L-009

AESの実装方法の違いによるCPAの比較

Tamper resistance of implementataion methods of AES against CPA

川村 和範* 岩井 啓輔* 黒川 恭一*
Kazunori Kawamura Keisuke Iwai Takakazu Kurokawa

1 はじめに

インターネットの普及と共に，情報を守るために暗号化された安全な通信が求められている．このような環境の中で，暗号解読手法の一つであるサイドチャネル攻撃として，電磁波解析攻撃や電力解析攻撃等が注目されている．電力解析には Brier ら [1] によって提案された CPA(Correlation Power Analysis) があり，ハミング距離モデルとハミング重みモデルという 2 つのモデルがある．2 つのモデルについて，AES の最終ラウンドへの適用例を以下の図 1 及び図 2 に示す．本研究では，ハードウェア実装及びソフトウェア実装された AES 回路に対する CPA における両モデルの差違を明らかにすることによって，回路を実装する際の耐タンパ性向上への指針を与える．

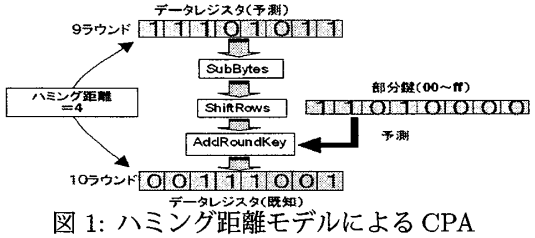

図 1: ハミング距離モデルによる CPA

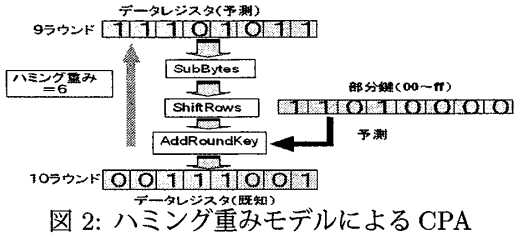

図 2: ハミング重みモデルによる CPA

2 ハードウェア実装された AES への CPA

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 及び SASEBO-R を用いた [4]．SASEBO-R には専用暗号 LSI が搭載され，AES 回路として，表 1 の通り S-Box の構成方法を変えた 7 種の回路が実装されている．

表 1: SASEBO-R に実装されている AES の略称

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 と同等のノードを持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

また，SASEBO には，Xilinx 社の Virtex-II Pro xc2vp7 が搭載され，SASEBO-R と同等の AES 回路を実装した．なお，擬似 RSL についての詳細情報が公開されていないため，AES-SSS1 は実装していない．また AES-S は，FPGA の AES-Comp と同様になるため省略した．今回の CPA では，対象となる AES 回路が，各ラウンドを 1 クロックで動作するループアーキテクチャで実装されていることを利用して，レジスタの遷移又は値と，それらが確定するクロックのエッジにおける消費電力との相関関係を評価した [2]．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 [3] を用いた．

2.1 実験環境

オシロスコープには IWATSU DS-4354ML，電源には KIKUSUI PMM18-2.5DU を用いた．クロックには NF CK1615 から 12MHz を供給した．

2.2 実験結果

AES に対して CPA のハミング距離・重みモデル各々を適用した結果として，SASEBO-R の結果を図 3，4 に，また SASEBO の結果を図 5，6 にそれぞれ示す．横軸は波形数，縦軸は特定した部分鍵のバイト数である．鍵長は 128 ビットとしたため，部分鍵は 16 バイトである．

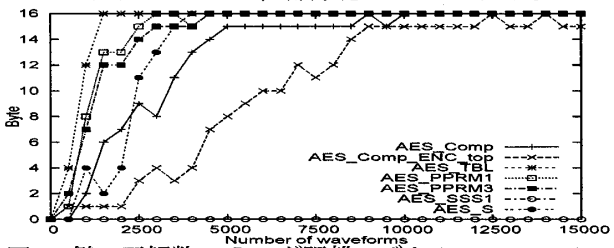

図 3: 鍵の正解数:ハミング距離モデル (SASEBO-R)

