

○大村孔平*, 林優一*, 水木敬明*, 曽根秀昭*
○Kouhei OHMURA*, Yu-ichi HAYASHI*, Takaaki MIZUKI*, Hideaki SONE*

*東北大学(Tohoku University)

キーワード: サイドチャネル攻撃(Side Channel Attack), 放射電磁界(EM Radiation)

連絡先:
〒980-8578 仙台市青葉区荒巻字青葉 6-3 東北大学サイバーサイエンスセンター曽根・水木研究室
大村孔平, Tel.:022-795-6094, E-Mail: a5tb2048@cs.he.tohoku.ac.jp

1. はじめに

1.1. 研究の背景

動作中の情報機器から外部に電磁界が漏洩するという問題があり、このような漏洩電磁界は周囲の機器の動作に影響を与えるだけではなく、機器外部に情報が漏れる原因となることが知られている[1]。例えば、暗号文の復号化処理を行っている機器から放射される電磁界には機器に実装された暗号モジュールの消費電力に関する情報が含まれており、これらの消費電力波形を取得・解析することで、第三者が復号鍵などの秘密情報を得ることが可能である。これはサイドチャネル攻撃と呼ばれ、近年注目されている情報機器に対する攻撃手法の一種である。

これまでサイドチャネル攻撃について行われた研究では、取得した消費電力波形から秘密情報を得る方法について議論されることが多かった。一方で、最近では秘密情報の伝搬メカニズムや伝搬範囲について議論がなされており[2][3]、サイドチャネル攻撃がより現実的な問題になってきている。こうした状況において、情報機器にサイドチャネル攻撃に対する対策を施すことが急務である。

暗号機器から漏れる消費電力波形の取得性に注目した過去の研究[3]において、暗号基板に実装されたモジュールの消費電力情報が基板および基板に接続された線路に伝搬するというメカニズムが述べられており、線路から放射される電磁波を観測することで実際にサイドチャネル攻撃が実行可能であることが示されている。また電源線だけでなく、基板に接続されたさまざまな線路に秘密情報が伝搬する可能性が示唆されている。

実際の情報機器の基板には電源線のほか USB ケーブル、LAN ケーブル、機器内部の配線など多くの異なるインピーダンスの線路が接続されており、上で述べたような秘密情報の伝搬についてもこのような状況の下で議論する必要がある。

本論文では、情報機器に接続された線路が秘密情報の伝搬に与える影響を調べるために、線路の長さ、本数および線路が 2 本の場合の取り付け間隔をパラメタとし、さまざまなパターンで基板に短絡線路を接続した場合について基礎的な実験を行う。また、得られた結果から情報機器に線路を接続する際の指針を与えることを目標とする。

1.2. RSA 暗号に対する単純電力解析攻撃

p を平文、c を暗号文、暗号鍵と復号鍵をそれぞれ e、d とすると、RSA 暗号における暗号化・復号化の処理は以下の式(1)で表される。

$$c = p^e \bmod n$$
$$p = c^d \bmod n \quad \cdots\cdots \quad (1)$$

一般に冪乗算は乗算と自乗算の組み合わせで実行される。すなわち、e (および d)の左側から 1 ビットずつを参照し、1 であれば自乗算と乗算を、0 であれば自乗算をそれぞれ行うという処理を繰り返す(図 1)。

$$49^{13} \bmod 10 = 49^{1101_{(2)}} \bmod 10$$
$$((49^2 \times 49)^2)^2 \times 49 \bmod 10$$

図 1:冪乗演算の実装

乗算と自乗算では演算に要する電力が異なり、オシロスコープを用いて消費電力波形を観測すれば演算内容の違いを肉眼で確認することができる。このように、消費電力の変化を直接解析に用いる方法を単純電力解析(SPA: Simple Power Analysis)と呼ぶ[4]。図 2 に示すような波形が取得できれば RSA 暗号の復号鍵を推定することが可能であると言える。

