偏りを有するデータセットを用いた暗号モジュールのサイドチャネル攻撃耐性評価

松林雅人[1]　ヘンドラ・グントゥル[1]　佐藤証[1]

概要：ISO/IEC 17825 はサイドチャネル攻撃への安全性において，暗号モジュールの内部データと外部で観測した動作波形に相関が見られるか，つまり内部データの情報が漏えいしているか否かをウェルチの T 検定で評価するものである．本稿ではこのモジュールの内部情報を知り得る評価者の立場を利用し，内部データのパターンに偏りを持たせることで情報が漏えいしやすい状況を作り，評価の精度を高める手法を提案した．サイドチャネル攻撃対策を施した AES 暗号回路による実験を通じて，本手法は標準の T 検定に対して 1/10 の波形数で同等の解析精度が得られるとともに，従来のサイドチャネル攻撃による安全性評価においても有効であることを示した．

Security Evaluation of Cryptographic Modules against Side-Channel Attack using Biased Data Set

MASATO MATSUBAYASHI[1]　HENDRA GUNTUR[1]　AKASHI SATOH[1]

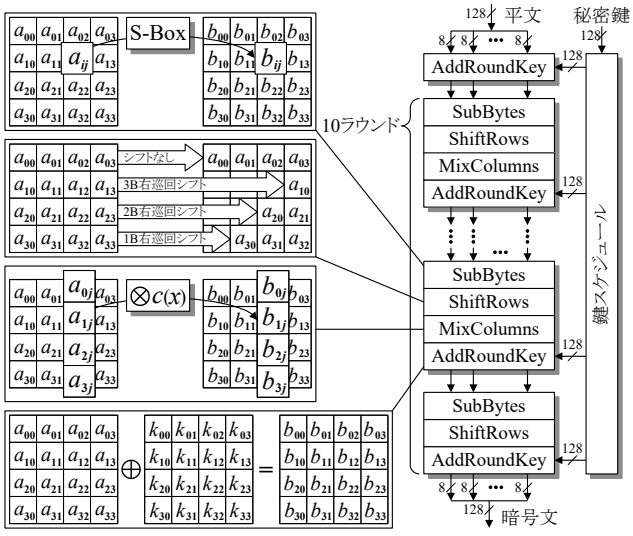
1. はじめに

我々は，暗号モジュール内部の秘密鍵を消費電力や放射電磁波等を解析して盗み出す“サイドチャネル攻撃”[1][2][3]の標準試験環境，SASEBO (Side-channel Attack Standard Evaluation Board) [4][5]および SAKURA (Side-channel AttacK User Reference Architecture) [6]ボードを用いた安全性評価の研究を行っている[7]-[11]．サイドチャネル攻撃を行う攻撃者にとって，暗号モジュールは内部状態を知ることのできないブラックボックスであるが，安全性の評価試験においては，モジュール内部の状態を利用することで効率的な解析が可能となる．2016 年に制定されたサイドチャネル攻撃に対する安全性評価手法の国際規格 ISO/IEC 17825 [12]では，暗号モジュールの内部データの情報が電力/電磁波形に漏洩しているか否かを，データと波形の相関関係としてウェルチの T 検定 [13]によって調べる．攻撃は無数の鍵候補の中から波形との相関値の高いもの調べるため，膨大な計算が必要となるのに対し，ISO/IEC 17825 の評価ではモジュールに“既知の鍵”を設定し，その一つの鍵と波形との相関を調べることにより内部データと相関のある情報が動作波形に漏れているかどうかを調べるため，通常のサイドチャネル攻撃を用いた安全性評価と比較して効率的かつ精度が高い．

ISO/IEC 17825 の安全性評価では，ランダムなデータを暗号化しているが，我々は消費電力に情報が漏洩しやすい状況を作るため，内部データのビットパターンを意図的に偏らせる手法を提案した[11]．本論文では，国際標準暗号 AES (Advanced Encryption Standard)[14]の様々な処理の過程でデータに偏りを発生し，その効果をサイドチャネル攻撃対策[15]-[19]を施した暗号 LSI [20][21]を用いて検証する．