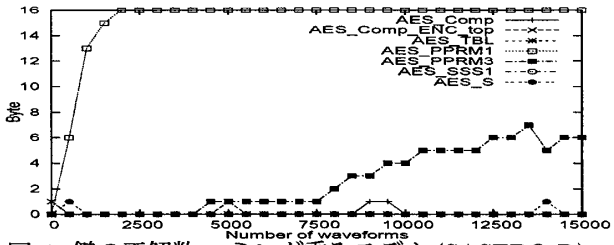

図 4: 鍵の正解数:ハミング重みモデル (SASEBO-R)

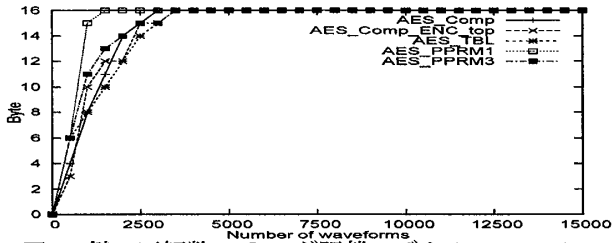

図 5: 鍵の正解数:ハミング距離モデル (SASEBO)

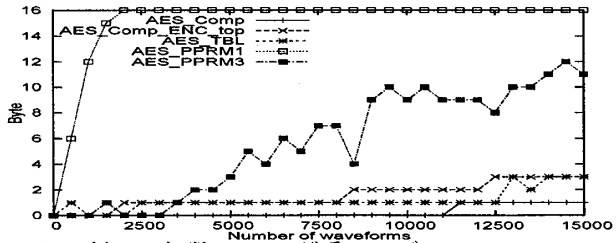

図 6: 鍵の正解数:ハミング重みモデル (SASEBO)

*防衛大学校情報工学科

SASEBO-R に関して，ハミング距離モデルでは，部分鍵の特定に必要な波形数に違いはあったものの，7 種のうち 6 種の AES 回路で，用いている全ての部分鍵を特定できた．ハミング重みモデルにおいては，AES-PPRM1 のみが 16 個の部分鍵を特定することができた．AES-SSS1 はハミング距離モデル，ハミング重みモデルともに部分鍵を特定できなかった．この結果から，疑似 RSL の CPA に対する有効性を確認することができた．SASEBO に関して，ハミング距離モデルでは，5 種の AES の部分鍵を全て特定できた．ハミング重みモデルでは，AES-PPRM1 のみ部分鍵を全て特定することができた．

SASEBO-R には ASIC，SASEBO には FPGA に暗号回路が実装されており，ASIC と FPGA に関して，図 3~6 より CPA のハミング距離モデル，ハミング重みモデルの差異は特に見られなかった．

3 ソフトウェア実装された AES への CPA

Xilinx 社の Virtex-II Pro xc2vp7 のソフトコア MicroBlaze 及びハードコア PowerPC を用いて SASEBO に AES をソフトウェア実装し，CPA を試みた．

3.1 実験環境

測定対象ボードには SASEBO，オシロスコープには Tektronix TDS 2024B，電源には TEXIO PA18-2B を用いた．クロックには NF CK1615 から 24MHz を供給した．ソフトウェアには Xilinx EDK10.1 を用いた．

3.2 実験結果

MicroBlaze 及び PowerPC で動作する AES の最終ラウンドに対して CPA を行った結果を図 7，8 に示す．ハミング距離モデルでは，部分鍵を特定できず，MicroBlaze のみハミング重みモデルで全ての部分鍵を特定することができた．