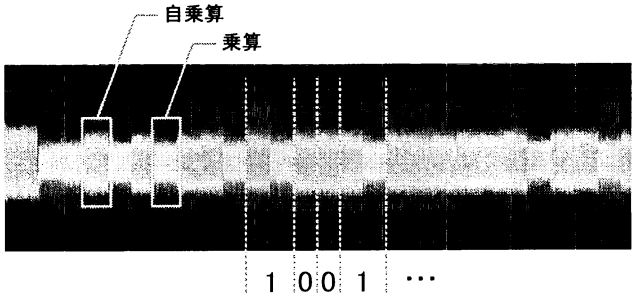
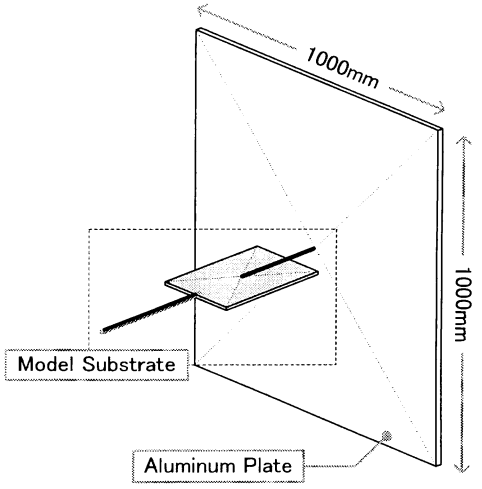


図 2:SPA 波形からの復号鍵推定の例

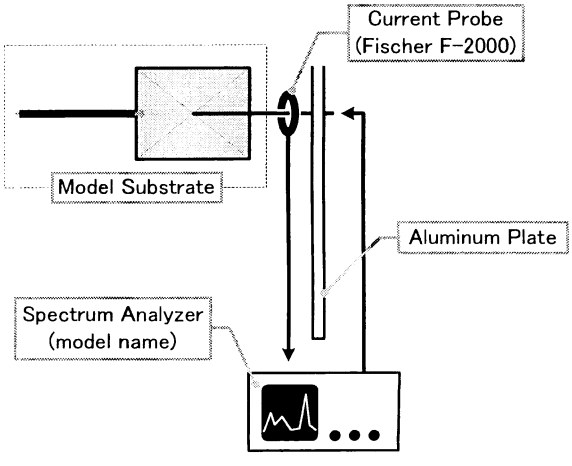
上述したような攻撃に対しては、論理面からの対策(たとえば RSA の場合、自乗算と乗算の消費電力が同じになるようダミーの演算を行うようにするなど)のほか、演算内容に関する情報が機器外部に伝搬しにくくなるように、機器の物理的設計の面からも対策を行う必要がある。近年 SPA 以外にも情報機器の消費電力を利用したさまざまな攻撃手法が提案されており、特に後者は暗号アルゴリズムに依存せず比較的広く用いることのできる対策手法として重要であると考えられる。

