平成 28 年度修士論文

# 暗号ハードウェアに対する物理攻撃の安全性評価手法の研究

電気通信大学情報理工学研究科
情報・通信工学専攻
コンピュータサイエンスコース

学籍番号：1531089
氏名　　：ヘンドラ･グントゥル
指導教員：佐藤 証 教授

# 要旨

高性能な情報機器とブロードバンドネットワークの普及により，暗号技術の利用が急速に拡大している．従来，暗号はアルゴリズムの理論的な安全性の研究が中心であったが，現在は暗号をソフトウェアやハードウェアとして実装した“暗号モジュール”の物理的な弱点を突く攻撃に対する安全性の研究が活発化している．本研究では，暗号モジュールの演算中の消費電力・放射電磁波・演算時間等を解析してそこに漏洩している秘密情報を抜き出すサイドチャネル攻撃を対象としている．

サイドチャネル攻撃に対する安全性評価手法の国際標準 ISO/IEC 17825 が 2016 年 1 月に制定された．その中で共通鍵暗号の漏洩情報の検出には，既知の内部状態に基づいて分類した電力や電磁波形とランダムな波形の間で，平均や標準偏差に有意な差があるかどうかをウェルチの T 検定で調べる手法が用いられる．本研究では，CMOS スタンダードセルライブラリで製造された暗号 LSI 上の様々な AES 回路に対して，この T 検定を実行し，その有効性を検証した．さらに，内部変数データのハミング重みを意図的偏らせて漏洩情報を強調する手法を導入し，T 検定の精度を向上させられることを示した．通常のサイドチャネル攻撃では攻撃者は内部状態を直接観測したり制御することはできないが，安全性評価という観点から，暗号モジュールの開発者や評価者がそれらを自由に設定することができる．つまり，そのような条件で漏洩情報が検出された場合，それが直ちに安全上の問題となるのではなく，漏洩する可能性のあることを意味している．逆にこのように極めて有利な条件による解析で漏洩情報が得られなければ，その暗号モジュールは非常に高い安全性を有しているということになる．本研究の手法は，通常のウェルチの T 検定よりもさらに有利な条件を与えるもので，それにより少ない波形で高い精度で漏洩情報が検出でき，つまりサイドチャネル攻撃に対する安全性評価のコストを大幅に削減するものである．

目次

# 1 序論

暗号はデジタルデータの秘匿や改ざん防止等に不可欠な基盤技術であり, デジタル情報機器や家電製品への組み込みが進んでいる. それにより従来は論理的な解析が中心であった暗号への攻撃，つまり安全性評価手法の研究は物理的なものへと広がってきた. 暗号をソフトウェアやハードウェアで実装したものを総称して暗号モジュールと呼ぶ, 1996 年に登場したサイドチャネル攻撃は[1][2]その暗号モジュールの動作中の物理情報である消費電力，電磁波，処理時間等を測定し，そこに漏れているモジュール内部の動作情報（以下，サイドチャネル情報）を解析し，暗号の秘密鍵を盗み出すものである. サイドチャネル攻撃は数十万円のオシロスコープと PC 等で実行できるため，暗号モジュールへの対策技術の実装とその安全性の検証が重要である.

暗号モジュールの物理的な安全性評価の国際標準として, ISO/IEC 19790 および 24759 [3][4]が標準化されていたが，2016 年に新たにサイドチャネル攻撃に対する安全性評価手法の国際標準 ISO/IEC 17825 [5]が制定された. サイドチャネル攻撃は，外部から観測したサイドチャネル情報から秘密鍵を求めるのに対し，ISO/IEC 17825 は秘密鍵を知った上で，それに依存したサイドチャネル情報が洩れているかどうかを確認する. 前者は多数の鍵候補と多数の波形データとの相関を調べるため, 膨大な計算量が必要となるが, 後者は鍵が既知である条件下での評価のため計算量が大幅に削減される. 共通鍵暗号に対する評価は，電力波形や電磁波形を既知の内部状態に応じて二つの母集団に分け，ウェルチの T 検定（以下，T 検定）を用いてその平均や分散に有意な差があるかどうかを調べるものである[6].

本研究では，T 検定を用いた安全性評価手法有効性を，サイドチャネル攻撃の研究の標準ボードとして用いられている SASEBO (Side Channel Attack Standard Evaluation BOard) シリーズ[7]の SASEBO-RII および，それを引き継いだ SAKURA (Side-Channel AttacK User Reference Architecture)シリーズ SAKURA-G を用いて検証する. 実験には共通鍵暗号の国際標準暗号 AES (Advanced Encryption Standard) [8]を様々なサイドチャネル攻撃対策[9][10][11][12][13]を施して実装した回路を用いる. また，サイドチャネル情報を含む電力波形や電磁波形は，演算時のトランジスタのスイッチングによって生じ，それは演算中のデータに依存する. そこで, 暗号処理中のデータのビットパターンに偏りを持たせることで, 内部動作に関する情報が消費電力や電磁波に漏れやすい状況を意図的に作り，その漏洩情報を解析することで解析の精度を向上させる手法を提案し，その有効性を検証する.

本研究は，以下のように構成されている.

第 2 章は，本研究に関連する技術について述べる. まず，SASEBO と SAKURA の両プロジェクトについて説明する. また，今回解析対象とした AES のアルゴリズムを示す. そして，物理攻撃の概要とサイドチャネル攻撃への回路の対策について述べた後,

ISO/IEC 17825 で採用された T 検定による安全性評価方法について詳解する．

第３章は，偏りを持たせたデータの生成法について述べた後，それを SAKURA-G 上の FPGA に実装した AES 回路で処理させ，その電力波形を用いた T 検定の精度がランダムなデータを処理した場合に対してどのように変化するかについて比較・考察する．

第４章は，様々なサイドチャネル攻撃対策を施した AES 回路を実装した暗号 LSI で偏りを有するデータを処理させ，その電力波形を SASEBO-RII で測定し，ランダムデータによる T 検定との比較を行う．また，同じ電力波形が T 検定にとどまらず様々なサイドチャネル攻撃にも有効であることを示す．さらに T 検定とサイドチャネル攻撃の結果の関係について考察し，T 検定では平均・標準偏差といった数値による安全性の判定だけでは不十分であり，その挙動についての検討の必要性についても指摘する．

第５章では，本研究で得られた知見を基に，全体の総括を行う．

# 2　関連技術

本章では, サイドチャネル攻撃の標準評価環境の構築を目的とした SASEBO プロジェクトおよび，それを引き継いだ SAKURA プロジェクトを紹介した後，本研究の実験でターゲットとした暗号 AES のアルゴリズムを示す．その後，サイドチャネル攻撃の概要と実験で用いた AES 回路に施した対策手法について述べる. さらに ISO/IEC 17825 の T 検定を用いた評価手法を説明する.