2. AES

図 1 に 128 ビット鍵を用いた AES の暗号化処理を示す．128 ビット平文入力を 4×4 行列の 16 バイトとして構成し，SubBytes, ShiftRows, MixColumns, AddRoundKey の 4 つの基本関数を 1 ラウンドとして，10 ラウンド繰り返す．鍵スケジュール部では，各ラウンドで用いる 10 個のラウンド鍵を秘密鍵から生成する．SubBytes は 1 バイト入出力の非線形変換 S-box を 16 個集めたもので，ShiftRows は 4 バイト単位の循環シフト，MixColumns は 4 バイト単位の線形変換，AddRoundKey はラウンド鍵との XOR をとる．復号はラウンド鍵を逆順に生成しながら，各基本関数の逆関数 InvSubBytes, InvShiftRows, InvMixColumns, AddRoundKey を暗号文に施す．



[1] 電気通信大学大学院 情報理工学研究科

図 1　AES の暗号化処理

3.　T 検定

ISO/IEC 17825 のウェルチの T 検定の流れを図 2 に示す. 秘密鍵“0x0123456789ABCDEF123456789ABCDEF0”による暗号化中の電力または電磁波形を 1～10 万波形取得し, Group 1 と Group 2 に分け, 各グループをさらに Subset *A*, *B* に分けて, 次式の 2 つの T 値を計算する.

$$T_1 = \frac{\mu_{A1} - \mu_{B1}}{\sqrt{\frac{\sigma_{A1}^2}{N_{A1}} - \frac{\sigma_{B1}^2}{N_{B1}}}},\quad T_2 = \frac{\mu_{A2} - \mu_{B2}}{\sqrt{\frac{\sigma_{A2}^2}{N_{A2}} - \frac{\sigma_{B2}^2}{N_{B2}}}} \qquad (1)$$

N_A, N_B: Subset A および B のサンプル数
μ_A, μ_B: A および B の波形トレースの標本平均
σ_A, σ_B: A および B の波形トレースの標準偏差

各 T 値の符号が一致し, かつ同一時間に閾値 C を越えたとき, Subset *A*, *B* の平均と標準偏差には偶然でない相関が得られたとして, テスト結果を Fail（安全でない）とする. なお, ISO/IEC 17825 で閾値は C=4.5 で, Fail と判定された差が偶然ではない確率は 99.999%以上であるとされる.

評価に必要な波形数 $2n$ はセキュリティレベル 3 で 10,000, 上位のレベル 4 では 100,000 となっている. また, Group, Subset の波形の分け方の違いで, 6 種類の評価 Test 0~5 が定義されている. Test 1~5 は, 最初に 128 ビットが全て 0 の平文を暗号化し, 暗号文出力を次の平文入力とする処理を $2n$ 回繰り返して集めた波形を DATA-SET 1 とし, それを前後 n トレースずつに分けて Group1, 2 を作る. Test 0 では, 暗号化の途中のラウンドのどこか一ヶ所で, 次の 4 条件を満たす平文 J を n 回暗号化して DATA-SET 2 を作る.

1) ラウンド入力とラウンド出力の少なくとも 1 バイトが等しい.
2) S-box 出力の少なくとも 1 バイトが 0.
3) AddRoundKey 入力の少なくとも 1 バイトが 0.
4) 平文の少なくとも 1 バイトが 0.

Test 0~5 では次のように, トレースを Subset に分けて T 検定を行う.

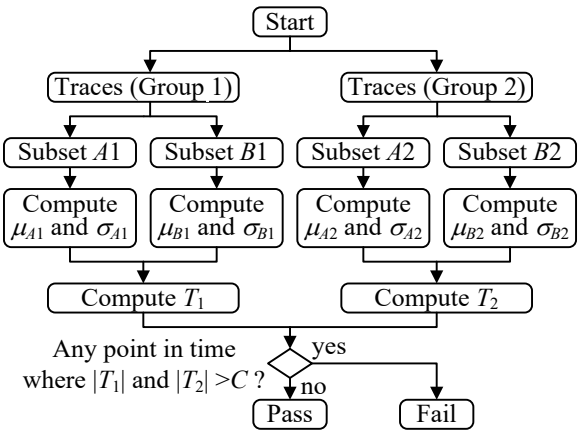


図 2　ISO/IEC17825 の T 検定の手順

- Test 0

n トレースの DATA-SET2 を前後半 n/2 ずつに分け, 前半を Subset A1, 後半を Subset A2 とする. また $2n$ トレースの DATA-SET 1 の最初の n/2 トレースを Subset B1, その次の n/2 トレースを Subset B2 とする.

- Test 1

Group1 のあるトレースが, ラウンド R (=1~10) で, ラウンド関数への入力データと出力データのビット i (=0~127) が一致すれば Subset A1 に, 不一致ならば B1 とする. Group 2 も同様に Subset A2 と B2 に分類する.

