L-011

SASEBO-R を使用した電磁波解析と電力解析の比較

Comparison of Power analysis and Electromagnetic analysis using SASEBO-R

菅野哲太郎† 岩井啓輔† 黒川恭一†
Tetsutaro Kanno Keisuke Iwai Takakazu Kurokawa

1．背　景

情報通信技術の発達と普及により、これらを悪用した犯罪も発生しておりセキュリティを確保する必要性がある。このセキュリティの中核に暗号が利用され、それに利用されている暗号アルゴリズムは一般にその内部を公開されている。これらは全て暗号処理に要する秘密鍵を暗号文及び平文から算出するために膨大な時間を必要とすることから、安全性を確保している。逆に、暗号アルゴリズム内の脆弱性により実際の鍵長より短い鍵長で解読可能を試みる論理的な手法による検証は、数多くの研究者により実施されている。現在使用されている暗号は現実的な時間内での解読が困難と立証されたものが使用されている。しかし、99 年に Kocher らによって暗号を実装したデバイスの消費電力と暗号処理の関係から暗号解読が可能であることが発表され[1]、デバイスへの暗号実装方法についても充分な研究を実施する必要性がある。電力解析については、これまでに多くの研究成果が発表されているが電磁波解析については研究成果が少なく[2]、特に部分鍵の特定に影響を及ぼす原因について定量的に求める必要がある。

2．サイドチャネル攻撃の概要

サイドチャネル攻撃により、暗号デバイスにおいて暗号処理時間や、それに要した消費電力等のサイドチャネル情報から、秘密鍵を特定する情報の取得が可能である。

2.1　電力解析

99 年に発表され、暗号処理時の単一の電力波形による単純電力解析(SPA:Simple Power Analysis)、SPA を多数実施しそれを統計処理により暗号鍵を特定する差分電力解析(DPA:Differential Power Analysis)などがある。これらは、暗号文単独攻撃であり、解読のために平文を必要としない。また、暗号処理時のハミング重み・距離と消費電力との相関から鍵を求める相関電力解析(CPA:Correlation Power Analysis)もあり、CPA は DPA に比較して鍵の特定に必要な波形数が少ないという利点がある[3]。

2.2　電磁波解析

暗号デバイスは、暗号処理を実行する際に電力を消費し、その際に電磁波も発生する。このデバイスから漏洩する電磁波は、処理の種類や処理しているデータに依存して変化する。そのため、暗号デバイスから漏洩している電磁波を解析することで、内部情報の取得が可能となる。なお、電磁波解析攻撃では、特定の箇所から放射されている電磁波を測定して解析を行えるため、高精度かつ測定位置の自由度が高い。電磁波解析は、暗号攻撃のためのサイドチャネル情報の獲得が電力か電磁波かの違いがあるだけであるため、その解析手法は電力のそれと同一で、単純電磁波解析(SEMA: Simple Electro Magnetic Analysis)、差分電磁波解析(DEMA: Differential ElectroMagnetic Analysis)、そして相関電磁波解析（CEMA: Correlation ElectroMagnetic Analysis）に分類される。過去の電磁波解析においては、暗号実装したデバイスの近傍での漏洩電磁波を捕らえている研究が主であり[4]、そのデバイスと繋がる電線からの漏洩電磁波を捕らえたものは無い。本研究では、電力解析の測定点であるシャント抵抗部からの漏洩電磁波を計測した。シャント抵抗は暗号デバイスの消費電力の計測のために設置されている。電流は回路に加わる電圧とその間の抵抗で線形的に求まるものであり、電磁誘導の法則に示されているとおり電流に応じて電磁波も発生する。

3．暗号 LSI に対する電磁波解析

3.1　実験環境(SASEBO-R)

SASEBO(Side Channel Attack Standard Evaluation Board) は暗号モジュールの物理解析攻撃の研究の共通プラットフォームを目的に開発された。SASEBO-R は暗号モジュールに LSI を使用しているのが特徴であり、図 1 にその概観を示す。TSMC 社製 0.13μm CMOS プロセスによる暗号 LSI をソケット内に実装している。制御用 FPGA に Xillinx 社製 VirtexIIPro シリーズ(XCIIVP30-5FG676C)を搭載している[5]。最大動作周波数動作 24MHz であり、本実験ではこの周波数を使用した。なお電源電圧は 3.3V である。

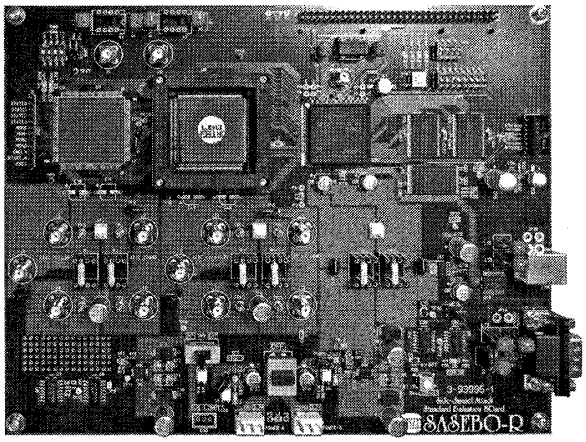

図 1　SASEBO-R

3.2　実験方法

暗号処理時の消費電力及び電磁波解析を実施した。測定位置は、電力はシャント抵抗の両端部、電磁波は同抵抗の周囲に 20 周巻き付けたもの（直径 2.5mm）である。オシロスコープ（TDS2024,2GS/s）で、これらから得られ