## 2.1　SASEBO プロジェクト

サイドチャネル攻撃の標準評価環境を構築し, 安全性評価の国際標準化に貢献するため，2007 年に産業技術総合研究所は SASEBO プロジェクトを立ち上げた[7]．それ以前は各研究機関が独自の実験環境を用いたため, 第三者による追試や検証が困難であった. SASEBO プロジェクトでは異なるハードウェアプラットフォームの評価を行うため, 下記のような様々なボードが開発・事業化された．標準ボードとして，国内外の 100 を超える研究機関に対して，累計で 1,000 枚以上出荷され当該研究が急速に発展した.

- SASEBO-B　　: Altera 社製 FPGA Stratix-II を搭載.
- SASEBO-G　　: Xilinx 社製 FPGA Virtex-II Pro を搭載.
- SASEBO-GII　　: Xilinx 社製 FPGA Virtex-V を搭載.
- SASEBO-W　　: IC カード評価用.
- SASEBO-R　　: 専用暗号 LSI 実験用.
- SASEBO-RII　　: 専用暗号 LSI 実験用．SASEBO-W のドータボード.

本研究で用いた SASEBO-RII の外観を図 2.1 に示す．SASEBO-RII は，SASEBO-W のドータボードとして専用の暗号 LSI を搭載する.

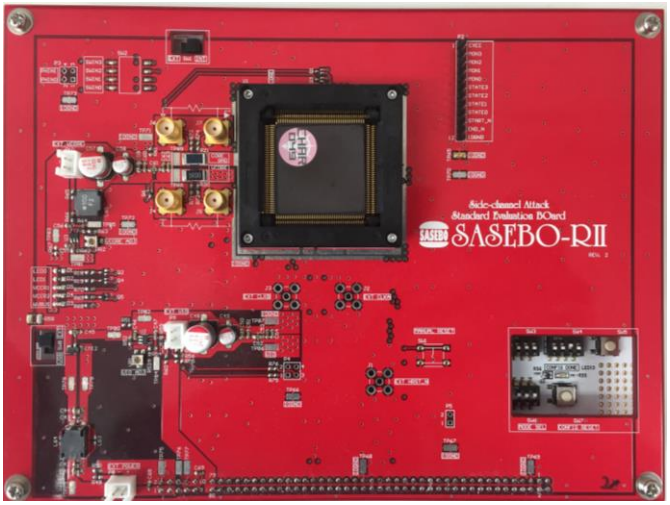


図 2.1　SASEBO-RII の概観

## 2.2 SAKURA プロジェクト

SASEBO プロジェクトは 2012 年に終了し, それに伴い SASEBO ボードの製造も中止された. しかし, その後さらにサイドチャネル攻撃の研究が活発になり, 安全性評価ボードの復活を求める声が絶えなかった. そこでため, 最も普及していた SASEBO-GII の後継機種として新たに Xilinx 社の FPGA Spartan-6 を搭載した図 2.2 の SAKURA-G ボードが新たに開発され, 電気通信大学と森田テックは 2013 年に SAKURA プロジェクトを立ち上げた. SAKURA-G は SASEBO-GII ボードの後継機として高い互換性を保ちながら, 速度・回路規模・ノイズ特性等の性能を大幅に向上させたものである.

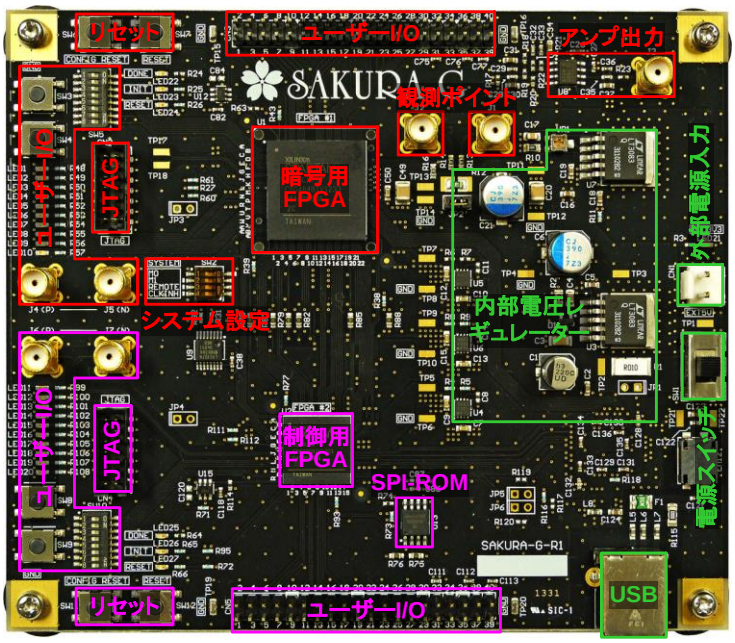


図 2.2 SAKURA-G の概観

## 2.3 Advanced Encryption Standard (AES)

共通鍵暗号は暗号化と復号で同じ秘密鍵を利用するもので, データを固定長のブロックに区切って処理するものを共通鍵ブロック暗号と呼ぶ. AES[8]は, 2000 年に米国国立標準技術研究所 NIST (National Institute of Standards and Technology)が米国連邦標準 FIPS-197 (Federal Information Processing Standard) として採用した共通ブロック鍵暗号で, その後 ISO/IEC 18033[18]としても国際規格化されている. AES のブロック長は 128bit (16Byte)で, 鍵長は 128, 192, 256 bit (16, 24, 32Byte) と可変である. 図 2.3 は本研究の実験対象とした 128bit 鍵長の AES の暗号化のアルゴリズムである. 入力された 128bit のブロック（平文と呼ぶ）を 4×4Byte に構成, ラウンド関数と呼ばれるランダム化関数を 10 回施して 128bit の暗号文に変換する. ラウンド関数は SubBytes, ShiftRows, MixColumns, AddRoundKey の 4 種類の基本演算で構成され, AddRoundKey では秘密鍵から順次生成されるラウンド鍵が用いられる. この基本演算を以下で詳解する.