- Test 2

Group1, 2 のトレースを, ラウンド R の S-box の出力ビットが i=0 ならば Subset A1, A2, i=1 ならば Subset B1, B2 に分類する.

- Test 3

Group1, 2 のトレースを, ラウンド R の出力ビット i=0 ならば Subset A1, A2 に, i=1 ならば Subset B1, B2 に分類する.

- Test 4

Group1, 2 のトレースを, ラウンド R の出力の 0 バイト目のパターンが i (=0x00~0xff)でなければ Subset A1, A2 に, i ならば Subset B1, B2 に分類する.

- Test 5

Group1, 2 のトレースを, ラウンド R の出力の 1 バイト目のパターンが i (=0x00~0xff)でなければ Subset A1, A2 に, i ならば Subset B1, B2 に分類する.

4.　提案手法

ISO/IEC 17825 は特定のビットやバイトのパターンで, 電力/電磁波形を Group や Subset に分類しているが, 意図的にそのデータパターンを作成しているのではなく, ランダムデータである. それに対して文献[22]では, 内部レジスタの遷移ビット数（ハミング距離）が偏るように平文を操作して電磁波の信号強度の分散を偏らせ, FPGA 上の AES 回路の電磁波解析攻撃 CEMA (Correlation Electro- Magnetic Attack) [3]の S/N 比を改善している. しかし, CEMA は最終ラウンドに特化した攻撃であり, かつ簡単なサイドチャネル攻撃対策で回避できてしまう.

これに対して我々は文献[11]で, 対策済みの AES 回路を実装した暗号 LSI を用い, AddRoundKey の出力の解析対象のバイト中の 1 のビットの数（ハミング重み）を全ラウンドで順次偏らせることで, 電力波形への情報漏洩の検出に成功している. さらに, 本研究ではさらに, SubBytes, MixColumns の各出力を偏らせて, 解析精度の向上を狙うものである.

一般に, データをランダム化する暗号回路には状態遷移確立の高い XOR ゲートが多用され, 2 入力の XOR では一方の入力が 0 ならば他方の入力がそのまま, 1 ならば反転されて出力される. そこで, 解析対象のハミング重みを 0,1,7,8 となるように操作する. ハミング重みが 0 と 8 は各 1 パターン, 1 と 7 は各

8 パターンとなる. このデータパターンを解析対象の 1~10 ラウンドの中間値の全 16 バイトにランダムに適用するが, 評価者の立場で鍵を知っているので, この偏らせた中間値から入力平文を逆算している. このとき解析対象以外の 15 バイトは偏りのないランダムな値とすべきであるが, 上記のパターンをランダムに割り当てている. これは解析対象のバイトを変えたときに, そのバイトも元から偏っていれば, 既に取得した波形を再利用することで評価の作業時間(波形取得時間)を削減できるからである. つまり, 解析対象のバイトをランダムとする場合に対して, 波形数を 1/16 に抑えることができる. ただし, ISO/IEC 17825 はランダムデータを解析するため, 対象のバイトが変わっても同じ波形を用いることができる. それに対して, 提案手法は各 1~10 ラウンドで偏りを持つデータを作り, それぞれ個別に波形を取得しなければならない点に注意が必要である.

5. 提案手法による評価実験と考察

製造プロセス 90nm の COMS スタンダードセルライブラリによる暗号 LSI [20][21]上の, サイドチャネル攻撃対策 MAO (Masked AND Operation) [15], WDDL (Wave Dynamic Differential Logic) [16], MDPL [17], 疑似 RSL (Random Switching Logic)-1, 疑似 RSL-2 [18][19] を施した 5 種類の AES 暗号回路に対して評価を行った. 疑似 RSL-1 は, 本来はカスタムデザインとなる RSL セルの論理ゲートをスタンダードセルライブラリで模擬したものである. さらに疑似 RSL-2 は SASEBO-G の FPGA Xilinx Vertex-II に実装した合成体の S-box [23]による AES 回路と同等のノードを持つように制約が与えられている. これらの AES 回路は輸出制限にかからないよう, 128 ビット鍵のうち上位 72 ビットが“0x000102030405060708”に固定され, ユーザは下位 56 ビットのみ設定が可能である. そこで実験では ISO/IEC 17825 で指定された鍵ではなく, 下記の値を用いた.

