Vol.2022-SLDM-199 No.8
2022/11/11

乱数を用いた軽量な電力解析攻撃対策実装の検討

小柳結依 [1]　請園智玲 [1]

概要： IoT エッジデバイスの増加に伴い，サイドチャネル攻撃が現実的な脅威となっている．本稿では，サイドチャネル攻撃の一種である電力解析攻撃の対策回路を提案し，評価する．提案回路は先行研究の対策回路と比べ，乱数値を用いて，高い耐タンパ性を省実装面積で実現することを目的とする．本稿の評価では，提案回路の耐タンパ性が十分ではないことが確認されたが，同時に改善のための考察を得られた．

キーワード：サイドチャネル攻撃，電力解析攻撃，乱数

Considerations of a Light-Weight Implementation using Random Value against Power Analysis Attacks

YUI KOYANAGI[†1]　TOMOAKI UKEZONO[†1]

Abstract: Increasing the number of IoT edge devices, Side-Channel Attack has become a practical threat. This paper proposes and evaluates a countermeasure circuit against Power Analysis Attack, a type of Side-Channel Attack. Our proposal aims to achieve higher tamper-resistance reducing the area than previous work by using random values. We confirmed that the tamper-resistance of our proposal was not sufficient from our evaluation, however we got a consideration for improvement.

Keywords: Side-Channel Attack, Power Analysis Attack, Random Value

1. はじめに

近年，IoT エッジデバイスの増加に伴い[1]，サイドチャネル攻撃による情報漏えいが脅威となっている．サイドチャネル攻撃は，計算機の応答時間，消費電力，電磁波などの物理的な情報の変化を観測・解析することにより計算機内部の情報を推定する攻撃である．IoT エッジデバイスにとってサイドチャネル攻撃の脅威は通信に使用する暗号鍵が漏洩することである．暗号鍵が漏えいした場合，IoT デバイス間で通信される情報が傍受／改ざんされる恐れがある．これにより，IoT により創造されるサービスの信頼性が低下する．

2000 年に Daemen や Rijmen らにより提案され，標準アルゴリズムとなった AES 暗号がある[2]．AES は 2022 年の現在もインターネット上の通信において標準で使用されている共通鍵暗号アルゴリズムである．AES は平文・暗号文の処理単位（ブロック）を固定長で実行する．このような固定長の暗号処理方式をブロック暗号と呼ぶ．AES は処理中のデータの扱いが容易なブロック暗号であり，かつ暗号処理に算術演算を用いないことから，小規模な実装で比較的高速な暗号処理を実現できる．AES の詳細については次節で示す．

AES はサイドチャネル攻撃，特に電力解析攻撃に対して脆弱である．電力解析攻撃はサイドチャネル攻撃の一種であり，計算機の処理中に生じる消費電力の変化を観測・解析することにより内部の情報を得る．このことから，電力解析攻撃は消費電力のサイドチャネルから AES の共通鍵を推定可能であることが広く知られている[3]．

電力解析攻撃には大きく分けて 3 つの攻撃方法が存在する．単純電力解析（SPA: Simple Power Analysis）[4]，差分電力解析（DPA: Differential Power Analysis）[4]と相関電力解析（CPA: Correlation Power Analysis）[5]である．SPA は消費電力波形（トレース）をもとに特徴を視覚的に確認して内部情報を推測する攻撃方法である．暗号アルゴリズムの各処理において消費電力を計測する必要があり，また，トレースのノイズが相対的に小さいことが求められるため，AES のような軽量で高速なブロック暗号に使用することは困難である．DPA はビット遷移に着目し，特定の 1 ビットが遷移したときの消費電力の差分を解析する攻撃方法である．詳細な暗号アルゴリズムや内部実装を知る必要がないため，AES への攻撃に使われるが，多量のトレースを必要とする．CPA は DPA よりもトレースを削減して使用できる手法であり，相関係数を用いて分析し攻撃する．本研究では CPA を攻撃評価に使用する．

電力解析攻撃への対策回路は多々存在するが，代表的な 1 つとして WDDL が挙げられる[3][6]．WDDL は全体の消

1 福岡大学 工学部電子情報工学科
Fukuoka University, Department of Electronics Engineering and Computer Science

