1Y-5

AESのS-Box構成の違いによるサイドチャネル攻撃の耐性評価

佐藤　隆亮†　　吉川　雅弥‡

名城大学情報工学科†‡

1. はじめに

近年，IC カードなどのハードウェア実装された暗号回路に対するサイドチャネル攻撃の影響が問題視されている．標準暗号である AES の専用ハードウェアでは，一般的に S-Box と呼ばれる処理ブロックが攻撃対象である．これまでに，いくつかの S-Box の構成方式が提案されており [1]，ASIC を対象とした評価実験では，面積や消費電力だけでなく，サイドチャネル攻撃に対する耐性（耐タンパ性）が異なることが報告されている [2]．そこで本研究では，合成体とテーブル方式で構成した 2 種類の S-Box について，FPGA を対象に実装評価と耐タンパ性評価を行う．

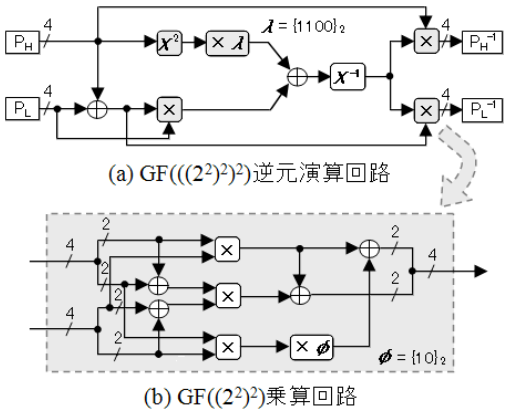
2. AES暗号ハードウェア

AES のアルゴリズムは，換字を行う SubBytes 処理，行ごとの巡回シフトを行う ShiftRows 処理，列ごとの演算転置を行う MixColumns 処理，鍵加算を行う AddRoundKey 処理，拡張鍵を生成する鍵スケジュールから成る．このうち SubBytes 処理は一般的に S-Box と呼ばれ，GF(2^8)上の逆元演算とアフィン変換を行う．S-Box は暗号化の中心処理であり，回路規模や消費電力に大きな影響を与える．そのため，このアーキテクチャを検討することが重要である．

代表的な S-Box 回路の構成方法には，合成体とテーブル方式がある．合成体は**図 1** に示すように，逆元演算回路に，アフィン変換回路を直列に繋ぐことで S-Box を実現する方法である．テーブル方式は，逆元演算とアフィン変換処理の結果を，真理値表で実現する構成方法で，HDL では case 文で記述する．これらを ASIC として実装した場合，合成体の方が，テーブル方式より回路規模が大幅に小さくなり，消費電力も低くなる [1] [3].

3. 合成体とテーブルの比較実験

暗号回路について，ASIC 実装した場合と FPGA 実装した場合を比較するために，2 種類の AES 回路をサイドチャネル攻撃用標準評価ボード SASEBO-GII へ実装し，サイドチャネル攻撃の 1 つである Differential Power Analysis (DPA) [4] による解析実験を行う．実験環境を**表 1** に示す．



(a) GF(((2²)²)²)逆元演算回路

(b) GF((2²)²)乗算回路

図 1. 合成体による GF(2^8)逆元演算回路

3.1. FPGA上での回路規模と消費電力

Verilog で記述した合成体とテーブル方式 [5] の実装結果を**表 2** に示す．表 2 中の Slice は 4 つずつの LUT と Flip Flop で構成された機能ブロックを表しており，合成体がテーブル方式に比べ，約 2 倍多く使用している．テーブル方式の場合，case 文で記述した S-Box が，自動的に BlockRAM へ実装されることで，使用される LUT の数が大幅に削減され，結果として，使用される Slice 数も削減された．一方，合成体においても 2 つの BlockRAM を使用しているが，これは制御用 FPGA とのバスを担う FIFO の read / write モジュールに各 1 つ使用されるためで，これはテーブル方式も同様である．

次に，実装した AES の暗号化処理における，最終ラウンド付近の測定波形を**図 2** に示す．測定には，電源ライン側の 1Ω シャント抵抗を用いた．Time = 0 が示すエッジのピーク電流値は，合成体が 0.0233[A]，テーブル方式が 0.0057[A]である．このように，FPGA 実装された合成体は，回路規模に比例して消費電力も大きくなる．

3.2. 耐タンパ性評価

耐タンパ性の検証では，まず，攻撃精度を検証するために，20000 波形を用いたハミング距離型 DPA により，攻撃タイミング周辺の差分平均電流の波形を導出した．この結果を**図 3**，**図 4** に示す．合成体と比べて，テーブル方式はピーク

Tamper resistance evaluation for two kinds of AES architectures
†Ryusuke Satoh　‡Masaya Yoshikawa
†‡Department of Information Engineering, Meijo University