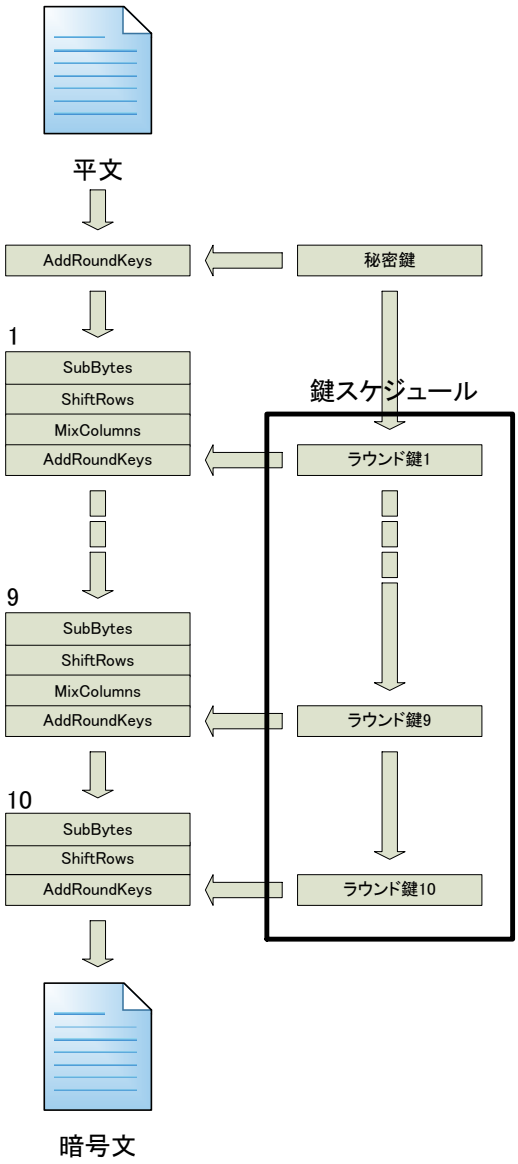


図 2.3　AES の暗号アルゴリズム

- SubBytes

SubBytes のアルゴリズムを図 2.4 に示す．入力の各バイト$\boldsymbol{a_{i,j}}$は非線形変換 Sbox で$\boldsymbol{b_{i,j}}$に変換される. Sbox はガロア体GF$(2^8)$上の逆変換の後, 次式のアフィン変換を行う.

$$\begin{bmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{bmatrix}\begin{bmatrix}x_0\\x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\end{bmatrix}+\begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix} \tag{2.1}$$

8bit 入出力の Sbox の変換値を表 2.1 に示す. 行は上位 4bit を, 列は下位 4bit を表す.

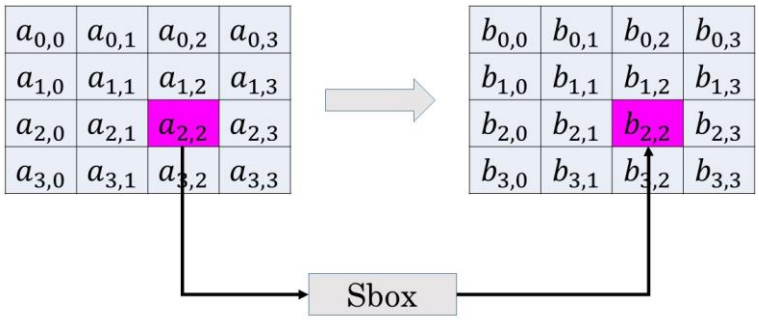


図 2.4　SubBytes

表 2.1　Sbox の変換値テーブル

| | | 下位 4 ビット | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 下位 4 ビット | 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| | 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| | 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| | 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| | 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| | 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| | 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| | 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| | 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| | 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| | A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| | B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| | C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| | D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| | E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| | F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

- ShiftRows

ShiftRows は図 2.5 のように各行に対して循環シフトを行う．

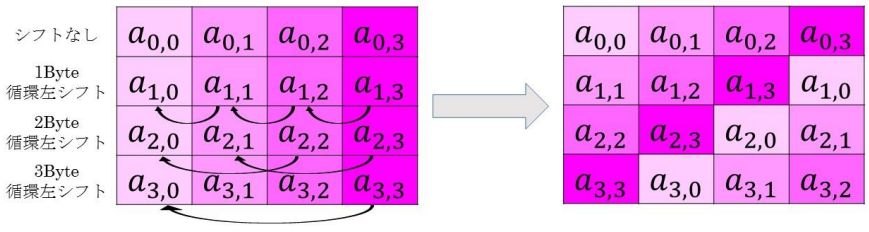


図 2.5　ShiftRows

- MixColumns

MixColumns は式(2.2)をよび図 2.6 に示すように，各列に対する線形変換である．

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \tag{2.2}$$

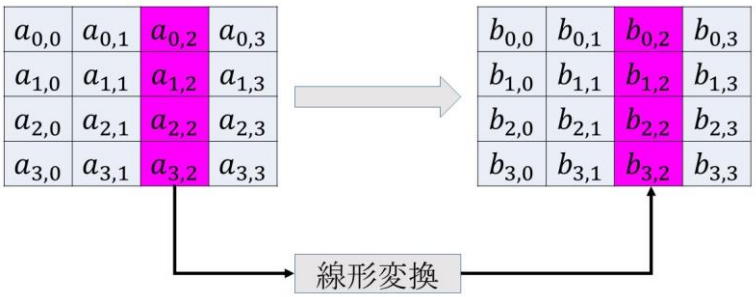


図 2.6　MixColumns

- AddRoundKey

  AddRoundKey は図 2.7 に示すように，128bit のデータと 128bit のラウンド鍵の XOR である．

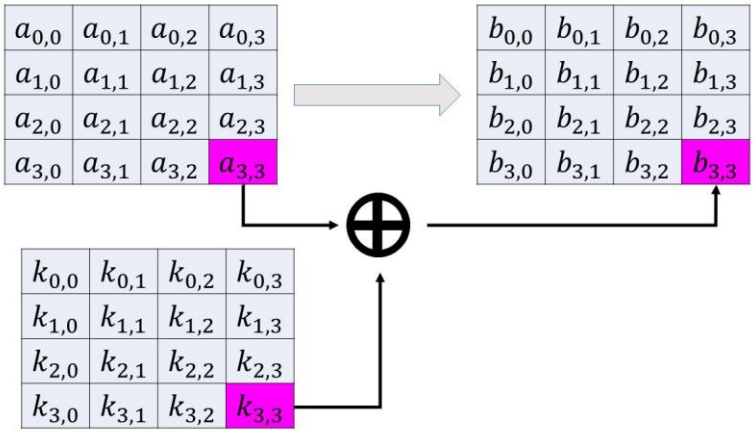

図 2.7　AddroundKey のアルゴリズム

- 鍵スケジュール

  鍵スケジュールを図 2.8　鍵スケジュールに示す．4×4Byte に配置された前ラウンド鍵$a_{i,3}(0 \le i \le 3)$（初期値は秘密鍵）を 1Byte 左に循環シフトし，各 Byte に対して Sbox 変換を施す．その結果と前ラウンド鍵$a_{i,0}(0 \le i \le 3)$，そして表 2.2 に示した Rcon を XOR して次のラウンド鍵$a_{i+1,0}(0 \le i \le 3)$とする．