2. 実験環境

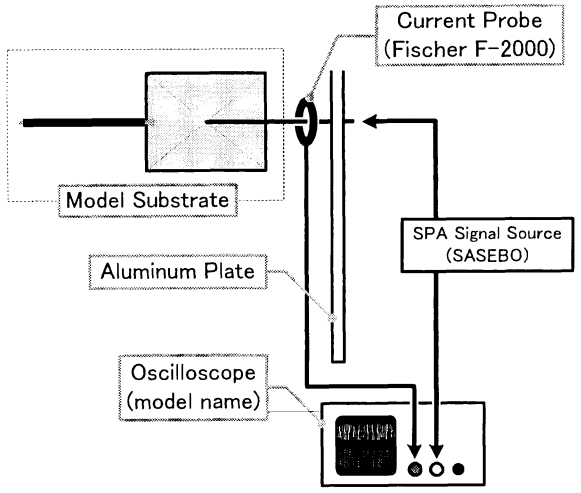
本実験の環境および用いたモデルの構造を図 3、図 4 に示す。



(a) モデル基板およびアルミ板の配置



(b) 周波数特性の測定環境



(c) SPA 波形の観測環境

図 3:実験環境

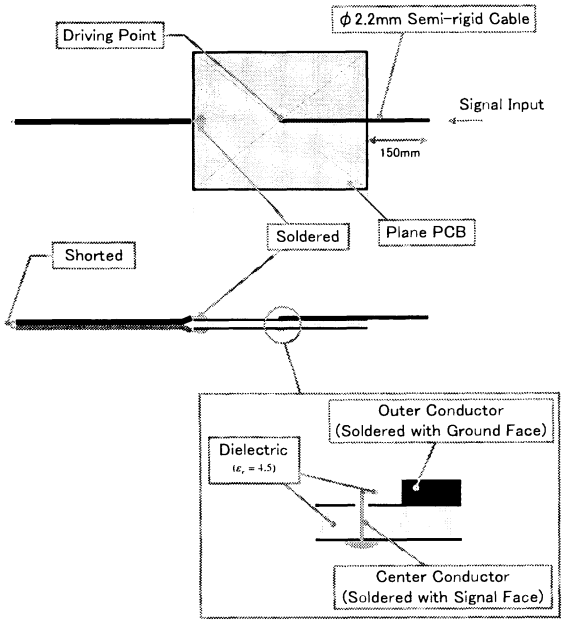


図 4:実験で用いたモデル基板の構造

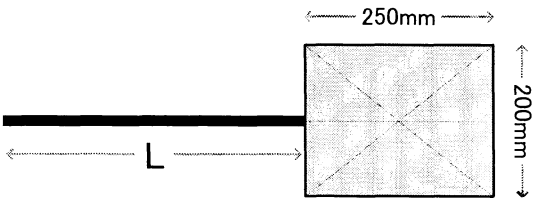
1 章で述べたとおり、情報基板上のモジュールが動作する際に生じる過渡電流が励振源となり、基板および基板に接続された線路に秘密情報を含むコモンモード電流が分布するというメカニズムが示されている。この現象をモデル化するために、本実験では励振源をもつ基板をモデル化した。本研究では基板に取り付ける線路の影響に焦点を置いており、基板上に実装される回路素子による影響をなくすために、素子が実装されていない基板(250mm*200mm*1.5mm)をモデル基板として用いた。用いた基板の導体間の比誘電率は $\varepsilon_r = 4.5$ である。基板に対する励振は、基板中心に接続されたセミリジッドケーブルを通して行った。使用したセミリジッドケーブルは外径 2.2mm、導体間の比誘電率は $\varepsilon_r = 4.5$ である。実験では、はじめに各モデル基板を 1V で励振し、その際に基板上および接続された線路から放射される電磁波の周波数特性を測定した。更に、RSA の暗号化処理を実行中のサイドチャネル標準評価ボード(SASEBO: Side-channel Attack Standard Evaluation BOard)で生じた過渡電流を各モデル基板の励振源として用い、この際線路から放射される電磁波を測定することで実際に SPA 波形を取得して比較した。モデル基板はそれぞれ基板に接続された線路の長さ、本数および取り付け間隔をパラメタとして変化させた。なお、ここで、アルミ板は測定系と被測定系を電磁的に分離するために用いた。

いずれの実験においても、放射電磁界強度の測定はアルミ板から75mmのセミリジッドケーブル上においてクランプ型電流プローブ(Fischer F-2000)を用いて行った。

3. 実験

3.1. 線路の長さによる影響の評価

まず、モデル基板に接続する線路の長さを250mm、500mm、1000mmに変化させ(図5)、各々の場合において線路から放射される電磁波の周波数特性を測定した。



L = 125mm, 250mm, 500mm, 1000mm

図 5:線路の長さによる影響を調べるためのモデル

実験の結果は図6の通りである。いずれのモデルにおいても、5～11MHz 付近にピークが現れた。接続する線路が長くなるにしたがってこれらのピークが左方向に推移していくことがわかる。

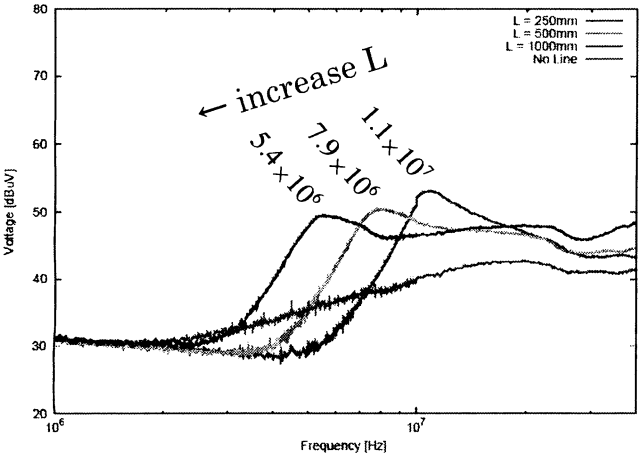
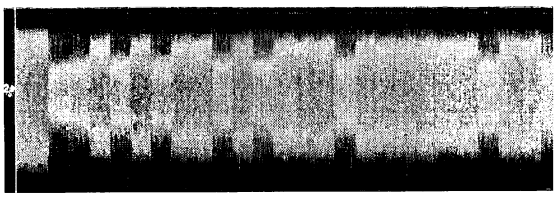