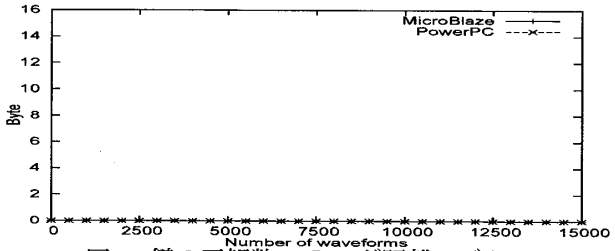

図 7: 鍵の正解数:ハミング距離モデル

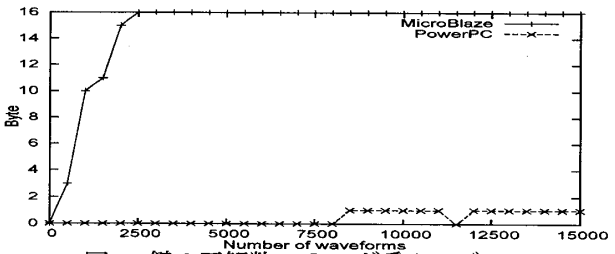

図 8: 鍵の正解数:ハミング重みモデル

ソフトウェア実装では，1 クロックで 1 ラウンドの処理を終えられず，数千クロックを要する．そのためトリガを用いることにより AES の最終ラウンドの各処理に分割して確認できる．PowerPC ではハミング重みモデルにおいて部分鍵を一部しか特定できなかったので，トリガを用いることで CPA を適用する範囲を最終ラウンド全体でなく，その内の各処理に細分化して CPA を行った．MicroBlaze でのハミング重みモデルの結果を図 9 に，PowerPC でのハミング重みモデルの結果を図 10 にそれぞれ示す．

ソフトウェア実装では，レジスタの値がすぐに入れ替わり，前の状態を保持しておくことができないために MicroBlaze，PowerPC 共にハミング距離モデルでは部分鍵

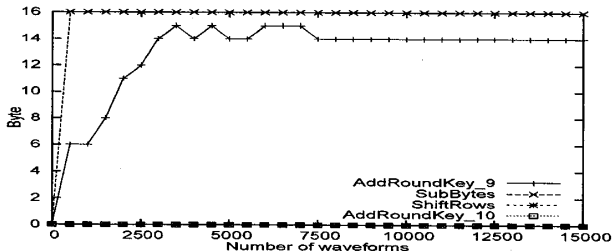

図 9: 鍵の正解数:ハミング重みモデル (MicroBlaze)

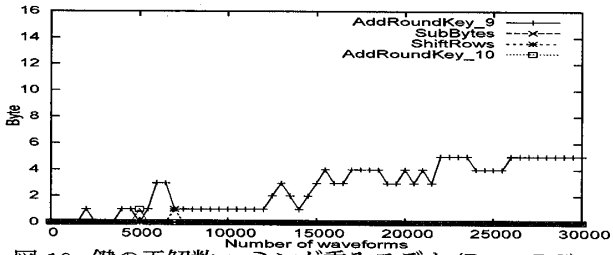

図 10: 鍵の正解数:ハミング重みモデル (PowerPC)

を特定できなかった．ハミング重みモデルでは，9 ラウンドにおける AddRoundKeys の結果をレジスタにストアし，10 ラウンドの SubBytes ではその値をレジスタからロードしているため，MicroBlaze においては，AddRoundKeys と SubBytes の処理で部分鍵をほぼ特定できた．PowerPC では結果があまり表れなかったので波形数を増やし，30000 波形取得した．その結果，PowerPC においては，AddroundKeys の処理で部分鍵を 5byte 特定することができた．

レジスタの値が頻繁に入れ替わるソフトウェア実装では，前のラウンドの値をレジスタに保持し続けられないため，図 7~10 の結果のようにハミング重みモデルが有効であることを確認した．

4 まとめ

ハードウェア実装及びソフトウェア実装された AES 回路に対してハミング距離モデルとハミング重みモデルそれぞれに基づいて CPA を行った．ループアーキテクチャを採用したハードウェア実装に対してはハミング距離モデル，ソフトウェア実装に対してはハミング重みモデルが有効であることが確認された．

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] 菅原健，本間尚文，青木孝文，佐藤証，“サイドチャネル攻撃標準評価 FPGA ボードを用いた暗号ハードウェアに対する電力解析実験，” マルチメディア，分散，協調とモバイルシンポジウム，Vol.2007，No.7D-5，pp.1415-1420，2007 年 7 月．

[3] 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，ISEC2008 1-15，pp.9-14，2008 年 5 月．

[4] 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．