表 2.2　Rcon の値

| | ラウンド | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **Rcon** | 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1B | 36 |
| | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

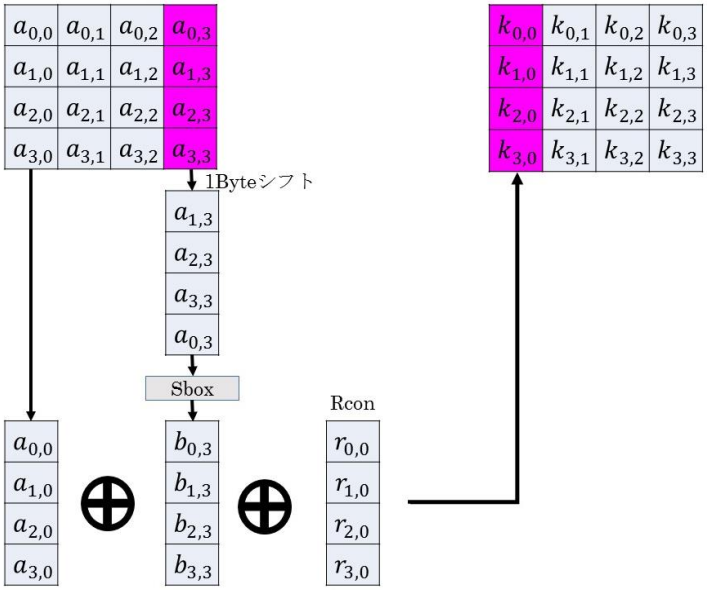


図 2.8　鍵スケジュール

## 2.4　物理攻撃

1996 年に登場したサイドチャネル攻撃を契機に, 様々な物理攻撃手法が考案された. 図 2.9 に物理攻撃の分類を，また表 2.3 に暗号モジュールへの操作の分類[19]を示す.

物理攻撃は，暗号モジュールの破壊・変形を伴うか否かによって侵入型攻撃と非侵入型攻撃に大別される．侵入型攻撃は暗号モジュールを分解・切る・溶かすなどにより外装を破壊し，電子顕微鏡や内部信号を読み出すプローブなどを通して，内部情報の観察および改変を行う攻撃である．一方，非侵入型攻撃は暗号モジュールを破壊・変形することなく内部情報を取得する攻撃方法で, 暗号モジュールにノイズ等を印加することにより誤作動を誘発して，本来は出力されない内部情報を利用するフォールト攻撃と，暗号処理中の電力・電磁波・処理時間などに漏洩する内部動作情報を解析するサイドチャネル攻撃に分類される．本研究ではこのサイドチャネル攻撃を対象としている．

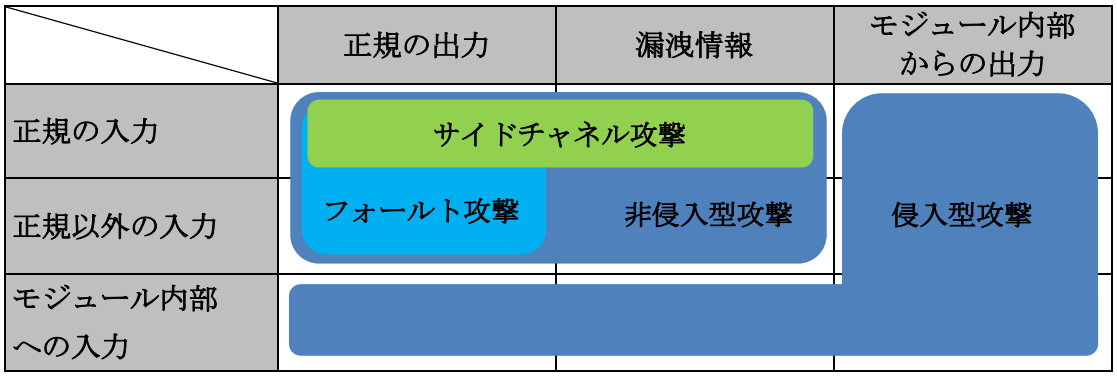


図 2.9　攻撃に利用する入力による攻撃手法の分類

表 2.3　暗号モジュールへの操作分類

| | | 内容 | 具体例 |
|---|---|---|---|
| 入力 | 正規の入力 | 正規 I/O から想定された信号入力 | 各種データポートからの入力，キーパッドからの入力等 |
| | 正規以外の入力 | 正規 I/O からの規格外の信号入力，およびモジュールの変形を前提としない信号やエネルギーの注入 | 規格外の電圧の信号，規格外の周波数の信号モジュール外から電界，磁界，電磁波，放射線等を照射 |
| | モジュール内部への入力 | 狭義タンパ―手段に基づくモジュールの変形を前提として入力される信号 | プローブ用ニードリによるターゲットへの直接信号入力<br>ターゲットへの光・電磁波，分子線，イオン線の直接照射等 |
| 出力 | 正規の出力 | 正規 I/O からの想定された信号出力 | 各種データポートからの出力，液晶パネルやディスプレイへの表示，音の出力等 |
| | 漏洩情報 | 正規 I/O からの想定外の漏洩情報，およびモジュールの変形を前提としない内部からの漏洩情報 | 処理時間変化，消費電力の変化，輻射電磁波等，いわゆるサイドチャネル情報 |
| | モジュール内部からの出力 | 狭義タンパ―手段に基づくモジュールの変形を前提として取り出される信号 | 回路パターンの解析（入力を必ずしも必要としない），プローブ用ニードリによる内部信号観測，ターゲットモジュールからの輻射電磁波なの観測，温度変化の観測等 |

