計測自動制御学会東北支部 第 256 回研究集会 (2010.3.12)
資料番号 256-7

情報機器の実装構造が電磁情報漏洩に与える影響の測定

Influence of Hardware Structure for Electromagnetic Information Leackage from Information Devices

○池松大志 *，林優一 *，水木敬明 *，曽根秀昭 *

○ Taishi Ikematsu*, 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, 電力解析攻撃, EMC, 電磁情報漏洩

連絡先：〒 980-8578　宮城県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
池松大志，Tel.: (022)795-6094，E-mail: a6tb2015@cs.he.tohoku.ac.jp

1. はじめに

近年、電子機器から放射される電磁波に機器内部の処理情報が含まれ、こうした電磁波を解析することで機器内部の秘密情報を遠方から取得可能であることが問題となっている [1, 2]。

こうした機器から漏れる電磁波のメカニズムの一例として、LSIから発生する過渡電流がグランドバウンスを引き起こし、その結果生じたコモンモード電流が機器を構成する基板や線路に伝播し、放射電磁波が発生するという仕組みがある [3]。コモンモード電流は機器から遠方に到達する電磁波を発生させる主要因の一つとなっており [4]、コモンモード電流に秘密情報が含まれた場合、機器の遠方で秘密情報が取得可能である事から、新たな脅威となりうる [5]。一方、このようなメカニズムによって発生する電磁波は、機器の実装構造（基板の大きさ、線路の長さ、本数）の違いによって秘密情報の漏れやすさに変化が生ずる事が指摘されている [6]。

本研究では、機器の配線時に取り回しの形態として用いられる線路の巻き方が電磁情報漏洩に与える影響について検討する。

2. 実験対象と評価方法

2.1 測定モデル

本測定では機器に接続された線路の巻き方をパラメタとして扱う。そのため、その他のパラメタの影響を小さくするために、プリント基板と電源線から成る単純な機器モデルを用いた。モデルは Fig.1 に示す様に、200 mm × 125 mm の二層プリント基板と 4000mm のより対線から構成される。基板中央には入力ポート（SMA コネクタ）が実装されている。実験では、暗号処理に用いる秘密鍵を秘密情報とし、AES[8] を実装したサイドチャネル攻撃用標準評価基板 SASEBO（Side-channel Attack Standard Evaluation Board）[7] から発生する過渡電流を入力信号として励振し、

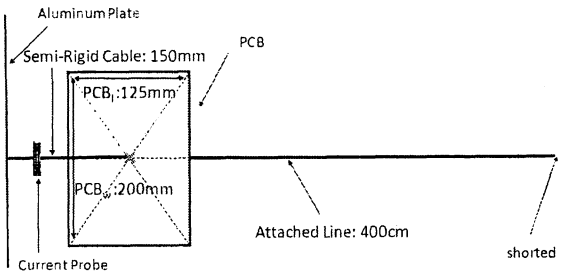

Fig. 1　測定モデル

機器外部に伝搬したコモンモード電流を観測する。

2.2　評価方法

本実験では機器外部で観測されたコモンモード電流に対して、電力解析攻撃を行うことで秘密鍵情報の漏洩評価を行う。電力解析攻撃は暗号モジュールにおいて暗号処理が行われる際に、処理データ（暗号・復号化するデータ、秘密鍵）によって機器の消費電力がわずかに変化することに基づいて秘密鍵情報を奪取可能か否か判定するための統計的解析法である。本手法を機器外部で取得されたコモンモード電流に適用することで、秘密情報の漏洩に対する定量的評価を行う。

3.　実験

本節では 2.1 節で示した測定モデルを用いて、電源線の巻き方が電磁情報漏洩に与える影響について検討する。本実験では巻き方の中でも、特に巻き数に着目した。具体的にはモデル基板に接続された線路に巻きを作り、モデル周囲に発生するコモンモード電流を計測する。また、取得したコモンモード電流に 2.2 節で示した評価方法を適用し、評価手法によって得られる秘密鍵取得に必要な波形数をパラメタとして巻き数によって変化する秘密情報漏洩の違いを観測する。