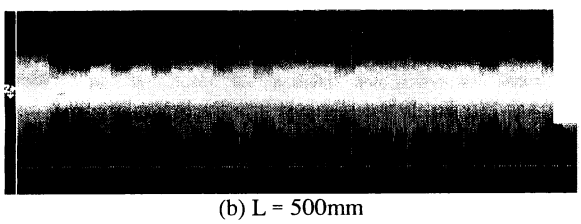
図 6:線路の長さを変化させた場合の周波数特性

ここで、ある周波数において周波数特性が高くなるということは、その周波数の電磁波が強く放射されていることを示している。たとえば図 6(a)の L=250mm の結果を見た場合、1.1×10^7 Hz (=11MHz)付近の電磁波が他の周波数成分と比較して強く放射されていることを示している。

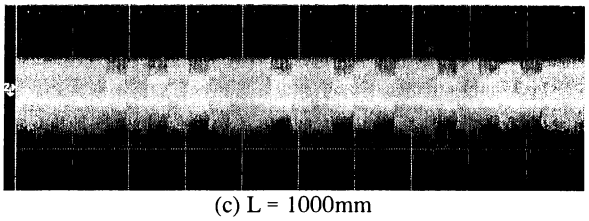
各モデルを用いて取得した SPA 波形を図 7 に示す。接続する線路の長さの変化に伴い、SPA 波の見え方が変化していることがわかる。なお、SPA 波形は 25MHz 以上の領域を遮断して観測した



(a) L = 250mm



(b) L = 500mm

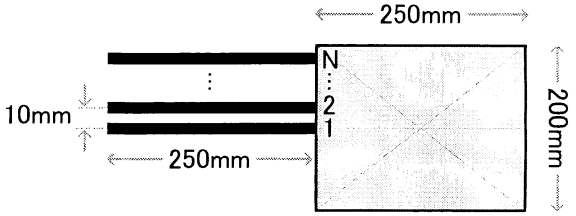


(c) L = 1000mm

図 7: 線路の長さを変化させた場合の SPA 波形

3.2. 線路の本数による影響の評価

次に、基板に取り付ける線路の本数を 1 本から 4 本まで変化させ(図 8)、線路から放射される電磁波の周波数特性を測定した。



N = 1, 2, 3, 4

図 8:線路の本数による影響を調べるためのモデル

結果は図 9 の通りである。線路の長さを変化させた場合と同様に、11～22MHz 付近にピークが現れた。これらのピークは取り付ける線路の本数を増やすほど右方向に推移していくことがわかる。

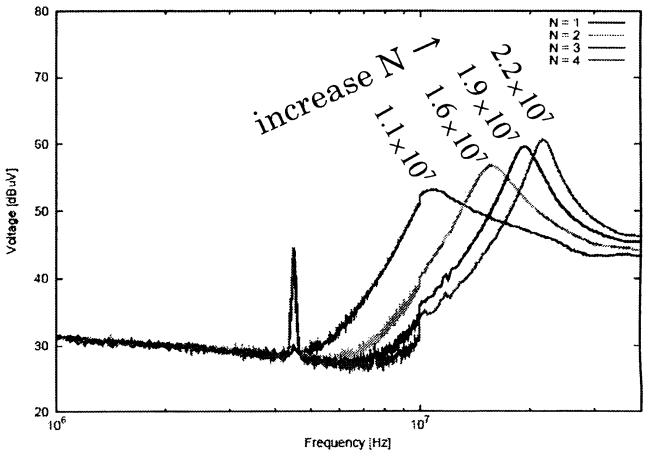
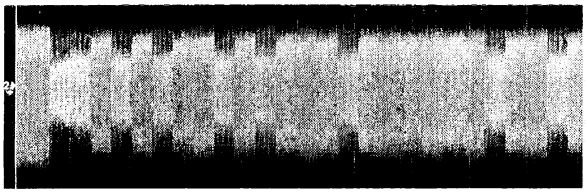