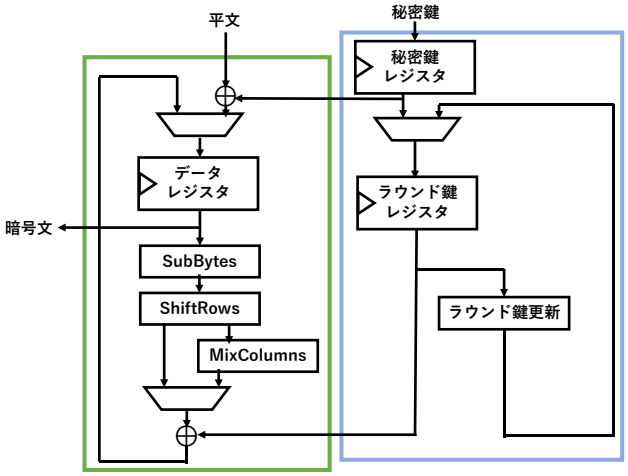

図 1　AES のハードウェア実装ブロック図

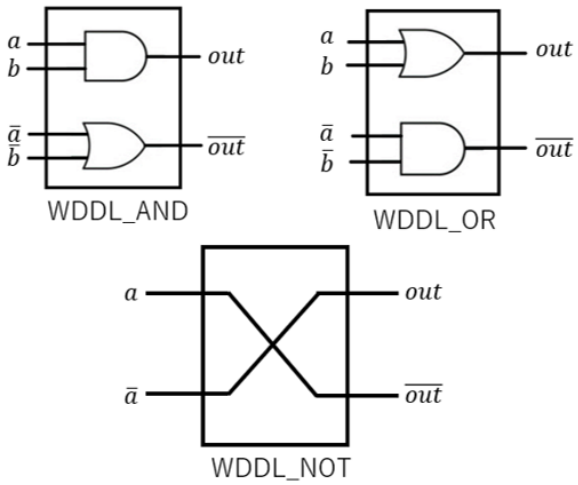

図 2　WDDL 実装時の置換素子

費電力を平滑化し，トレースから特徴を消すことで，CPA による観測対象を隠蔽（マスク）する．これにより，内部情報の漏えいを阻害する性能を耐タンパ性と呼ぶ．WDDL は耐タンパ性を向上させる一方で，消費電力を平滑化するための回路が無対策回路と比べて倍以上の面積を必要とする．

我々は WDDL と同様の着想で，省面積に耐タンパ性を実現する W-FF を提案した[7]．W-FF は，1 クロックサイクル内の前半に後半の値の反転値を強制的に入力する D-FF の出力制御を有する回路であり，既存の D-FF と置換することのみで耐タンパ性向上を実現できる．我々は，W-FF をさらに省面積に改良した FPU（Force Pull Up），FPD（Force Pull Down）を提案した[8]．FPU／FPD は W-FF と同様に 1 クロックサイクル内の前半と後半に分けて出力値を変更することで，耐タンパ性の向上を実現する．FPU は 1 クロックサイクルの前半に強制で 1 を出力し，FPD は強制で 0 を出力する．これにより，回路内ビット遷移確率を変化させるとともに，W-FF に比べ回路面積の削減を実現した．これら先行研究では，両者において実装面積は WDDL と比べ小さくなったが，耐タンパ性は WDDL と比べ低いことが確認された．

本稿は，W-FF，FPD，FPU の基本設計を活用し，電力消費のタイミングに乱数の特性を加えることにより，耐タンパ性を向上させる実装を提案し評価する．

本節では，本研究の背景を示した．2 節では，本研究の攻撃対象である AES アルゴリズムの概要について述べる．3 節では先行研究である WDDL，W-FF，FPU，FPD について示す．4 節で提案手法について説明し，5 節で評価する．最後に，6 節で本研究の結論を述べる．

2. AES

AES は 128 ビットのブロック長で処理を進めるブロック暗号である．鍵長は 128 ビット，192 ビット，256 ビットを扱うことができる．本稿の評価では鍵長 128 ビットの AES を対象とする．ブロック暗号はデータ送信者と受信者が同じ鍵（共通鍵）を用いて暗号化／復号する共通鍵暗号の 1 つであり，ブロック長に区切ったデータ単位で暗号処理を実行する．

