L-020

AES に実装されたレジスタに対する相互情報量解析の適用
The mutual information analysis against a register in AES circuit

若林　邦爾†　　岩井　啓輔†　　黒川　恭一†

Kuniji Wakabayashi Keisuke Iwai Takakazu Kurokawa

1　はじめに

近年、インターネットの普及や IC カードの普及とともに情報セキュリティの重要性が高まっている．暗号モジュールに対する様々な攻撃手法が提案、考察されている中で、攻撃の痕跡を残さない強力な攻撃手法の一つとして、サイドチャネル攻撃の研究が活発に進められている．電力情報を用いたサイドチャネル攻撃としては、DPA (Differential Power Analysis), CPA (Correlation Power Analysis) [1] などが提案されている．DPA は、分類した波形を統計処理し、両者の差分をとることで秘密鍵を導出する手法であり、単純であることから、汎用的で自由度が高い攻撃手法である．CPA は DPA より強力といわれており、レジスタの遷移と消費電力が線形相関を持つことを仮定した攻撃手法である．これに対して MIA (Mutual Information Analysis) [2]も電力情報等を用いたサイドチャネル攻撃の一種であり、漏洩情報と測定値の間の相互情報量を利用する攻撃手法で、比較的新しく、評価及び研究事例が少ない．先行研究は [3]及び[4]が発表されており、いずれも AES 回路に対して MIA と CPA を比較し考察している．本研究では、SASEBO-R の AES 暗号回路に対して MIA を適用し、耐性評価の指針を探る．

2　MIA の概要

MIA は、漏洩情報に関する情報量と測定値に関する情報量から算出される相互情報量を比較し、最大を示した時の推測鍵を秘密鍵と推定するものである．相互情報量は(1)式により算出される．

$$I(X;Y) = H(X) - H(X \mid Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)\log\frac{p(x,y)}{p_X(x)p_Y(y)}dxdy \quad (1)$$
$$(x \in X, y \in Y)$$

ここで $P_X(x)$、$P_Y(y)$はそれぞれ X、Yの周辺確率分布を表し $P(x, y)$は X、Yの同時確率分布を表す．$I(X;Y)$は Xと Yの相互情報量、$H(X)$は Xの情報量、$H(X|Y)$は、Y が起こった時の Xの条件付情報量を表す．

本研究では、ループアーキテクチャにより実装された AES 暗号回路に対する攻撃を行うため、先行研究と同様に漏洩情報 L としてレジスタの中間値と出力値のハミング距離(以下、HD)を、測定値 O として暗号回路の消費電力をそれぞれ用いた．MIA において漏洩情報をレジスタ遷移とした場合の CPA との大きな違いは、CPA はピアソン積率相関係数により秘密鍵を導出する手法であるのに対し、MIA は消費電力と HD の相互情報量をもとに秘密鍵を導出するという部分にある．漏洩情報を HD とした場合、(1)式は(2),(3)及び(4)式で表される．

$$I(O;L) = H(O) - H(O \mid L) \quad (2)$$

$$H(O) = -\sum_{i=0}^{8} P(O_i)\log_2 P(O_i) \quad (3)$$

$$H(O \mid L) = -\sum_{j=0}^{8} P(L_j)\sum_{i=0}^{8} P(O_i \mid L_j)\log_2 P(O_i \mid L_j) \quad (4)$$

ここで $P(O_i)$,$P(L_j)$及び $P(O_i/L_j)$ は、ヒストグラムを作成し算出する．消費電力に関するヒストグラムの階級(以下、bin)は、先行研究と同様に、HD の分類数と同数で、出現した値の最大値から最小値を等分したものを用いた．

CPA 及び DPA を MIA の特徴と比較すると、まず CPA では、AES の 1byte の処理ブロック（以下、処理ブロック）のデータサイズの中から、1bit または 2,3bit の選択 bit を設定し適用する方法は想定していないため、処理ブロックの中で柔軟に選択関数を設定することができないこと、また DPA では、複数の bit を組み合わせた選択関数に対する適用は可能であるが、統計処理の後に有意な差が見られない場合に、相関の強弱を測ることは難しいということがある．一方、MIA では確率分布により決定された値から算出される相互情報量を用いるため、CPA や DPA より選択関数の設定が幅広く、DPA より相関の度合いを多様に表すことが可能であり、攻撃者にとって有利であると考えられる．

† 防衛大学校　情報工学科

3　実験及び結果

本研究では、AES の最終ラウンドのレジスタ遷移を攻撃対象として MIA 及び CPA を適用した．MIA については、処理ブロックにおける全 bit、1bit 及び 2,3bit の例に分けて適用した．

3.1 実験環境

評価基板には産業技術総合研究所及び東北大学で開発されたサイドチャネル攻撃用標準評価基板 SASEBO-R [5]を用いた．SASEBO-R には、AES 暗号回路が表 1 に示す 7 種の実装方法により実装されている．使用した機器を表 2 に示す．CPA には、サイドチャネル攻撃評価用自動測定ソフトウェア [6]を用いた．