- 侵入型攻撃

侵襲攻撃は内部情報に直接アクセスするため，原始的ではあるが非常に高い攻撃を有する．しかし，侵襲攻撃には情報の取得に高額な機器と高度な専門知識が必要で，なおかつ内部情報を取得するのに相当の時間を要する．また暗号モジュール内部に光や振動を検知するセンサを搭載することでそれらの攻撃を検知することが可能で，これにより攻撃を認識した場合に内部情報を削除することで比較的容易に対策することができる．攻撃の前段階として IC チップ内部のメモリや配線，プロセッサ演算装置などの位置を調べるために，光学顕微鏡などを用いて構造を観察するレイアウト解析を行う．これにより攻撃対象を特定し最適な攻撃を行うことが可能となる．以下では侵襲攻撃の分類と解説を行う．侵襲攻撃は解析方法により，プローブ解析，メモリの直接攻撃，マイクロサージェリーに分類される．プローブ解析はアドレスバスやデータパス等の配線またはメモリセルの電位を，微細なプローブを用いて解析する手法である．メモリの直接攻撃はメモリ上の秘密情報を読み取る攻撃手法である．特に読み出し専用メモリ（ROM）の場合，光学的な特徴によりメモリ上のデータが 0 か 1 かを判別できるため危険性が高い．マイクロサージェリーは IC チップの配線を切断・他回路に接続することによって

内部情報を出力させる攻撃で，本来暗は号化される内部データも暗号回路を迂回させて配線するなどして取得することができる．

- フォールト攻撃

フォールト攻撃は暗号モジュールのクロックや電源にノイズを印加したり，レーザーや電磁波等を照射することで，意図的に暗号化処理を誤作動させ，本来出力されない内部情報等を用いて秘密鍵を解析する手法である．フォールト攻撃の手順は処理の誤作動を引き起こす作業と，取得した内部情報を解析し秘密鍵を導出する二段階に分けることができる．前者はレーザーや電磁波が代表的な手法として用いられているが，この他にも様々な物理的刺激が考案されている．これらの物理的刺激がフォールト攻撃を可能とする要件として，回路の誤作動誘発と，その正確なタイミングを制御が重要となる．フォールト攻撃で誤った演算結果から秘密鍵を解析するが，どの演算を誤ったかによって解析手法が変わってくる．そのため，正確なタイミングでの誤作動誘発が必要となる．また，フォールト攻撃の代表は Boneh らによって考案された正常時と異常時の暗号文出力の差分から鍵を求める差分故障解析 DFA(Differential Fault Analysis)[20]である．

- サイドチャネル攻撃

サイドチャネル攻撃は，暗号モジュールの消費電力波形や，放射電磁波形などに漏洩している内部動作情報を用いて，秘密鍵を取り出す攻撃である．サイドチャネル攻撃の分類を表 2.4 に示す．

表 2.4　サイドチャネル攻撃の分類

| サイドチャネル情報 | 名称 | 説明 |
|---|---|---|
| 処理時間 | タイミング攻撃 | 処理時間を測定し，秘密情報を入手する |
| 消費電力 | 単純電力解析 | 単一の消費電力波形から秘密情報を入手する |
| | 差分電力解析 | 複数の消費電力波形から秘密情報を入手する |
| 放射電磁波 | 単純電磁波解析 | 単一の電磁波形から秘密情報を入手する |
| | 差分電磁波解析 | 複数の電磁波形から秘密情報を入手する |

タイミング攻撃はデータに依存する処理時間を解析し，内部情報を解析する攻撃手法である．データに依存する条件分岐や，プログラムの最適化により，処理時間は変化する．これを利用して予想した鍵による処理時間と実際の処理時間の差から秘密情報を特定するものである．消費電力や放射電磁波は，モジュール内部のトランジスタのスイッチングによって発生する．トランジスタを制御するのは鍵を含む内部データなので，秘密鍵と消費電力・放射電磁波には何らかの相関関係があるものとして解析する．消費電力や電磁波はオシロスコープのような安価な機器で取得できるため，サイドチャネル攻撃は現実的な脅威が非常に高い．消費電力を解析するサイドチャネル攻撃は，単純電力

解析 SPA(Simple Power Analysis)[21]と差分電力解析 DPA(Differential Power Analysis)[2]に大別される．SPA は波形から直接秘密鍵を読み取るもので，DPA は鍵に依存する微小な消費電力の変化を，数千～数十万波形から統計的な処理によって解析する手法である．消費電力の代りに放射電磁波を用いるものはそれぞれ，単純電磁波解析 SEMA(Simple Electro-Magnetic Analysis)，DEMA(Differential Electro-Magnetic Analysis)と呼ばれる．

## 2.5 サイドチャネル攻撃対策

サイドチャネル攻撃に対し，様々な攻撃対策が提案されている．本研究では，Masked-AND Operation (MAO) [9]，Wave Dynamic Differential Logic (WDDL) [10]，Masked Dual-Rail Pre-charge Logic (MDPL) [11]と Random Switching Logic (RSL) [12]の各対策を施した AES 回路を用いた評価実験を行う．MAO, WDDL と MDPL の回路は横浜国立大学が公開している回路[13]を実装している．各対策法を以下に示す．

- Masked-AND Operation(MAO)

Masked-And Operation は，Trichina らが提案した乱数マスクによる DPA 対策方式である．通常のマスク法はアルゴリズムレベルで対策を行うが，MAO は演算素子レベルでマスクを行うため図 2.10 の独自の AND ゲートを用いる．真のデータ$a$と$b$はそれぞれ独立な乱数$m_a$と$m_b$と XOR され，$\tilde{a}$と$\tilde{b}$として入力される．$a$と$b$の論理積$a \bullet b$を新たな独立な乱数入力$m$でマスクされた値$(a \bullet b) \oplus m$が出力される．このゲートの処理中には$a$と$b$も出力$a \bullet b$も現れない．

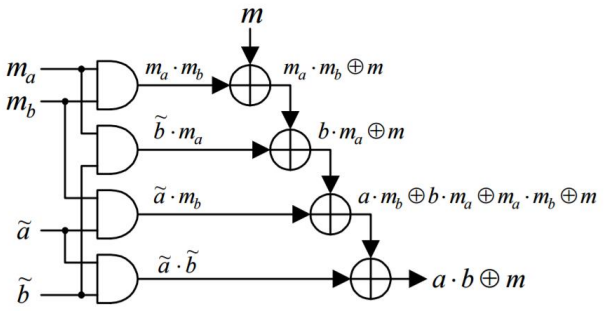


図 2.10　Masked-AND 基本構成

- Wave Dynamic Differential Logic(WDDL)