0x000102030405060708090A0B0C0D0E0F

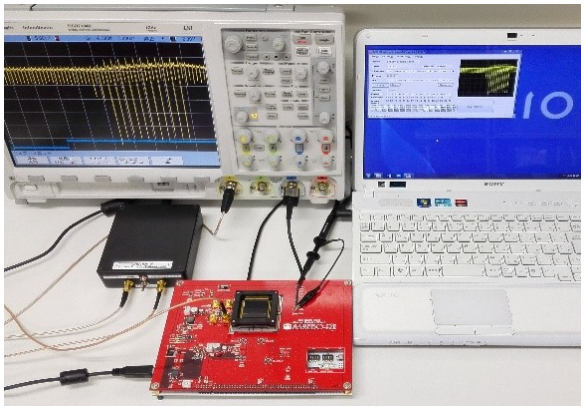


図 3 実験環境

表 1 実験の諸条件

	実験条件
AES 回路	ループアーキテクチャ, 合成体 S-box
秘密鍵	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
製造プロセス	90nm 1.0V TSMC CMOS スタンダードセル
パッケージ	160pin QFP セラミック
観測ポイント	GND 側 1Ω シャント抵抗
動作周波数	3 MHz
アンプ	Mini-Circuits ZFL-1000LN+ (20dB), ZFL-1000+ (17dB)
オシロスコープ	Agilent DSO7104B
ｻﾝﾌﾟﾘﾝｸﾞﾚｰﾄ	500MSa/s
ポイント数	5,000

図 3 に実験環境を, 表 1 に諸条件を示す. 標準評価ボード SASEBO-RII 上の暗号 LSI は PC で制御し, GND 線に挿入した 1Ω 抵抗の電圧降下として現れた電力波形を, 20dB 及び 17dB のアンプで増幅した後にオシロスコープで取得する. 解析に用いる波形数はセキュリティレベル 3 では 10,000, レベル 4 では 100,000 であるが, ノイズを低減するため, 同じ平文を 10 回暗号化し, その電力波形を平均化したものを 1 波形としている. また, データを偏らせる提案手法に対しては 10 波形を平均化した 10,000 波形, つまりレベル 3 と同様に 100,000 回計測を行っている. さらに, T 検定とは別に, 同じ波形を用いて BDPA (Bevan’s multi-bit DPA) [24]および Zero-Offset 2DPA [25]（以下, ZO-DPA), CPA (Correlation Power Analysis)[3]を行い, 鍵の導出を試みた.

図 4-1~2 は WDDL 対策済みの回路の波形を, ラウンドの特定の入出力ビットが同じかどうかで振り分ける Test 1, 図 4-3~4 は SubBytes 出力のビットで振り分ける Test 2, 図 4-5~6 はラウンド出力（AddRoundKey 出力）のビットで振り分ける, ISO/IEC 17825 の T 検定の結果である. 各テストでは, 10,000 波形のセキュリティレベル 3 と, 100,000 波形のレベル 4 の双方で評価している. 縦軸は解析対象の振り分けビットを含むラウンドごとの T 値の値で, それが横軸の時間（ラウンド）とともにどのように変化するかを示している. なお, 各ラウンドで振り分けビットの数である 128 個の T 値が計算されるが, 図では最も値の大きかったものを示している.

図 4-1~2 の Test 1 はレベル 3 も 4 も, 各ラウンドで情報漏えいを示す T 値が見られない. Test 1 はラウンドの入出力ビットが一致するかしないという, つまり中間値レジスタの特定ビットが遷移するかしないかというハミング距離モデルに基づく解析である. 対策が施されていない回路であれば, レジスタの遷移によって, 組み合わせ回路が動作して消費電力が変動するが, WDDL では組み合わせ回路の状態をレジスタとは無関係にリセットするため, 常に消費電力が発生し, その動作はハミング距離モデルと合致しないことが漏えい情報を検知できなかった理由である. なお, 11 ラウンド目に T 値のピークが見られるが, これは最終ラウンドで出力する暗号文は隠す必要がなく, そのまま出力レジスタに保持されるためと考えられる.

図 4-3~4 の Test 2 で, 10,000 波形のレベル 3 は, T 値に絶対値が 4.5 以上のピークが見られないが, 100,000 波形のレベル 4 では各ラウンドでピークが検出されている. なお,

1 ラウンドに 2 つのピークが見られるが, これは 2 線方式の回路を用いる WDDL で, 演算時の放電と, 準備時の充電の双方で情報が漏洩しているためである. 2 線方式は入力信号が 0 か 1 かにかかわらず相補型に組み合わせられた回路が動作する仕組みであるが, 消費電力を常に一定とするためには, 2 線入力に対して対称に作られた専用のライブラリを用い, かつ信号配線も注意深くバランスするようにレイアウトしなければならない. 今回の実験の AES 回路はスタンダードセルライブラリで製造され，論理的には 2 線が対称に動作するものの，実際には信号が 0 か 1 かによって消費電力に僅かな差が生じる．このため，多くの波形を集めて解析することで, その僅かな差を検出することができる. 図 5-1 は SubBytes 出力のビットパターンを偏らせた提案手法であり, レベル 3 では検出できなかったとリーク情報を，レベル 4 の 1/10 の 10,000 波形で検出に成功していることがわかる.

