

電力解析攻撃耐性を有する非同期 AES 回路の検討

1240288 市ノ木 一希 【コンピュータ構成学研究室】

1 はじめに

近年, IoT(Internet of Things) デバイスが様々な分野で活用されるに伴って, 高いセキュリティも求められている. 特に, 電力解析攻撃等のサイドチャネル攻撃によって暗号鍵を盗み出す行為に対しても耐性を有する回路技術の開発が急務となっている. 一方で, IoT デバイスは, 応用分野の多様性に適応するために, 専用 ASIC (Application Specific IC) チップではなく, 回路を書き換え可能な FPGA デバイスにより実現されることが多い.

そこで本研究では, AES (Advanced Encryption Standard) 暗号化回路を対象として, 電磁波 EM プローブによる電力解析攻撃に対する耐性を備えた AES 回路の FPGA 実装法について検討した. 提案回路は, 特に, ラウンド処理の実行タイミングを水平型 (時間的) に隠蔽するために, セルフタイム型データ転送制御回路により非同期的にパイプライン処理を実現している.

2 セルフタイム型耐タンパ AES 回路

AES 暗号化では, 各バイトを Sbox を用いて置換し, 順番を入れ替え, 4 バイト毎に行列演算し, ラウンド鍵を使って変換する処理を繰り返し行う. 128bit の場合には 10 ラウンド行う. このとき, 同期型 AES 回路では, クロックに同期して電磁波, すなわち物理的漏洩情報 PLI (Physical Leakage Information) が放射されるため, それらを電力として解析すれば容易に暗号鍵の解読が可能になる. その対策法として, 振幅 (垂直) 方向ならびに時間軸 (水平) 方向の PLI を隠蔽する技術が検討されている [1].

前者の技術として, (冗長) 補償器の挿入や相補型回路が提案されている [1]. 一方, 後者については, 同期回路では完全な PLI 隠蔽が困難であるという技術的課題がある. よって, 本研究では, 水平 PLI 隠蔽を可能にする AES 回路をセルフタイム回路により非同期化する回路を設計した. 設計した耐タンパ AES 回路の構成

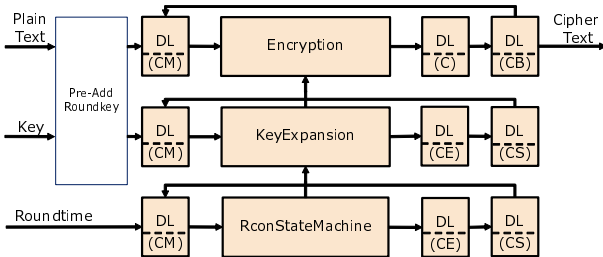


図 1 水平 PLI 隠蔽可能な AES 回路の構成

を図 1 に示す.

本回路では, 入力されてくる平文を鍵で最初に変換し, 以降のラウンド処理を繰り返す. 各ラウンドでは, (a) 暗号化 (Encryption), (b) 鍵拡大 (KeyExpansion), (c) ラウンド制御用状態機械 (Rcon-StateMachine) が並列に動作すると共に, 緩やかに, 各パイプライン処理が同期するようにセルフタイム回路でハンドシェイク制御する回路構成となっている.

本回路では, (c) 内で管理するラウンド数を用いて, (b) においてラウンド鍵を生成し, その後, (a) 内でそのラウンド鍵を用いた変換を実行するため, (a) の処理時間が最長になる. よって, (a) の完了を待って, (b) や (c) は次のラウンド処理を開始する必要がある. このため, (a) の最終段から出力される Send 信号を (b) と (c) へ送信し, 緩やかに同期させている. この同期用制御回路 CS も新たに設計した.

この制御方法によって, 各パイプライン処理が完全に同期しないため, 時間軸方法の PLI を隠蔽する効果が期待できる.

3 評価

AMD 社 FPGA Zynq-7010 上に提案 AES 回路を実装した. FPGA 回路資源と使用率を表 1 に示す. 30% 弱の回路規模で 128bit 暗号化回路を実現できることが判った. また, 配置配線後の実遅延シミュレーションで観測した結果, 約 1.54ms で 128bit 暗号化が可能であることを確認した. また, 図 1 の各パイプラインのラウンド開始時刻が約 9000ps ずつ時間差動作できており, 水平 PLI 隠蔽が期待できることを確認した.

現在は先行研究を元に非同期型 AES 回路を設計した段階であるため, 提案回路が持つ電力解析攻撃に対する隠蔽能力の高さを実証できていない. よってオシロスコープ等を用いて物理的に波形を調べ, 回路が有する垂直・水平隠蔽能力の検証が必要である.

参考文献

- [1] J.-S. Ng, et al. "A Highly Secure FPGA-Based Dual-Hiding Asynchronous-Logic AES Accelerator Against Side-Channel Attacks," IEEE Trans. VLSI Sys., vol. 30, no. 9, pp. 1144–1157, Sept. 2022.

表 1 提案 AES 回路の回路規模・回路使用率

Resource	Utilization	Ratio [%]
LUT	4998	28.40
FF	1191	3.38