Wave Dynamic Differential Logic は，Tiri らによって提案された DPA 対策方式である．図 2.11 は WDDL の基本構成要素を示しており，ゲートスイッチング時の消費電力を一定することを目的に 2 線ロジックの Sense Amplifier Based Logic (SABL)を応用している．データ入力回路ロジックの Precharge 信号が 1 のとき，組み合わせ回路への入力全て 0 となる．そして，Precharge 信号が 0 に代わると，各入力データは相補信号とペアとなって演算回路に送られる．どのような入力データに対しても回路全体のスイッチング回数は変わらずほぼ一定の消費電力となるため，電力解析攻撃への対策として有効である．

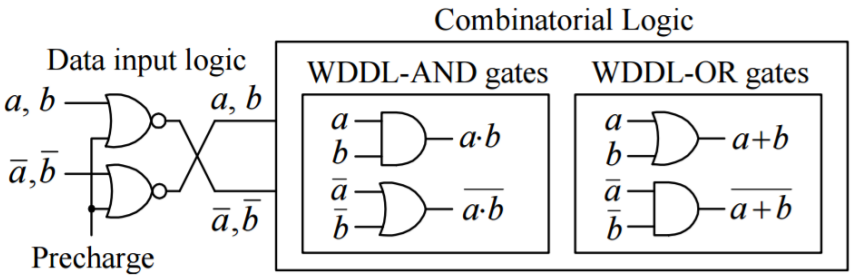


図 2.11　WDDL の基本構成

- Masked Dual-Rail Pre-charge Logic(MDPL)

Masked Dual-Rail Pre-charge Logic は，Popp らが提案した WDDL と乱数マスクを組み合わせた DPA 対策法である．図 2.12 に MDPL の基本構成を示す．図 2.12(a)の MAJ ゲートは，3 入力のうち 0 か 1 の多い方のビットを多数決で出力する．図 2.12(b)の MDPL-AND ゲートは，MAJ ゲートを 2 つ相補的に配置し，マスクされた入力$a_m$，$b_m$とマスク$m$に対して式(2.3)を計算する．表 2.5 に MDPL-AND ゲートの真理値表を示す．

$$\begin{cases} q_m = MAJ(a_m, b_m, m) = MAJ(a \oplus m, b \oplus m, m) = a \bullet b \oplus m \\ \bar{q}_m = MAJ(\bar{a}_m, \bar{b}_m, \bar{m}) = MAJ(a \oplus \bar{m}, b \oplus \bar{m}, \bar{m}) = a \bullet b \oplus \bar{m} \end{cases} \quad (2.3)$$

WDDL では相補的に動作する回路の寄生容量が等しくなければ，厳密には消費電力は均一とならない．それに対して，MDPL は図 2.12(c)のように乱数$m$（および$\bar{m}$）の値に応じて MAJ ゲートの出力がランダムに遷移するため，相補的な配線容量が釣り合っていない場合でも消費電力が均一化される．

表 2.5　MDPL-AND ゲートの真理値表

| $a$ | $b$ | $m$ | $a_m$ | $b_m$ | $q_m$ | $\bar{m}$ | $\bar{a}_m$ | $\bar{b}_m$ | $\bar{q}_m$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |

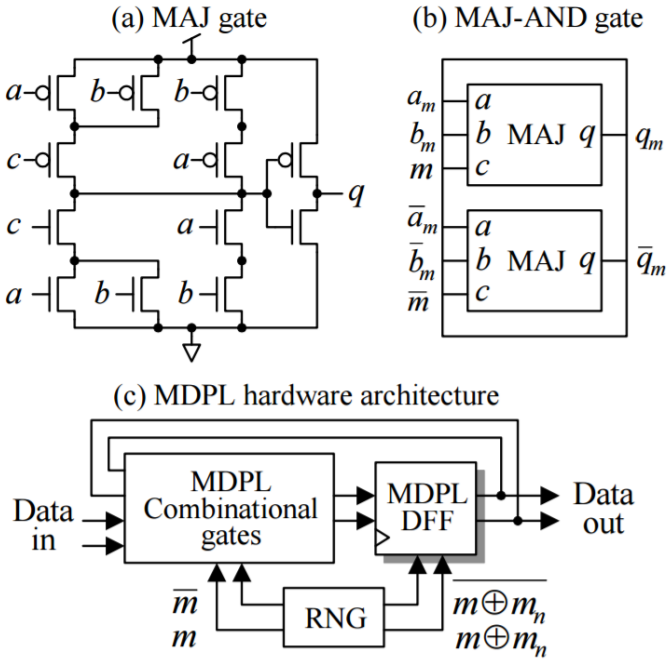


図 2.12　MDPL の基本構成

- Random Switching Logic (RSL)

Random Switching Logic は，三菱電機が提案した出力強化信号付きの多数決論理ゲートの対策法である．図 2.13 に RSL の NAND ゲートを示す．信号の遅延時間を考慮していない単純なマスク対策では，レジスタの過渡遷移から情報が漏洩する可能性がある．これを防ぐために，RSL ゲートでは入力$(x_z, y_z)$，出力イネーブル$(\overline{en})$，そして乱数マスク$(r_z)$で信号遅延を制御する．RSL-NAND ゲートの処理過程は以下の通りである．

入力：$\overline{en}$, $\begin{cases} x = a \oplus r_x \\ y = b \oplus r_x \end{cases}$, $\begin{cases} r_z \\ r_{xz} = r_x \oplus r_z \\ r_{yz} = r_y \oplus r_z \end{cases}$

出力：$\overline{a \bullet b} \oplus r_z$

手順 1：過渡遷移抑制 $\overline{en} = 1$

手順 2：$x$をリマスク $x_z = x \oplus r_{xz} (= a \oplus r_z)$，$y$をリマスク $y_z = y \oplus r_{yz} (= b \oplus r_z)$

手順 3：RSL-NAND ゲートへ入力データをセット RSL-NAND$(x_z, y_z, r_z, \overline{en})$

手順 4：データ確定後に出力をイネーブル$\overline{en} = 0$

RSL ゲートは専用の回路ライブラリが必要なため，本研究では，これと等価の論理をスタンダードセルライブラリで組んだ疑似 RSL による暗号回路に対して評価を行った．図 2.12 に疑似 RSL-NAND の構成を示す．