図 4-5~6 は，ラウンド出力のビットで振り分ける Test 3 の結果であるが, 今回の AES 回路は 4 つの基本関数をまとめたラウンド関数ブロックを繰り返し実行するループアーキテクチャを採用しており，図 1 にも示したように，AddRoundKey がラウンド出力となっている. AddRoundKey 出力は次のラウンド処理の入力となって電力波形に影響を及ぼすため，その出力ビットで振り分ける場合，T 値のピークは 1 ラウンド遅れる点に注意が必要である．レベル 3 も 4 も T 値にピークが検出されているが，図 5-2 の提案方式は，Test 2 と同様にレベル 4 と同じ高いピークが 1/10 の波形で検出できていることがわかる.

図 5-3 は MixColumns の出力を偏らせた本手法による解析結果で，各ラウンドで T 値に大きなピークが見られる. このように ISO/IEC 17825 のテストで定義されていない中間値でも情報漏えいの検出が可能である．また図 5-1~3 からわかるように，T 値のピークの強さは解析する中間値の場所によって異なるため，アルゴリズムに応じてその基本関数の出力を調べることも，より確実な安全性評価には重要である.

上記の T 検定で用いた WDDL 対策済み AES 回路の 4 種類の波形に対し, 最終ラウンド(10 ラウンド)の SubBytes 入力（第 9 ラウンドの AddRoundKey 出力）のデータを選択関数として解析する BDPA によるサイドチャネル攻撃を行った結果を図 6-1~4 に示す. T 検定では秘密鍵を求めることが目的ではなく, 各ラウンドの内部データと波形に相関があるかどうか, つまり情報漏えいの可能性を調べるものである. これに対して BDPA は最終ラウンドの波形と相関の高い鍵を導出するものである. グラフは, 16 個の正しい部分鍵（バイト）の相関値が 256(=2^8)個の部分鍵候補の中で何番目に高いかを, 波形数の増加とともにそれぞれ示している. 16 本の線が全て一番上に達した段階で, 秘密鍵の全 16 バイトが求まったことになる. もちろん, 一番上でなくとも上位に位置した部分鍵は情報が漏れていることを意味する.

図 6-1 は ISO/IEC 17825 の T 検定に用いたランダム平文入力で, 4,500 波形程度でほぼすべての鍵バイトが求まっていることがわかる. それに対して提案手法で AddRoundKey 出力（SubBytes 入力）を偏らせた波形を用いた図 6-3 の攻撃では, 1,000 波形も要さずに全ての鍵が求まっており, サイドチャネル攻撃対策を施した回路においても, データを偏らせることの有用性が示された. なお, ZO-DPA は MDPA と同様の結果が得られている.

なお, 第 9 ラウンドの SubBytes, MixColumns 出力を偏らせた図 6-2 と 6-4 では精度が上がっていない. MixColumns が悪くなる理由は不明であるが, 選択関数で解析している場所と異なるデータを偏らせても意味はなく, アルゴリズムや実装法を十分に検討する必要がある. そのような検討を必要としない T 検定は, 情報漏えいの可能性の有無を調べる手法として非常に優れた手法である.

CPA による解析では，ランダムおよび偏りを持ったデータのいずれも鍵を導出することはできなかった．CPA は第 9 と第 10 ラウンドの出力のハミング距離を選択関数としているが，これは中間値を保持するレジスタのデータのスイッチングと消費電力に相関があるというモデルである．しかし，WDDL は内部の組み合わせ回路を一旦リセットするので, ラウンド間の状態遷移でこのモデルが成り立たない. これは，中間値の特定のビットの遷移を調べる Test 1 の T 検定でも情報漏えいが検出できなかったことと合致する結果である.

以上のように，ISO/IEC 17825 の T 検定は暗号回路の任意の中間値に対して，その情報が動作波形へ漏えいする可能性を簡単に調べることができ，サイドチャネル攻撃のように暗号アルゴリズムを調べて攻撃方法を検討する必要はなく汎用性が高い．また，中間値のデータパターンを偏らせる本手法は，その解析精度を大幅に向上させ，サイドチャネル攻撃対策 WDDL を実装した AES 回路に対しても有効でることが示された.