表 1　SASEBO-R における 7 種の AES 暗号回路

略　称	実装方法の概要
AES-Comp	合成体によるS-boxを用いたAES
AES-Comp-ENC-top	AES-Compの暗号化部のみのAES
AES-TBL	case文で記述したS-boxを用いたAES
AES-PPRM1	Positive Prime Reed-Muller 論理による1段のAND-XORロジックによるS-boxを記述したAES
AES-PPRM3	Positive Prime Reed-Muller 論理による3段のAND-XORロジックによるS-boxを記述したAES
AES-SSS1	擬似RSLによるDPA対策を施したAES
AES-S	FPGAと同等のノードをもつネットリストとなるように制約を与えて論理合成したAES

表 2　使用機器

項　目	機器名称
供給電源	KIKUSUI PMM18-2.5DU
オシロスコープ(2GS/s)	IWATSU DS-4354ML

3.2 実験結果

結果を処理ブロックでの HD(0≦l≦8(l=HD 数)) に対応した 9 種類の場合（以下、8bit の MIA）と、処理ブロックで選択した 1bit の遷移及び選択した 2,3bit の遷移に対応した種類の場合(以下、1bit の MIA 及び複数 bit の MIA)の順で示す．8bit の MIA は、攻撃対象とする HD の空間サイズが CPA と同じである．

3.2.1 7 種の AES 暗号回路に対する 8bit の MIA

図 1 は、SASEBO-R に実装されている 7 種の AES 暗号回路について MIA を適用し、推測鍵が秘密鍵であった数(以下、特定した鍵数)と波形数の関係を表したグラフである．同じ波形数で比較した場合、特定した鍵数は、CPA に比べて MIA の方が少なく、CPA が部分鍵 16 個全てを特定した時でも、MIA では CPA と同じ波形数で約 4 割～7 割程度の特定数にとどまった．