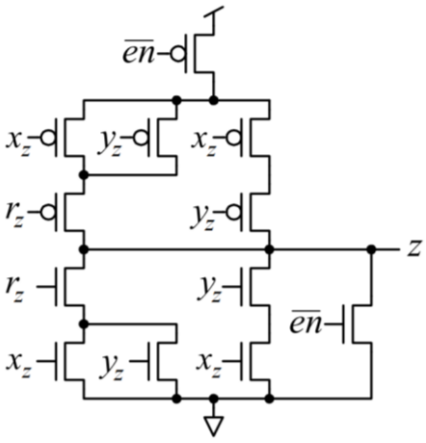


図 2.13　RSL-NAND ゲート

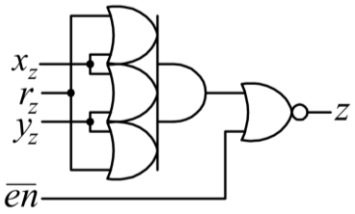


図 2.14　疑似 RSL-NAND ゲート

## 2.6　AES への電力解析

本研究で用いた AES 回路に対する代表的な電力解析攻撃手法を表 2.6 に示す．AES の電力解析は通常，32bit 単位の処理を行う MixColumns がスキップされる最終ラウンド（第 10 ラウンド）に対して行われる．残りの SubBytes，ShiftRows，AddRoundKey は 8bit 単位の処理のため，128bit の秘密鍵の推定が 8bit 毎に独立に行え，$2^8 = 256$パターンの推定を 16 回行って電力波形との相関を調べればよい．8bit×16 個 (=128bit)の推定鍵を以下では鍵候補と呼ぶ．最終ラウンドで出力される暗号文は既知のため，ある 8bit の鍵候補 $k$ に対応する暗号文の 8bit の部分を $c$ とすると，相関の計算に用いる 8bit の中間値 $\boldsymbol{I}$ は式(2.4)で求められる．なおここで$S^{-1}$は 128bit の関数 SubBytes を構成する 8bit 置換 Sbox の逆関数を表す．

$$\boldsymbol{I} = S^{-1}(\boldsymbol{c} \oplus \boldsymbol{k}) \tag{2.4}$$

表 2.6　AES 回路に対する攻撃手法

| 攻撃手法 | 特徴 | 攻撃区間 |
|---|---|---|
| DPA | 推定する部分鍵で計算した中間値の特定の 1 ビットの値によって電力波形を 2 グループに分け，双方の平均の差を計算し，推定鍵と相関がみられるかどうかを調べる． | 10 ラウンド |
| B-DPA | 複数の中間値に対する DPA の結果を総和する． | 10 ラウンド |
| ZO-DPA | 波形の 2 乗平均の差を計算する． | 10 ラウンド |
| CPA | 推定する部分鍵で計算した中間値の（ハミング距離）と電力波形の相関を調べる．未対策の暗号モジュールであれば，DPA 攻撃より少ない波形数で攻撃が可能． | データ出力 |

- Differential Power Analysis(DPA)

Kocher らが提案した DPA では，中間値$I$のあるビットの推定値が$b_i = 1$のときの平均電力波形$\overline{W}_{b_i=1}$と，$b_i = 0$ときの平均電力波形$\overline{W}_{b_i=0}$との差である平均電力差分$\Delta(b_i)$を式

(2.5)で求める．各鍵候補に対してこれを求め，最も絶対値が大きい（相関が高い）ものを正しい鍵と推定する．

$$\Delta(b_i) = \bar{W}_{b_i=1} - \bar{W}_{b_i=0} \quad (\mathrm{i} = 0 \cdots 7) \tag{2.5}$$

- Bevan’s multibit DPA (B-DPA)

DPA の$\Delta(b_i)$の絶対値を複数ビット（通常は処理の最小単位の 8bit）集めて，その和のその大きいものを正しい鍵と推定する[22].

$$\sum_{b_i \in I} |\Delta(b_i)| \tag{2.6}$$

- Waddle’s Zero-Offset Second-Order DPA (ZO-DPA)

Waddle らは DPA を拡張した 2 次の DPA を複数提案している[23]．その中で最も基本的な攻撃が式(2.5)の電力波形の 2 乗平均の差$\Delta_{2nd}(b_i)$を計算する Zero-Offset セカンドオーダーDPA (ZO-DPA)である．$N_{Condition}$は$\bar{W}^{(2)}_{Condition}$の条件が成立するときの波形数である．

$$\bar{W}^{(2)}_{Condition} = \sum \bar{W}_i^{\,2} / N_{Condition} \tag{2.6}$$

$$\Delta_{2nd}(b_i) = \bar{W}^{(2)}_{b_i=1} - \bar{W}^{(2)}_{b_i=0}$$

本研究では B-DPA とこれを組み合わせ, $\Delta_{2nd}(b_i)$を 8 ビットに集めた式(2.7)で相関を評価している．

$$\sum_{b_i \in I} |\Delta_{2nd}(b_i)| \tag{2.7}$$

- Correlation Power Analysis (CPA)

DPA は中間値のビットで電力波形を振り分けるが，Correlation Power Analysis はレジスタのスイッチングと消費電力の相関に注目し，中間値の遷移ビット数，つまりハミング距離$HD$と電力波形の相関を式(2.8)で計算し，$N$波形数の際，最大とする $k$ を正しい鍵と推定する[16].

$$r[W, HD] = \frac{\frac{1}{N}\sum_{t=0}^{N-1} W \cdot HD - \frac{1}{N}\sum_{i=0}^{N-1} W_i \cdot \frac{1}{N}\sum_{t=0}^{N-1} HD(I)_i}{\sqrt{\frac{1}{N}\sum_{i=0}^{N-1}(W_i - \bar{W})^2}\sqrt{\frac{1}{N}\sum_{i=0}^{N-1}\left(HD(I)_i - \overline{HD(I)}\right)^2}} \tag{2.8}$$

8bit 単位で解析するためハミング距離は 0~8 の値となる．8bit レジスタの変化前後の中間値をそれぞれ$a$，$b$とし，$HW(a)$を$a$のハミング重みとすれば，$a$と$b$のハミング距離は以下の式になる．

$$\begin{aligned} HD(I) &= HW(a \oplus b) \\ &= HW\left(S^{-1}(c_x \oplus k) \oplus c_y\right) \end{aligned} \tag{2.9}$$

ここで，$c_x$と$c_y$は暗号文の着目している 8bit である．

## 2.7 T 検定によるリーク情報の解析

ISO/IEC 17825 における差分電力解析攻撃 DPA, および差分電磁波解析攻撃 DEMA に対する耐性評価である T 検定の流れを図 2.15 に示す．電力波形または電磁波形を 1 万～10 万波形取得し，それを二つの Group 1, 2 に分け，さらに各 Group を Subset *A*, *B* に分けて次の $T_1$ および $T_2$ を計算する．

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

ここで,

$N_A$, $N_B$：サブセット *A* および *B* のサンプル数

$\mu_A$, $\mu_B$：*A* および *B* の波形の標本平均

$\sigma_A$, $\sigma_B$：*A* および *B* の波形の標準偏差

である. そして, $T_1$ および $T_2$ の絶対値が同一方向かつ同一時間に閾値 *C* を超えたとき, Subset *A*, *B* の波形の平均と標準偏差に偶然ではない（暗号モジュール内部のデータに依存した）有意な差が見られたと判断し, テスト結果を Fail とする. なお ISO/IEC 17825 では *C*=4.5 としており, 判定が Fail と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.