AES では 128 ビットの入力データを 4×4 の 1 バイトの行列（ステート）で表現し，ステート内のデータを SubBytes，ShiftRows，MixColumns，AddRoundKey の 4 つの関数を用いて変形する．これら 4 つの関数を合わせてラウンド関数と呼ぶ．AES はこのラウンド関数を規定回数繰り返すことにより，暗号化／復号処理を実現する．例えば，128 ビットの鍵長の場合，16 ラウンドの繰り返しが必要となる．

SubBytes 関数の処理は S-box と呼ばれる換字処理を用いる．S-box は有限体上の逆元演算とアファイン変換を組み合わせて定義される．AES の S-box は 8 ビットの入力に対して 8 ビットが出力される関数である．このため，128 ビットの入力データを扱うためには，計 16 個の S-box を並行に動作させる必要がある．ShiftRows 関数はステートの行を巡回シフトする関数である．MixColumns 関数は定数行列をステートの列に乗算する関数である．AddRoundKey 関数は XOR による鍵加算である．このとき加算される鍵は秘密鍵ではなく，ラウンド毎に個別に秘密鍵から生成されるラウンド鍵である．

図 1 は AES のハードウェア実装におけるデータパスを示している．図の左側はラウンド関数の処理順で各関数のハードウェアが接続されている．XOR を示す⊕は AddRoundKey の処理に相当する．図の右側は秘密鍵からラウンド鍵を生成する鍵スケジュール部である．ラウンド鍵レジスタにはラウンドが進む毎に前回のラウンドと異なる値のラウンド鍵が生成される．図に示されるハードウェア実装では，ラウンド関数による暗号化は鍵スケジュールによるラウンド鍵の生成と並行に実行される．ラウンド関数は規定回数繰り返されるが，最終ラウンドのみラウンド関数内の MixColums 関数が実行されないため，ラウンド関数を実現するハードウェアには ShiftRows と MixColumns の

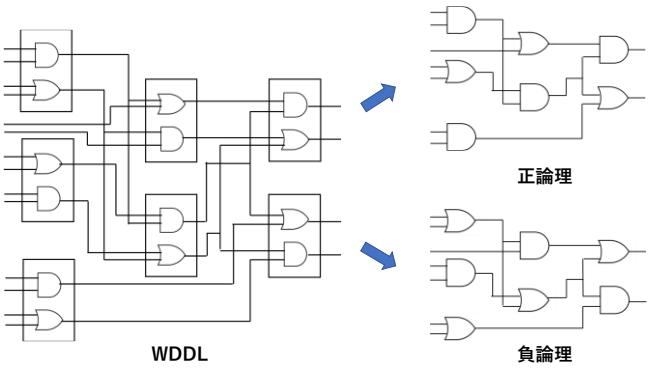

図 3　WDDL による組み合わせ回路実装の例

関数の出力を受けるマルチプレクサが存在する．

AES ハードウェアの性能は S-box の実装方法に大きく依存する．AES を実装した専用ハードウェアの中で最も大きい面積を占める回路が S-box であり，一般的には高速化のために 16 並列の S-box が実装されている．このことから，AES の専用回路の電力消費の多くが S-box 内で発生する．このため，本研究は S-box の入力を記憶するデータレジスタのフリップフロップを提案手法のフリップフロップと置き換えることにより，耐性の向上を図っている．

3. 先行研究

本節では，本稿で提案する手法の元となった先行研究について述べる．

3.1 WDDL

WDDL は全体の消費電力を平滑化することにより，消費電力のサイドチャネルから情報を消す手法である．図 2 に WDDL 設計における AND，OR，NOT の置換素子を示す．WDDL 設計は，WDDL として設計する前の組み合わせ回路の論理の中の AND，OR，NOT 素子を WDDL 用の素子に置換することによって実現される．これらを WDDL_AND，WDDL_OR，WDDL_NOT と呼ぶ．これらの素子は入力と出力の数が 2 系統存在する．例えば，WDDL_AND に注目した場合，内部は AND ゲートと OR ゲートの 2 つにより構成されている．WDDL_AND において，AND ゲートは正論理のために，OR ゲートは負論理のために用いられる．これは，正論理が電力を消費しないビット遷移の場合に負論理が電力を消費する相補の関係を構築するためである．これにより，電力の平滑化が実現できる．この平滑化を実現するために WDDL 設計では入力ビットを毎サイクル 0 に戻すプリチャージサイクルが必要となる．WDDL_OR と WDDL_NOT においても同様である．よって，WDDL は全体の消費電力を平滑化でき，CPA に対して高い耐タンパ性を示す．