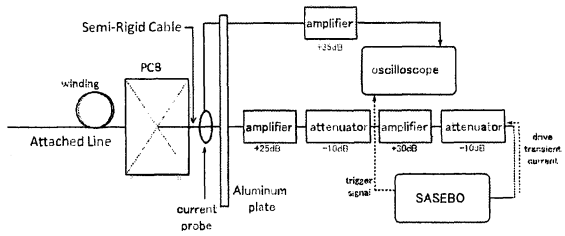

Fig. 2　測定環境

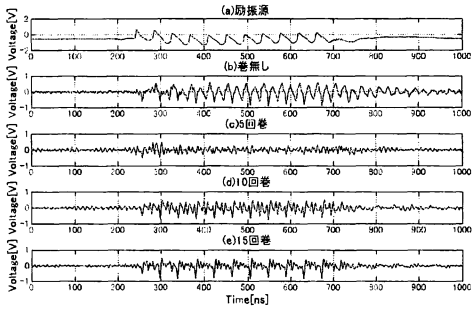

Fig. 3　巻き数によって変化する時間波形

3.1　実験条件

Fig.2 に測定環境を示す。SASEBO に実装されたモジュールから発生する過渡電流を計測し、それをアンプにより増幅させた後、SMA コネクタを通じてモデル基板に励振する。この際、セミリジットケーブル上に設置した電流プローブを用いて、モデル周囲に発生するコモンモード電流を計測する。電流プローブによって計測したコモンモード電流をアンプで増幅して、オシロスコープで表示し、データの取得を行う。データ取得を行う線路の巻き数は、5 回、10 回、15 回、巻無しの 4 パターンで計測を行った。また、線路の巻きは基板から 20cm の位置に配置し、円周は 20cm とした。

3.2　実験結果

測定結果は Fig.3 に示す。巻き数の変化に伴い取得されるコモンモード電流に差異が観測された。それぞれの条件で励信信号、観測点は同一である事から、線路の巻き数によって機器の実装構造が変化し、機器外部に伝搬するコモン

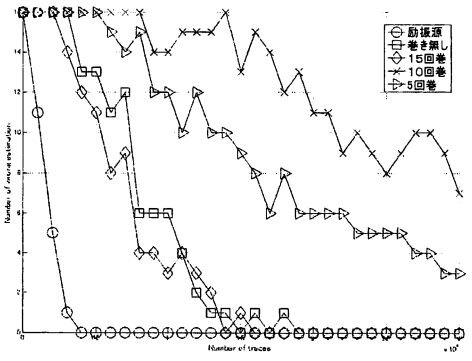

Fig. 4　巻き数によって変化するエラーレート

モード電流の周波数特性に変化が生じたため、波形に差異が生じたと考えられる。

3.3　取得波形に対する電力解析攻撃

各条件下で観測されたコモンモード電流に対して電力解析攻撃を行った。具体的な解析方法は Correlation Power Analysis（CPA）[9] を用い、AES の最終ラウンドにおけるレジスタの Hamming Distance を電力モデルとして、取得波形との相関値を計算することで秘密鍵の取得を試みた。秘密鍵の値は、アルゴリズム仕様書[8] に示されたテストベクタとした。平文として 30,000 個を入力し、対応する 30,000 波形を取得した。波形の取得は、SASEBO から出力されるトリガ信号によって制御した。鍵の推測対象は AES アルゴリズムの 10 ラウンド目のラウンド鍵を対象とし、電力モデルは 16 バイト（=128 ビット）ある鍵のうち 1 バイトずつを推測して作成した。解析結果をエラーレートで表示したものを Fig.4 に示す。横軸は解析に用いた波形数、縦軸は 16 バイトのラウンド鍵全体のうち正しい鍵を推測できなかったバイト数である。少ない波形数でエラーレートが低い場合、秘密情報の解読が容易であることを表している。なお、推測鍵の決定には相関値の最大値と最小値の差が最も高くなるものを選択した。これは相関値が正負両方に現れることを考慮したものである

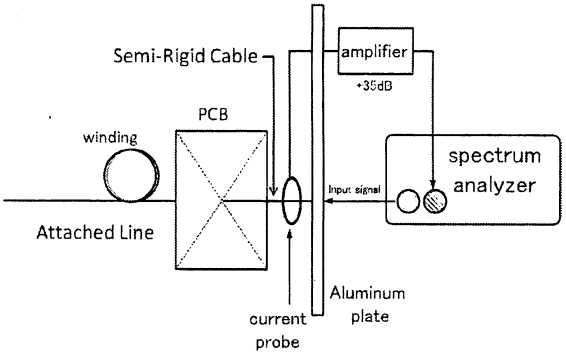

Fig. 5　周波数特性の測定環境

[5]。Fig.4 より、線路の巻き数毎にエラーレートを比較した際、差異が観測された。巻無しと 15 回巻は 15,000 波形程度で全ての鍵の一致に成功しているが、5 回巻、10 回巻では 30,000 波形使用しても秘密鍵をすべて一致させることができない。以上より、線路の巻き数を変化させた場合、秘密情報の漏洩に差異が生ずることが明らかとなった。