†防衛大学校　情報工学

た漏洩情報を取得、観測した。なお周波数成分は、SASEBO-R の仕様書ではオシロスコープの帯域制限を 20MHz とした例が記載されている、本実験では 20MHz の帯域制限をかけたものとかけていないものを観測した。なお、暗号攻撃対象アルゴリズムは AES（PPRM1）である。これは１段の AND-XOR ロジックで S-box を記述したものであり、SASEBO に実装されたアルゴリズムの中でも少ない波形数で鍵特定に至るものである[6]。

4. 実験結果

4.1 単純解析

計測したシャント抵抗部からの単純波形を 20MHz 帯域制限をかけたものを図２に、そうでないものを図３にそれぞれ示す。これらのグラフから消費電圧と同様な漏洩電磁波が観測された。しかし、電磁波に関しては帯域制限のある場合では、ほぼ正弦波に近い形になっており、逆に制限の無い波形は電力波形に近い形になっている。

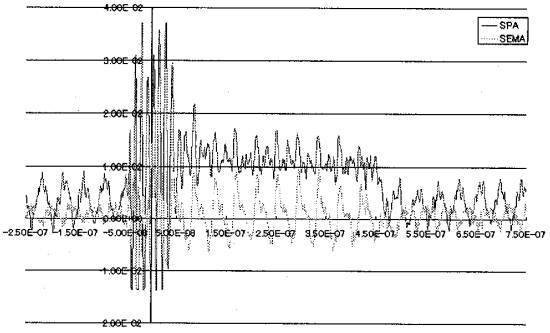

図２　単純解析波形（20MHz 帯域制限あり）

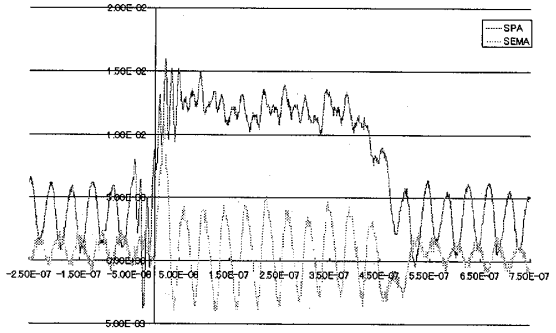

図３　単純解析波形（20MHz 帯域制限なし）

4.2 相関解析

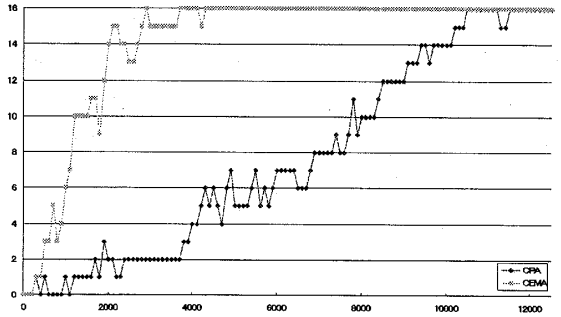

図４　相関解析結果

帯域制限のかかっている相関解析結果を図４に示す。この結果から、帯域制限の無い場合には CEMA はより少ない波形で鍵を全数特定しているが、CPA は倍以上の波形を必要としている。

4.3 鍵特定と分散

表１に、鍵特定に至る波形の位置の平均とその偏差を示す。CEMA は CPA に比較して攻撃範囲が狭くなった。電磁波は、同一箇所に集中する傾向がある。暗号攻撃の範囲によって鍵特定に要する波形数が異なることから、CEMA の場合は位置が特定することで、より少ない波形数で鍵が特定されてしまう。反対に、攻撃範囲が外れてしまうと、CPA より部分鍵特定に要する波形数が多くなる。

表１　部分鍵特定と波形平均位置とその標準偏差

解析法	区間	平均位置	標準偏差	部分鍵特定数 (Tr:取得波形数)
電　力	2033-2233	2109	28.39	15/16 (Tr=15000)
	2033-2133	2097	18.08	14/16 (Tr=15000)
	2133-2233	2157	15.29	16/16 (Tr=15000)
電磁波	2033-2233	2090	6.3	16/16 (Tr = 5600)
	2033-2133	2090	6.3	16/16 (Tr = 5600)
	2133-2233	2153	11.26	12/16 (Tr = 5600)

5. まとめ及び以後の課題

シャント抵抗部からも CPA だけでなく CEMA が可能であるが、同一の結果にはならないことが示された。特に帯域制限の無い場合は電磁波解析は少ない波形数で全数を特定しており、鍵特定の波形位置も集中する傾向が見られた。これは、取得した漏洩情報が必ずしも同一でなく、電磁波にあって電力に無い情報とは何かを突き詰めていくことが今後の課題である。また今回の実験では暗号アルゴリズムは AES の PPRM1 のみだったが、SASEBO には AES の実装方式については複数あるため、これらに対する電力及び電磁波の解析も行っゆく。

参考文献

[1]P. Kocher, J. Jaffe and B. Jun, "Differential power analysis", CRYPTO'99, LNCS1666, pp. 388-397, 1999.
[2]K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results", CHES2001, LNCS2162, pp. 251-261, 2001.
[3]E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model", CHES2004, pp. 16-29, 2004.
[4]福永利徳, 高橋順子, 山越公洋, 瀬賀研二, "サイドチャネル攻撃標準評価ボードを用いた電力および電磁波解析実験", SCIS2008, 1A2-3, 2008.
[5]本間尚文, 宮本篤志, 菅原健, 青木孝文, 佐藤証, "サイドチャネル攻撃評価用 ISO/IEC 標準暗号プロセッサの開発", SCIS2009, 2A1-1, 2009.
[6]渡部良太, 高橋芳夫, 松本勉, "暗号モジュールへの信号ラインからのサイドチャネル攻撃", CSS2008, D5, 2008.