図 3 に WDDL で構成した組み合わせ回路の例を示す．WDDL は図のように 2 つのゲートを内包することから，無対策回路と比べ倍の素子数が必要となり，それに比例して実装面積が増大する．本研究では，WDDL の実装面積の増大に着目する．

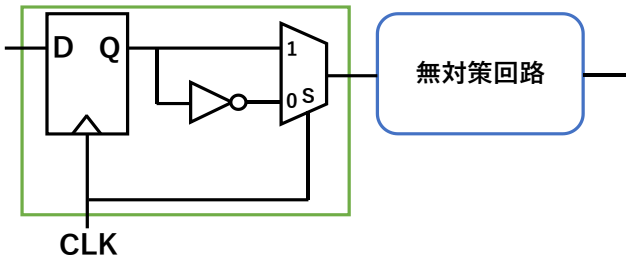

図 4　W-FF

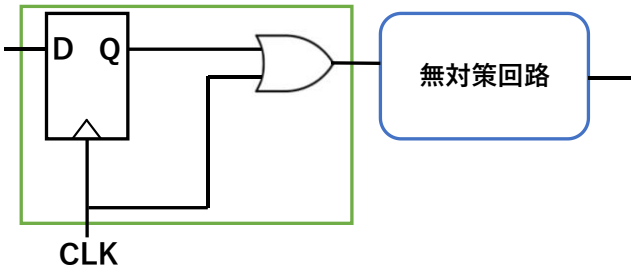

図 5　FPU

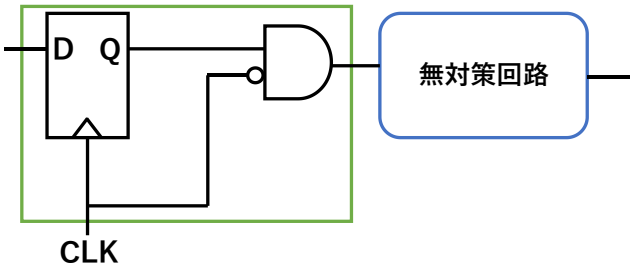

図 6　FPD

3.2 W-FF

我々はサイドチャネル対策手法として W-FF を提案した[7]. W-FF は WDDL のデュアルレールに近い効果を WDDL より省面積で得ることを目的とした耐タンパ性向上のための専用回路設計手法である. 図 4 には W-FF を用いた S-box を示す．緑の線で囲われた回路が W-FF を示し，青い角丸長方形で示された回路が無対策の S-box を示す．W-FF は D-FF の出力を 2-1 マルチプレクサに入力している．2-1 マルチプレクサは，片方に D-FF の出力(Q)を，他方に反転値が入力される．2-1 マルチプレクサの選択信号はクロック（CLK）を指定し，立ち上がりごとに反転値から交互に後続の組み合わせ回路に値を入力することで，WDDL のデュアルレールにと同じ効果を得ることを目的としている．W-FF 設計は一定の耐タンパ性の向上が確認され，かつ実装面積の削減が実現された．

3.3 FPU と FPD

我々は W-FF より省面積に実装するサイドチャネル対策回路として FPU と FPD を提案した[8]．FPU と FPD は，D-FF に論理ゲートを 1 つまたは 2 つのみ追加することで，W-FF に近い耐タンパ性をさらに省面積で実現することを目的としている．図 5 に FPU を図 6 に FPD をそれぞれ示す. FPU は D-FF と OR ゲートを組み合わせた回路であり，