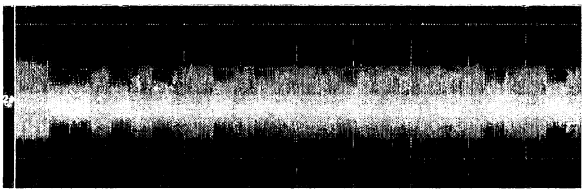
図 9:線路の本数を変化させた場合の周波数特性

また、各モデルを用いて取得した SPA 波形を図

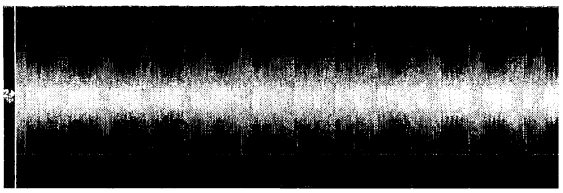
10 に示す。接続する線路の本数の変化に伴い、SPA 波形の見え方が変化していることがわかる。4.1 節と同様に、SPA 波形は 25MHz 以上の領域を遮断して観測した。



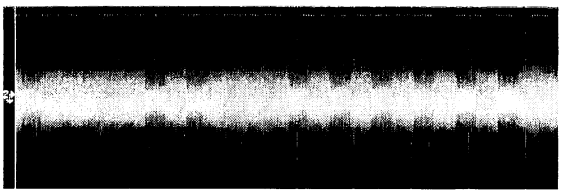
(a) N = 1



(b) N = 2



(c) N = 3



(d) N = 4

図 10: 線路の本数を変化させた場合の SPA 波形

3.3. 線路の取り付け間隔による影響の評価

最後に、基板に線路を取り付ける間隔を 10mm、60mm、90mm に変化させ(図 11)、各モデルにおいて線路から放射される電磁波の周波数特性を測定した。

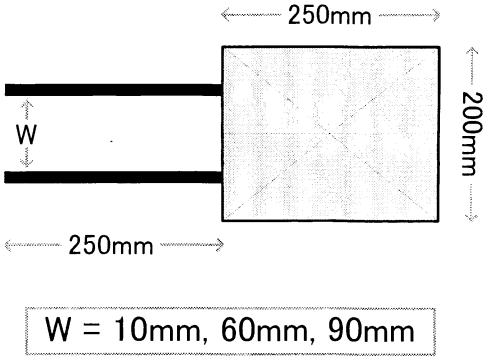


図 11:線路の取り付け間隔による影響を調べるためのモデル

結果を図 12 に示す。実験結果においては 16MHz 付近にピークが現れている。線路の間隔を変化させても周波数特性には大きな変化が見られなかった。

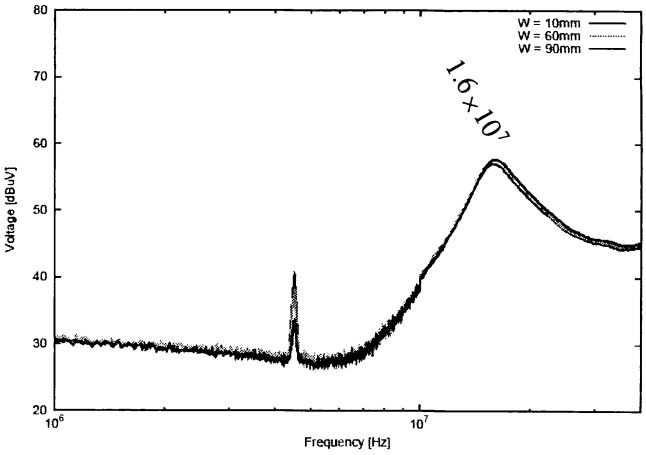
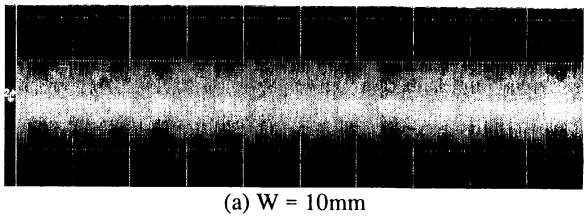
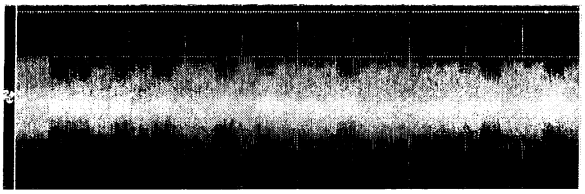