6. むすび

本稿では，ISO/IEC 17825 の T 検定において，解析対象とするデータのハミング重みを偏らせることで，漏えい情報の検出精度を向上させる手法を提案し，サイドチャネル対策 WDDL を施した AES 回路を用いてその有効性を検証した．その結果，ランダムなデータを用いた T 検定に対して, 提案手法は 1/10 の波形数で同じ精度が得られることが示された．また，サイドチャネル攻撃においてもデータを偏らせることで，鍵導出に必要な波形数を大幅に削減することが可能となった．ただし，それはあくまで安全性評価試験としての，暗号回路の内部状態を全て把握可能な条件下での解析である．従って，あくまで情報漏えいの可能性の検査であり，内部状態にアクセスできない攻撃者が解読可能になる意味ではない．逆に，そのような条件下でも情

報の漏えいが検出されなければ，サイドチャネル攻撃に対する高い安全性を有しているということが言える．

本稿では，WDDL に対する提案手法の有効性を示したが，今後は他の対策を施した暗号回路に対してもその有効性を検証していくとともに，さらなる精度向上についても検討を進めていきたい．

参考文献

[1] P. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” CRYPTO ’96, LNCS 1109, pp. 104-113, Aug. 1996.

[2] P. Kocher, et al., “Differential power analysis,” CRYPTO ’99, LNCS 1666, pp. 388-397, Aug. 1999.

[3] E. Brier, et al., “Correlation power analysis with a leakage model,” CHES 2004, LNCS 3156, pp. 16–29, Aug. 2004.

[4] 佐藤証，他，“暗号モジュールの安全な実装を目指して －サイドチャネル攻撃の標準評価環境の構築－”, Synthesiology, vol. 3, no. 1, pp. 56-65, Apr. 2010.

[5] 産業技術総合研究所, “Evaluation Environment for Side-channel Attack”. https://www.risec.aist.go.jp/project/sasebo/#

[6] “SAKURA Hardeware Security Project”. http://satoh.cs.uec.ac.jp/SAKURA/index.html

[7] H. Guntur, et al., "Side-channel AttacK User Reference Architecture SAKURA-G,” GCCE2014, SS-CBS-1, Oct. 2014.

[8] M. Matsubayashi, et al., “Side-channel AttacK User Reference Architecture Board SAKURA-W for Security Evaluation of IC Card,” GCCE2015, SS-RSE-1, Oct. 2015.

[9] M. Matsubayashi, et al., “Clock Glitch Generator on SAKURA-G for Fault Injection Attack Against a Cryptographic Circuit,” GCCE2016, OS-CBS-1, Oct. 2016.

[10] Y. Nomata, et al., “Comparison of Side-Channel Attacks on Cryptographic Circuits Between Old and New Technology FPGAs,” GCCE2016, OS-ONS-6, Oct. 2016.

[11] ヘンドラ・グントゥル，他，“ISO/IEC 17825 による暗号回路の電力解析に対する安全性評価と偏りを有するデータセットを用いた解析精度の向上”， SCIS2017, 3C3-3, 2017 年 1 月.

[12] ISO/IEC 17825:2016, Information technology -- Security techniques -- Testing methods for the mitigation of non-invasive attack classes against cryptographic modules, Jan. 2016.

[13] G. Goodwill, et al., “A Testing Methodology for Side-Channel Resistance Validation,” NIAT 2011, Sep. 2016. http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/08_Goodwill.pdf

[14] NIST, “Advanced Encryption Standard (AES),” FIPS-197, Nov. 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pd

[15] E. Trichina, “Combinational Logic Design for AES SubByte Transformation On masked Data,” Cryptology ePrint Archive, 2003/236, Nov. 2003.

[16] K. Tiri， et al., “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” Proc. DATE 2004, pp. 246-251, Mar. 2004.

[17] T. Popp， et al., “Masked Dual-Rail Pre-charge Logic: DPA-Resistance without Routing Constraints,” CHES 2005, LNCS 3659, pp. 172-186, Sep. 2005.

[18] D. Suzuki, et al., “Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level,” IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, vol. E90-A, no. 1, pp. 160-168, Jan. 2007.

[19] M. Saeki, et al., "A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques," CHES 2009, LNCS 5747, pp. 189-204, Sep. 2009.