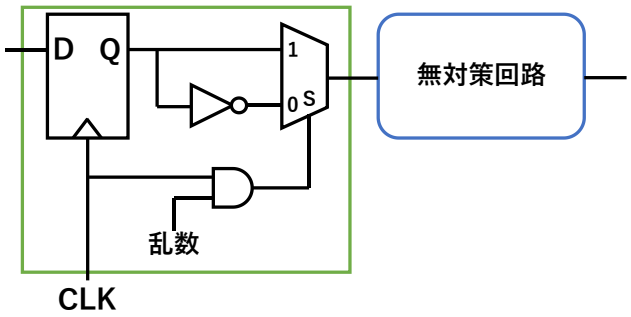

図 7　MW-FF

OR ゲートへの入力は D-FF の出力と CLK である．また，FPD は D-FF と AND ゲートを組み合わせた回路であり，AND ゲートへの入力は D-FF の出力と CLK の反転値である．このように回路を構成することで，CLK が 1 のときの無対策回路への入力を FPU の場合は 1 に，FPD の場合は 0 に強制する．これは WDDL のプリチャージサイクルから着想を得ており，D-FF の出力値のビット遷移を必ず 0 または 1 を間に入れることで，ビット遷移確率を変動させる効果を持つ．

FPU も FPD も無対策回路と比べ誤差程度の面積増加しか確認されなかった．しかしながら，耐タンパ性は W-FF と比べ低かったことから，本研究では W-FF より耐タンパ性向上が期待できる回路構成を提案する．

4. 提案手法

本節で我々は乱数を加えることにより耐タンパ性を向上させる回路として MW-FF を提案する．図 7 に MW-FF を示す．MW-FF は W-FF の回路に，AND ゲートと乱数生成器からの入力を加えた回路である．AND ゲートには CLK と乱数値が入力され，その出力はマルチプレクサの選択信号として利用される．

MW-FF では，クロック前半で W-FF における反転出力を S-box に入力する動作が常に行われなくなり，反転出力の入力が乱数により決定されることとなる．これにより，必ず反転が入力されるという W-FF の制約が無くなり，さらなる耐タンパ性の向上が期待できる．

5. 評価

5.1 実験環境

図 8 に本稿の評価環境を示す．本稿の評価では，128 ビット AES の専用回路を FPGA 上に実装した．FPGA には Xilinx 社の Spartan6 XC6SLX9 を使用した．FPGA は図中の赤い基板上の青のボード内に実装されている．図中の左上の黒い基板は USB 接続のオシロスコープであり，赤い基板のシャント抵抗の電圧を測定している．この電圧が FPGA の使用した電流値となり，消費電力波形を得ることができる．