図 12: 線路の取り付け間隔を変化させた場合の周波数特性

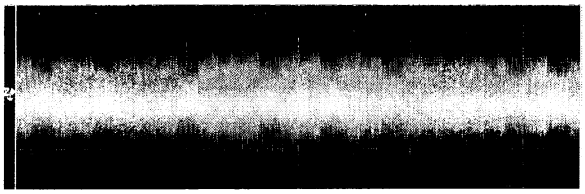
また、各モデルを用いて取得した SPA 波形を図 13 に示す。周波数特性と同様に、線路の取り付け間隔を変化させても SPA 波形の見え方には大きな変化は見られなかった。ここでも、SPA 波形の観測は 25MHz 以上の領域を遮断して行った。



(a) W = 10mm



(b) W = 60mm



(c) W = 90mm

図 13: 線路の取り付け間隔を変化させた場合の SPA 波形

4. 考察

4.1. サイドチャネル攻撃対策への応用

3.1 節および 3.2 節で行った実験において、接続する線路の長さや本数の変化に伴ってモデル基板の周波数特性や SPA 波形の見え方が変化することがわかった。このことは、周波数特性を変化させることによって SPA 波形の見え方を変化させることができる可能性を示している。

たとえば、図 14 に示すような周波数特性を持つ機器 Device A があったとする。もしも斜線部分の帯域に消費電力波形などの秘密情報が含まれていた場合、この機器は秘密情報を放射しやすい(すなわち、サイドチャネル攻撃に弱い)機器であるといえる。

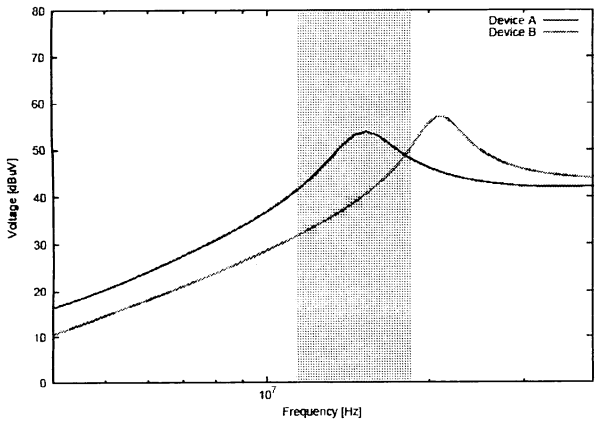


図 14: サイドチャネル攻撃対策への応用

一方で、Device B は Device A と比較して秘密情報が含まれる帯域の周波数特性が低く、秘密情報を放射しにくい。すなわち、Device A と比べてサイドチャネル攻撃に強い機器であるということができる。

このように、秘密情報が放射されにくくなるよう周波数特性を調節することができれば、機器のサイドチャネル攻撃に対する耐性を上げることができる。3 章で行った実験の結果は接続する線路の長さや本数を変化させることによって周波数特性を調節できるということを示しており、機器の物理的設計の面からサイドチャネル攻撃対策を行える可能性がある。

5. まとめ

本論文では、情報機器に線路を接続する際の指針を与えることを目標とし、そのための基礎的な研究として情報機器に接続された線路が秘密情報の伝搬に与える影響を調べるための実験を行った。また、RSA を実装した SASEBO で復号化処理の際に生じた過渡電流を励振源として基板に接続された線路上で実際に SPA 波形を観測し、接続する線路の長さおよび本数を変化させた場合においてその見え方が変化することを確認した。

実験の結果、モデル基板 5MHz～22MHz 付近にピークが現れることがわかった。このピークは接続した線路の長さが長くなるほど左方向に、線路の本数を増やすほど右方向に推移することがわかった。また、線路を接続する間隔にはほぼ影響を受けないということがわかった。

また、様々な条件で線路を接続することによって機器の周波数特性が変化することを利用し、秘密情報を放射しにくい機器を設計可能であるを示した。

6. 参考文献

[1] K. Gandolfi, C. Mourtel, F. Olivier, "Electromagnetic analysis: concrete results", CHES2001, pp.251-261, 13-16 May 2001.

[2] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, Pankaj Rohatgi, "The EM Side—Channel(s)", CHES2002, pp.29-45, 2003

[3] 林優一, 菅原健, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, 佐藤 証, "電源ライン上の漏洩情報を用いたサイドチャネル攻撃," コンピュータセキュリティシンポジウム 2008, D5-2, October 2008.

[4] Paul Kocher, Joshua Jaffe, Benjamin Jun, "Introduction to Differential Power Analysis and Related Attacks", 1998.