電磁波解析攻撃耐性を有する非同期 AES 暗号回路に関する研究

市ノ木 一希　【 コンピュータ構成学研究室 】

A Study on an Asynchronous AES Cryptographic Circuit Resistant to Electromagnetic Analysis Attacks

Kazuki ICHINOKI　【 Advanced Computer Engineering Laboratory 】

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，電磁波解析攻撃等のサイドチャネル攻撃 SCA(Side Channel Attack) 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 [1] 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 プローブによる電磁波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．そのため，電力解析攻撃耐性を有していない同期 AES 暗号回路と提案回路に対し，実際に電磁波解析攻撃を実施することで，提案回路における SCA 耐性を確認した．

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 S-box 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 [2].

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 [2]．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．

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）が並列にかつパイプライン動作すると共に，各パイプラインが緩やかに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は同期しないため，時間軸方法の PLI を隠蔽する効果が期待できる．

3　漏洩電磁波解析による攻撃

提案回路の電磁波解析攻撃耐性を評価するため，サイドチャネル攻撃 (SCA) の 1 つである相関電磁波解析 (CEMA) を行う．本手法は，漏洩電磁波と中間値のハミング距離とが比例関係にあることを仮定して，任意の平文の暗号化において S-box の置換を行う際のハミングウェイトおよび消費電力に比例して漏洩する電磁波の相関関係から鍵を推測する．手順を以下に記載する．

- 暗号デバイスに平文（または暗号文）を入力し、動作時の漏洩電磁波を多数取得
- 鍵の候補（部分鍵）に基づいて、処理中の中間データのハミング距離を計算
- 取得した漏洩電磁波と予測したハミング距離との相関関係（ピアソンの積率相関係数）を計算
- 最も高い相関を示した部分鍵が、実際の正解鍵であると判定する

4　提案回路の実装とその電磁波解析攻撃実験

4.1　回路規模・実行時間

提案回路の実装に要した 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，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．

表 1　提案非同期 AES 回路の回路規模・回路使用率

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

4.2　電磁波解析攻撃実験

電磁波解析攻撃のセキュリティ強度の計測を行うために，AMD 社 FPGA Zynq-7010 上に提案 AES 回路および同期回路を実装した．また，計測機器として Agilient 社のオシロスコープ DSO9104A およびテクシオテクノロジー社の近傍界プローブセット GKT-008 を使用し，漏洩電磁波を取得した．予備実験として，FPGA からオシロスコープへのトリガ信号ケーブル内での伝搬遅延時間を特定するために，トリガ信号の立ち上がりから任意時間 T 後に 128 ビットが発振するテスト回路を作成し，実遅延シミュレーションによる T_s と，オシロスコープで計測した電磁波の変化から推測できる T_{oc} との差分から，トリガ信号ケーブル内の信号伝搬遅延時間を推定した．また，AES 暗号回路の動作を実遅延シミュレーションからトリガ信号の立ち上がり時間，1 ラウンド目の S-box の開始時刻および処理時間を確認した．

本実験では，FPGA ボード上のボタン押下後，$T_s = 100ns$ 遅延を設定し，AES 暗号回路の動作を開始させた．平文は最初の 1Byte を 0x00〜0xFF までの 256 通りとして，残りの 15Byte は全て 0xFF とすることで，漏洩電磁波を 256 回計測する．それらの計測データとハミング重みとの相関を図 1 のように算出する python プログラムを作成した．図 1 は，最大相関値となる部分鍵が 0x00 と推定された例を示している．

提案非同期 AES 回路および同期 AES 回路において，２種の部分鍵で暗号化している状況で，漏洩電磁波解析攻撃を実施した結果を表 2 に示す．

同期 AES 回路への電磁波解析攻撃は可能で正しく部分鍵を推定できた．一方，提案非同期 AES 回路に対する攻撃では正しく推定できなかった．この限りでは，提案 AES 回路は同期 AES 回路に比べて電磁波解析攻撃耐性が高いと言える．ただし，部分鍵が 0x00 の場合しか，実験できていないため，確定的な結論とは言えないため，今後，より多くの部分鍵を対象とした攻撃実験を実施する必要がある．また，今回の実験では，ピーク相関係数が関連研究の結果と比較すると多少低くなった．これは，FPGA 周辺のノイズや計測時間のばらつきの影響によるのではないかと考えられる．

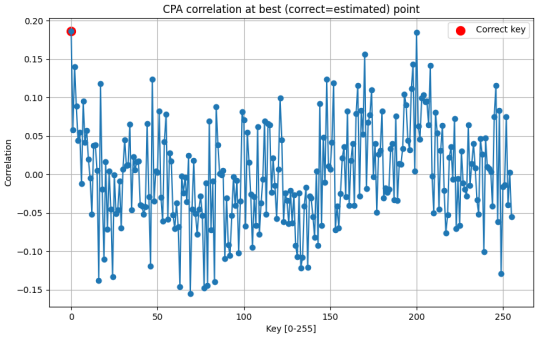

図 1　漏洩電磁波に対する各候補鍵の相関値分布例

表 2　各 AES 回路に対する攻撃結果 (抜粋)

回路	正解鍵	観測窓 [ns]	推定	相関係数
提案	0x00	—	不可	0.077
	0xAA	—	不可	0.173
同期	0x00	-12.9〜-6.9	成功	0.186
	0xAA	-19.2〜-13.2	成功	0.162

5　まとめ

本研究では，電力解析攻撃および電磁波解析攻撃耐性を高めるため，非同期 AES 暗号回路を提案した．FPGA チップを用いた漏洩電磁波解析攻撃の実験を通して，提案回路は同期 AES 暗号回路に比べて攻撃耐性を有する可能性が高い結果が得られた．ただし，実験の試行回数が限定的であるため，今後試行実験を積み重ねて，より高い確証を得ることが必要である．また，FPGA の漏洩電磁波を計測する際に FPGA 周辺機器等の様々なノイズの影響があった可能性も考えられるため，試行回数の増加やシールドの使用等により，AES 暗号回路の漏洩電磁波の計測精度を向上する必要がある．さらに，電磁波攻撃耐性の強度を定量化するために適した信頼性モデルを検討することも，電磁波解析攻撃耐性を有する回路を IoT 応用市場に普及させる上では重要な課題である．

参考文献

[1] S. Sanjaya, et al., “Application-Specific Power Side-Channel Attacks and Countermeasures: A Survey,” arXiv, 2512.23785, 2025.

[2] 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.