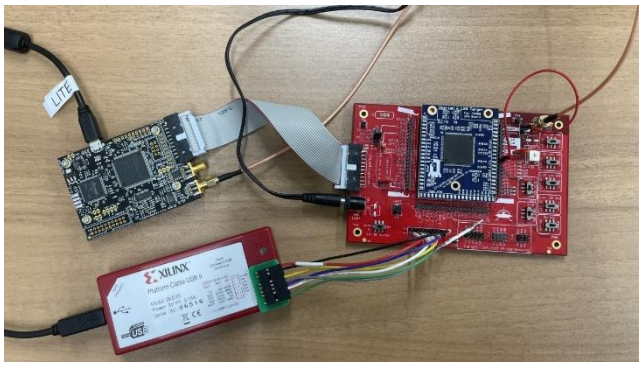

図 8　トレース計測環境

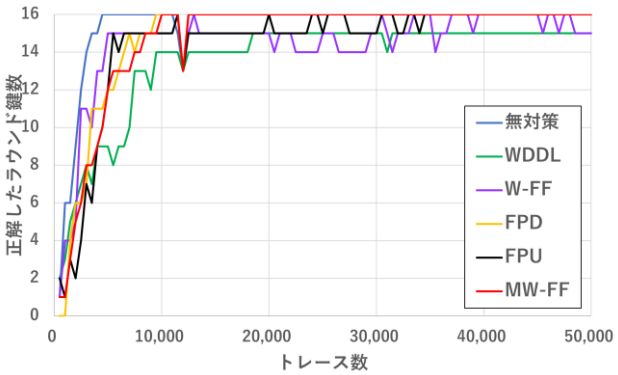

図 9　耐タンパ性

攻撃は 2 フェーズあり，最初のフェーズでは暗号化処理中の FPGA の消費電力をオシロスコープで計測することによりトレースを取得する．次のフェーズでは，取得したトレースを対象に CPA により攻撃し，秘密鍵を推定する．本稿は，各方式の耐性を評価するために，耐タンパ性の指標として，鍵の正しい推定値を求めるために必要なトレース数を求めた．このため，最初のフェーズで 50,000 トレースを取得している．攻撃は鍵の 1 バイトごとに施行され，その際，真のラウンド鍵の値と最も高い正の相関を示した値を CPA が予測したラウンド鍵とし，16 バイトの中で予測したラウンド鍵の正解のバイト数が低いほど高い耐タンパ性を示す手法とした．このとき，正解数が 16 であるならば，すべてのラウンド鍵が正しく推定されたことを示し，鍵スケジューラのアルゴリズムによりラウンド鍵から秘密鍵を復元できる．

5.2 評価結果

図 9 に耐タンパ性の評価結果を示す．図の x 軸は CPA に入力したトレース数を示し，y 軸はそのトレース数で CPA が推定したラウンド鍵の正解数を示す．赤の線が提案手法である MW-FF である．MW-FF は約 12,000 トレースを入力した時点ですべてのラウンド鍵が正しく推定され，収束している．一方，WDDL，W-FF，FPU は 12,000 トレースを超えても収束せず，MW-FF より高い耐タンパ性を持つことが示された．本研究の MW-FF は，W-FF より高い耐タンパ性を得ることを目的としているため，MW-FF の回路構成では目的が果たされていないことが確認された．

MW-FF の耐タンパ性が低かった要因として，S-box への入力値のビット遷移確率に偏りが生じたことが推測できる．このため，MW-FF の回路構成を変更し，ビット遷移確率の偏りを減少させる手法を今後提案していく．

6. おわりに

本稿では，先行研究である W-FF と FPD／FPU の耐タンパ性を上回る省実装面積の電力解析攻撃対策回路である MW-FF を提案し評価した．MW-FF は乱数値を用いることにより，耐タンパ性の向上を目的とする．しかしながら，耐タンパ性の評価で目標とした W-FF を上回ることができなかった．

本稿の評価により，MW-FF を適用した場合，S-box への入力のビット遷移確率に偏りが生じる可能性があり，それにより CPA による攻撃の成功率が向上する可能性があることが考察された．

本稿で示した MW-FF の回路構成の他にも乱数を活用する設計アプローチは存在がするため，今後は他の回路構成で，MW-FF の評価する予定である．また，本稿では回路の実装面積を評価していないため，新しい回路構成の提案とともに実装面積の評価を合わせて行う予定である．

謝辞

本研究の一部は，福岡大学の研究助成（課題番号：205008）および科学研究費補助金（研究課題/領域番号：20H00590，20K11823）の助成を受けたものです．

参考文献

[1] 総務省 情報通信白書 令和 3 年 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105220.html, (2022 年 10 月参照．)
[2] T. Jamil, “The Rijndael algorithm,” IEEE Potentials, Vol. 23, Issue 2, pp.36-38, 2004.
[3] K. Tiri and I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” Proc. of Design, Automation and Test in Europe Conference and Exhibition (DATE2004), pp. 246-251, February 2004.
[4] P.Kocher, J.Jaffe, and B.Jun, “Differential Power Analysis,” Proc. of International Cryptology Conference (CRYPO1999), Lecture Notes in Computer Science, Vol. 1666, Springer, pp. 388–397, August1999.
[5] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with A Leakage Model,” Proc. of International Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, Vol. 3156, Springer, pp. 16-29, 2004.
[6] K. Tiri et. al., “Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment,” Proc. of The annual Conference on Cryptographic Hardware and Embedded Systems 2020 (CHES 2020), pp. 354-365, 2005.
[7] Tomoaki Ukezono, "Resistance for Side-Channel Attack by Virtual Dual-Rail Effect", Proc. of 3rd International Conference on Electrical, Communication and Computer Engineering (ICECCE 2021), paper-89, Jul. 2021.
[8] Yui Koyanagi and Tomoaki Ukezono, "An Extremely Light-Weight Countermeasure to Power Analysis Attack in Dedicated Circuit for AES", Proc. of 19th International SoC Design Conference (ISOCC 2022), pp. 85-86, Aug. 2022.