4.　周波数特性の検討

本節では線路の巻き数によって秘密情報の漏洩に差異が生ずる原因を考察するために、線路の巻き数ごとに変化するコモンモード電流の周波数特性を測定した。測定環境は Fig.5 と同様の環境下で行った。

励振源は振幅 107dBuV(0dBm) の正弦波とし、計測される波形をアンプで増幅し, スペクトラムアナライザで周波数特性を測定した。Fig.6 に測定した各条件の周波数特性を示す。なお、Fig.6 に示した各値はアンプでの増幅分を差し引いた値となっている。結果より、周波数特性が各条件によって変化していることが分かる。特に 10 MHz から 30 MHz 付近の周波数帯では共振、半共振が現れ、それらの周波数が巻き数によって大きく変化していることが観測された。このことから、線路の巻き数によって機器の実装構造により構成されるフィルタの周波数特性に差異が生じ、秘密情報を含む周波数帯に与える影響

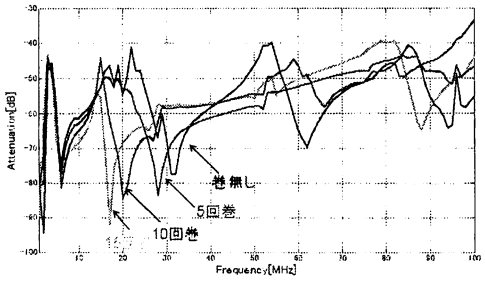

Fig. 6　巻き数によって変化する周波数特性

が変化したため、秘密情報の漏洩に差異が生じたものと考えられる。

5. まとめ

本稿では、電子機器の電源線の巻き方が電磁情報漏洩に与える影響について検討を行った。機器から生ずる漏洩信号として機器外部に発生するコモンモード電流を用い、電力解析を線路の巻き方によって変化するコモンモード電流に適用し、機器外部に漏洩する秘密情報を電力解析攻撃を用いて評価した。実験および評価の結果から、これまで検討されて来た、機器を構成する基板の大きさ、機器に接続された線路の長さ、線路の本数と同様に線路の巻き方が秘密情報の漏れやすさに影響を与えることが明らかとなった。

参考文献

1) D.Agrawal, B.Archambeault, J.R.Rao, P.Rohatgi, " The EM side-channel(s), " CHES 2002, LNCS 2523, pp.29-45,2002.

2) P.C.Kocher, J.Jaffe and B.Jun, " Differential power analysis, " Proc.CRYPTO, LNCS, vol.1666, Springer, pp. 388?397, 1999

3) T.Sudo, H.Sasaki, N.Masuda and J.Drewniak, " Electromagnetic interference (EMI) of system-on-package (SOP), " IEEE Trans. Advanced Packaging, 27(2), pp. 304?314, 2004

4) Clayton R. Paul, "Introduction to Electromagnetic Compatibility(Wiley Series in Microwave and Optical Engineering)," Wiley-Interscience,2006.

5) Y.Hayashi, T.sugawara, Y.Kayano, N.Homma, T.Mizuki, A.Satoh, T.Aoki, S.Minegishi, H.Sone and H.Inoue, "An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current",EMC'09 Kyoto,Jul.2009,Kyoto Japan.

6) 大村孔平, 林優一, 水木敬明, 曽根秀昭, " 情報機器に接続された線路が機器からの電磁的情報漏洩に与える影響, " 電気学会マグネティックス研究会資料,Vol.MAG-09 No.94-107 Page.19-24 (2009.10.22).

7) Side-channel Attack Standard Evaluation Board, http://www.rcis.aist.go.jp/special/SASEBO

8) NIST FIPS PUB. 197, Advanced encryption standard(AES)

9) Eric Brier, Christophe Clavier, and Francis Olivier, "Correlation Power Analysis with a Leakage Model," Proc.CHES 2004,Lecture Notes in Computer Science, vol.3156, Springer,pp.16-29,2004