表 1. 波形測定，DPA 実験環境

暗号回路用デバイス デバイス動作クロック 電源	Virtex-5 XC5VLX30 2MHz PC からの USB 給電
FPGA 実装ツール Synthesize - XST / HDL Options / ROM Extraction	Xilinx ISE Design Suite 12.3 有効
オシロスコープ プローブ ターミネータ 測定サンプリングレート	Agilent DSO1022A Agilent N2863A 300MHz 50Ω 0.5GSa / sec

表 2. AES 2 種の回路規模（ゲート数）

エレメント ＼ S-Box 構成	合成体	テーブル方式
Flip Flop [数]	1,271	1,271
LUT [数]	4,666	2,732
Slice [数]	1,904	962
18k BlockRAM [数]	2	10

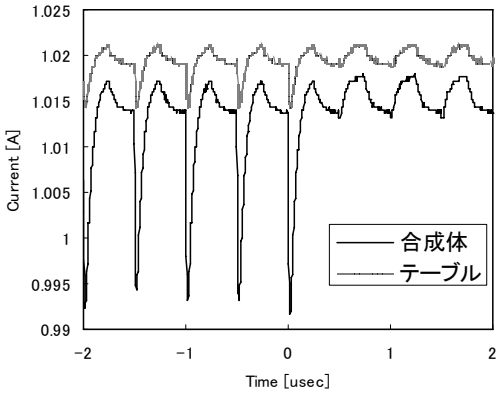


図 2. 暗号化処理時の測定波形

電流値が小さいため，差分波形のピークも小さくなり，正解鍵と不正解鍵の差が非常に小さい．

次に，差分波形から特定できた正解鍵の数と必要波形数の関係を**図 5** に示す．合成体では，解析に用いた電力波形の数が 4000 で，1 つの鍵（1 byte）以外は正解し，10000 波形以降では全てが正解となった．一方，テーブル方式では，5000 波形では 1 つも正解することがなく，10000 波形以上使用しても 3 つしか正解鍵を特定できなかった．

このように，FPGA 実装では，これまで報告されている ASIC 実装の場合と異なり，DPA 耐性はテーブル方式の方が合成体より高くなった．そのため，暗号回路の実装では，実装対象を考慮したアーキテクチャの選択が重要である．

4. まとめ

本研究では，AES を合成体とテーブル方式の 2 種類で構成して FPGA へ実装し，その耐タンパ性を定量的に評価した．また，実装評価実験により，FPGA 実装は，ASIC 実装と比較して，その特性が逆であることを明らかにした．今後の課題は，電磁波解析攻撃について検証していく予定である．

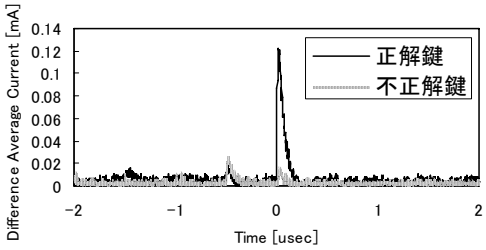


図 3. DPA で得た合成体の差分波形

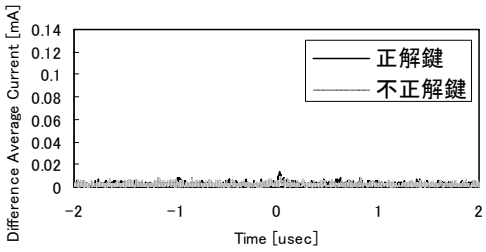


図 4. DPA で得たテーブル方式の差分波形

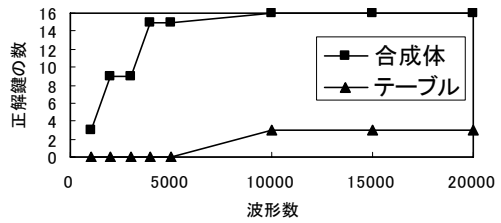


図 5. DPA で得た推定拡張鍵の正解数

謝辞

本研究は JST,CREST「ディペンダブル VLSI システム基盤技術」の研究の一環として行われた．

参考文献

[1] 森岡澄夫, 佐藤証, “共通鍵暗号 AES の低消費電力論理回路構成法,” 情報処理学会論文誌, vol.44, No.5, pp.1321-1328, May 2003.

[2] 川村和範, 岩井啓輔, 黒川恭一, “AES の実装方法の違いによる CPA の比較,” FIT2009, L-009, pp.147-148, 2009.

[3] Dr. S. Morioka, “数学いらずの AES 暗号 SubBytes 設計ガイド,” Design Wave Magazine, pp.152-157, Jan 2004.

[4] P.Kocher et al, “Differential Power Analysis,” Crypto 1999, LNCS 1666, pp.388-397, 1999.

[5] 東北大学 Cryptographic Hardware Project, http://www.aoki.ecei.tohoku.ac.jp/crypto/