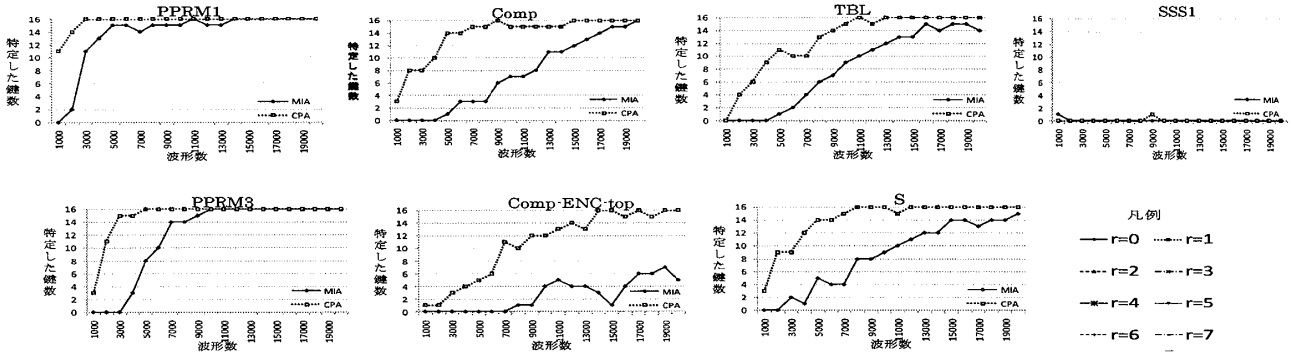

図 1　MIA と CPA の比較結果

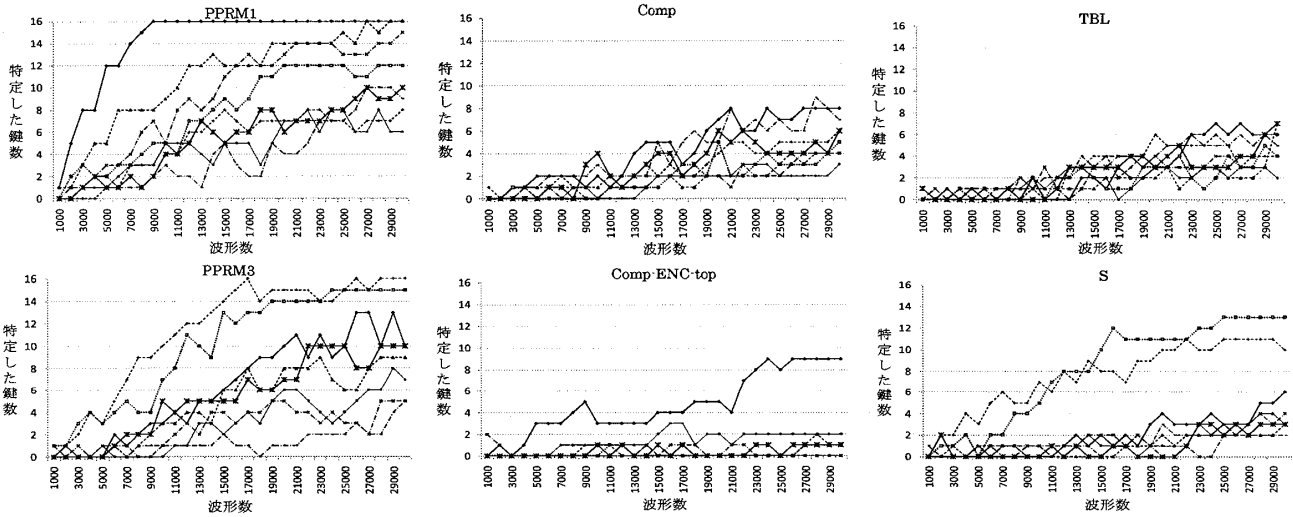

図 2　1bit の MIA の結果

3.2.2 1bitのMIA

次に、選択した1bitの遷移に着目し、遷移の有無により2つに分類する方法でMIAを適用した．これは分類数を減らすことでbinを大きくし、ノイズの低減等の効果により消費電力の偏りがより大きく現れた場合に効率が向上すると考えたためである．適用した結果を図2に示す．rが選択bitを表し、r=0が各処理ブロックにおけるMSBである．各種暗号回路の各bitにおいて、特定した鍵数または特定に必要な波形数にばらつきが見られた．PPRM1においては、レジスタのMSBを選択bitとした時の攻撃効率がかなり高く、9000波形で16個の秘密鍵全ての特定に成功した．8bitのMIAでは5000波形で15個の秘密鍵を特定したが16個全ての秘密鍵特定に11000波形を要している．SSS1については、どのbitも鍵の特定には至らなかったため省略した．

3.2.3 複数bitのMIA

次に、1bit の MIA により得られた結果から相関の度合いを考慮し、特定した鍵数が多かった bit から 2,3bit 選択し MIA を適用した結果を図 3 に示す．AES-S のみ、2bit 選択した MIA の結果が最も効率が高かった．PPRM1、PPRM3、Comp-ENC-top、S においては、複数 bit の MIA の方が 8bit の MIA より効率が高かった．

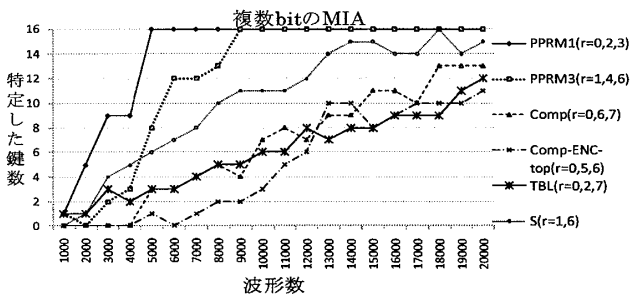

図 3　複数 bit の MIA の結果

4 まとめ

SASEBO-R において AES 暗号回路のレジスタに着目した場合 CPA の方が MIA より効率が高い攻撃手法であり、レジスタの遷移と消費電力との線形相関を抽出する方が秘密鍵の導出に効率的であったと考えられる．処理ブロックの 1bit に着目した場合、AES-PPRM1 においては MSB の 1bit で部分鍵を全て特定できたことから、レジスタの特定の bit が秘密鍵との相関を強めていることが分かった．また実装方法によっては、複数 bit の MIA の結果が、8bit の MIA より効率が向上することから、レジスタの遷移を攻撃対象とした場合でも、選択 bit の設定が攻撃効率を左右すると考えられる．今後は、従来の攻撃手法では成功しなかった暗号または実装方法に対して MIA を適用するため、選択関数に関して研究を進める．

参考文献

[1] E.Brier, C.Clavier, and F.Olivier, "Correlation Power Analysis with a Leakage Model, "CHES 2004, LNCS 3156, pp.16-29, 2004.

[2] B.Gierlichs, L.Batina, P.Tuyls, B.Preneel, "Mutual Information Analysis, "CHES 2008, LNCS 5154, pp.426-442, 2008.

[3] 佐藤弘季, 堀洋平, 今井秀樹"SASEBO-GⅡ上の AES に対する相互情報量電力解析攻撃, "SCIS 2010, Jan, 19-22.

[4] 田口飛鳥, 堀洋平, 今井秀樹"サイドチャネル攻撃標準評価ボードを用いた CPA と MIA の比較評価, "IEICE Technical Report, IT2009-102, ISEC2009-110, WBS2009-81(2010-3).

[5] 産業技術総合研究所情報セキュリティ研究センター, "サイドチャネル攻撃用標準評価基板仕様書第 1 版, "http://www.rcis.aist.go.jp/files/special/SASEBO/SASEBO-ja/SASEBO_Spec_Ver1.0_Japanese.pdf/, 2007 年 3 月.

[6] 岩井啓輔, 南崎大作, 黒川恭一, "サイドチャネル攻撃評価用自動測定ソフトウェアの開発, " 電子情報通信学会技術研究報告, Vol.108, No.38, ISEC20081-15, pp.9-14, 2008 年 5 月.