[20] RCIS, “ISO/IEC 18033-3 Standard Cryptographic LSI ~ with Side Channel Attack Countermeasures ~ Specification - Version 1.0 -,” Sep. 2009. https://www.risec.aist.go.jp/project/sasebo/download/CryptoLSI2_Spec_Ver1.0_English.pdf

[21] Yokohama National University Information and Physical Security Research Group, “Cryptographic Circuits with Logic Level Countermeasures against DPA” http://ipsr.ynu.ac.jp/circuit/index.html

[22] 嶋田晴貴，他，“選択したデータセットを用いた暗号デバイスの電磁情報漏えいの効率的な安全性評価”，信学論, vol. J96-B, no. 4, pp. 467-475, 2013 年 4 月.

[23] A. Satoh, et al., "A Compact Rijndael Hardware Architecture with S-Box Optimization," ASIACRYPT 2001, LNCS 2248, pp. 239–254, Dec. 2001.

[24] R. Bevan，et al., “Ways to Enhance DPA,” ICISC 2002, LNCS 2587, pp.32342, Dec. 2003.

[25] J. Waddle，et al., "Towards Efficient Second-Order Power Analysis," CHES 2004, LNCS 3156, pp 1-15, Aug. 2004.

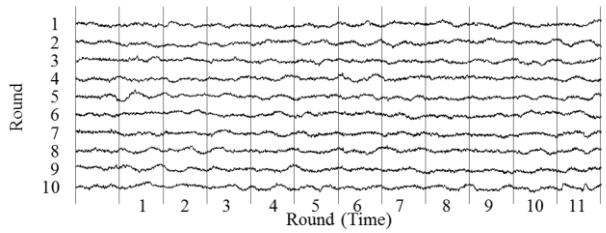


図 4-1 WDDL の Test1 (入出力ビットの一致)による T 検定 (Level 3)

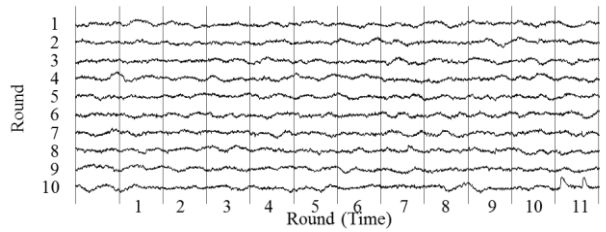


図 4-2 WDDL の Test1 (入出力ビットの一致)による T 検定 (Level 4)

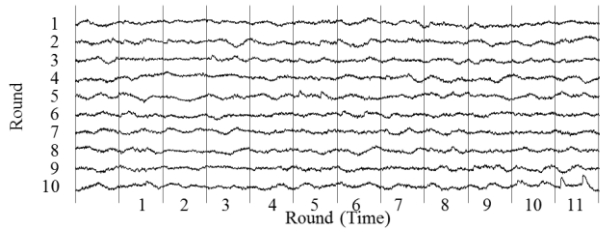


図 4-3 WDDL の Test2 (SubBytes 出力)による T 検定 (Level 3)

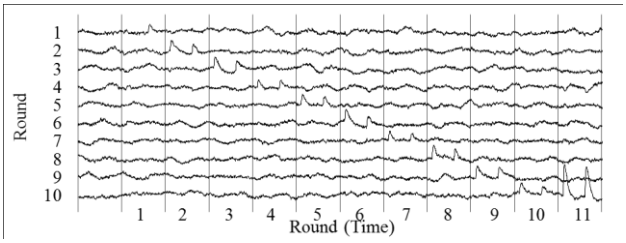


図 4-4 WDDL の Test2 (SubBytes 出力)による T 検定 (Level 4)

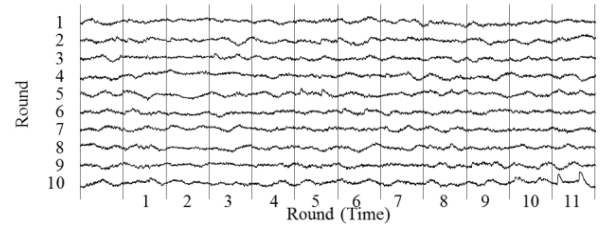


図 4-5 WDDL の Test3 (AddRoundKey 出力)による T 検定 (Level 3)

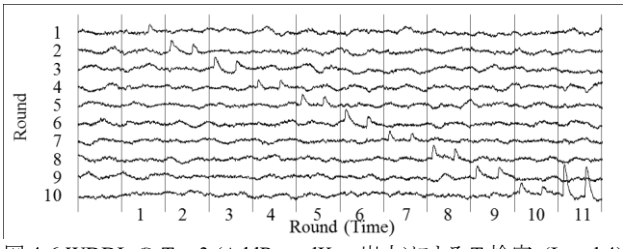


図 4-6 WDDL の Test3 (AddRoundKey 出力)による T 検定 (Level 4)

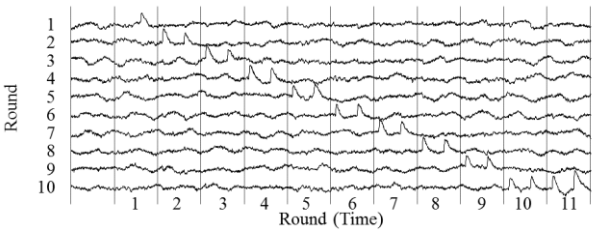


図 5-1 WDDL の本手法(偏らせた SubBytes 出力)による T 検定

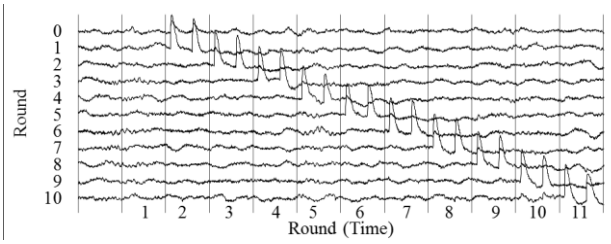


図 5-2 WDDL の本手法(偏らせた AddRoundKey 出力)による T 検定

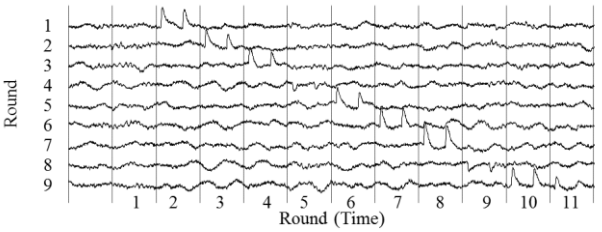


図 5-3 WDDL の本手法(偏らせた MixColumns 出力)による T 検定

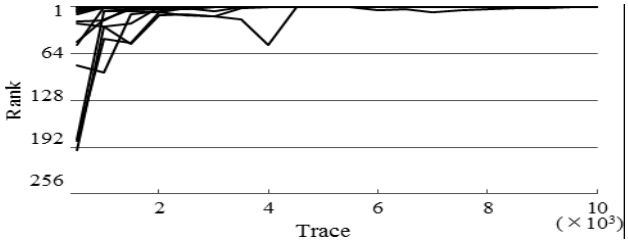


図 6-1 WDDL の BDPA 結果

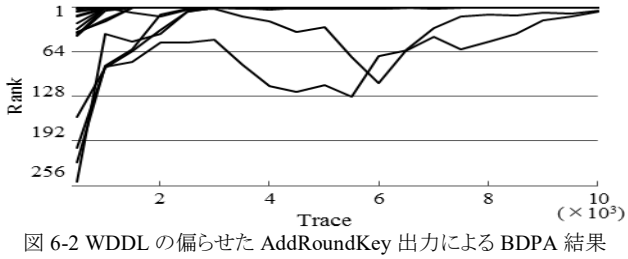


図 6-2 WDDL の偏らせた AddRoundKey 出力による BDPA 結果

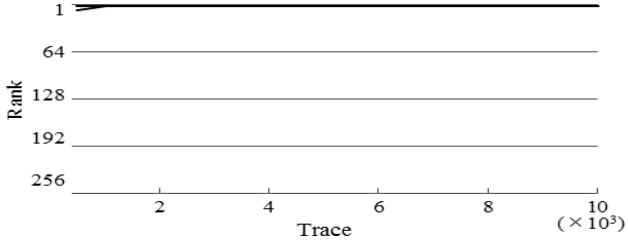


図 6-3 WDDL の偏らせた SubBytes 出力による BDPA 結果

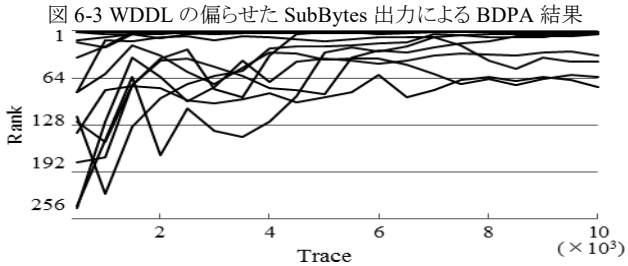


図 6-4 WDDL の偏らせた MixColumns 出力による BDPA 結果