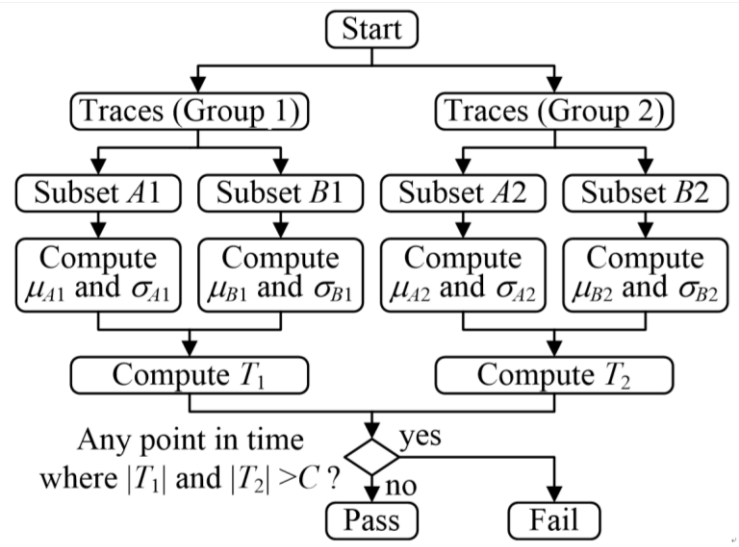


図 2.15　ISO/IEC 17825 の T 検定の手順

波形の Group と，その Subset への分類方法によって Test 0~5 の 6 種類の評価が行われる．128 ビット鍵の AES 暗号モジュールの評価では，次の秘密鍵を用いる．

0x0123456789abcdef123456789abcdef0

Test 1~5 では，128 ビットの平文 0 を入力して暗号化を行い，その暗号文出力を次の平

文入力とすることを 2*n* 回繰り返して集めた波形 DATA-SET 1 を用いる. その DATA-SET 1 を前後 *n* 波形ずつに分けて 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 つの条件を満たす固定の平文 *J* を上記の秘密鍵で *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間で少なくともどこか 1 バイトが等しい.
2) Sbox 出力の少なくともどこか 1 バイトが 0.
3) AddRoundKey に出力されるデータの少なくともどこか 1 バイトが 0.
4) データの少なくともどこか 1 バイトが 0.

Test 0~5 では次のように，波形をサブセットに分けて T 検定を行う.

- Test 0

*n* 波形の DATA-SET2 を前後半 *n*/2 ずつに分け，前半を Subset *A*1，後半 Subset *A*2 とする．また 2*n* 波形の DATA-SET 1 の最初の *n*/2 波形を Subset *B*1，その次の *n*/2 波形を Subset *B*2 とする.

- Test 1

Group1 のある波形が，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 *A*1 に，不一致ならば *B*1 とする．Group 2 も同様にして Subset *A*2 と *B*2 に分類する.

- Test 2

Group1, 2 の波形を，ラウンド *R* の Sbox 出力のビット *i* が 0 ならば Subset *A*1, *A*2 に，ビット *i* が 1 ならば Subset *B*1, *B*2 に分類する.

- Test 3

Group1, 2 の波形を，ラウンド *R* の出力のビット *i* が 0 ならば Subset *A*1, *A*2 に，ビット *i* が 1 ならば Subset *B*1, *B*2 に分類する.

- Test 4

Group1, 2 の波形を，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 *A*1, *A*2 に，*i* ならば Subset *B*1, *B*2 に分類する.

- Test 5

Group1, 2 の波形を，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 *A*1, *A*2 に，*i* ならば Subset *B*1, *B*2 に分類する.

評価にはセキュリティレベル 3 と 4 があり，レベル 3 は T 検定に 10,000 波形必要である．つまり暗号化を 2*n*=10,000 回繰り返す．また上位のレベル 4 では，2*n*=100,000 となっている.

# 3 偏りを有するデータによる FPGA 上の AES 回路の評価

本章では, ランダム生成データと偏りを有するデータをSAKURA-G上に実装したAES回路で暗号化し，その電力波形に対してISO/IEC 17825のT検定評価を行う．ISO/IEC17825は, 暗号モジュールの動作中の内部状態を知ることができる評価者の立場を前提に，ラウンド毎に処理中のデータの特定のビットやバイトのパターンを調べ，それに応じて電力波形あるいは電磁波形を分類している．暗号文出力を次の平文入力とするため，その波形はランダムなデータによって生じたものと言ってよい．一方，文献[17]のCEMA 実験では，評価者の立場から入力データを 操作し，内部レジスタの遷移ビット数（ハミング距離）を偏らせることで，電磁波の信号強度の分散を偏らせて，解析の精度 (S/N 比)を上げることに成功している．しかし，サイドチャネル攻撃対策を施した回路にCEMAやCPAは働かないため，本研究ではデータのハミング“重み”を偏らせ，それをT 検定の波形の分類に用いることで解析精度の向上を図る．

## 3.1 偏りデータの作成

暗号モジュールの処理中の消費電力は中間値のハミング重みに相関があると仮定する．8ビットの中間値のハミング重みが最も少ないとき（ハミング重みが0と1）と最も大きいとき（ハミング重みが7と8）に相関があれば，消費電力からランダム入力より多くの情報漏洩が見られるのだろう．

偏りを有するデータは，中間値の着目バイト$I_a$のハミング重みが0,1,7,8となるように平文を生成する．式(3.1)に示すようにハミング重みが0と1とのパターン$HW_0$と$HW_8$は各1パターン，重み1と7のパターン$HW_1$と$HW_8$はそれぞれ8パターンとなる．

$$
\begin{aligned}
&HW_{0178} = \{HW_0, HW_1, HW_7, HW_8\} \\
&HW_0 = \{00\} \\
&HW_1 = \{01, 02, 04, 08, 10, 20, 40, 80\} \\
&HW_7 = \{7\mathrm{F}, \mathrm{BF}, \mathrm{DF}, \mathrm{EF}, \mathrm{F7}, \mathrm{FB}, \mathrm{FD}, \mathrm{FE}\} \\
&HW_8 = \{\mathrm{FF}\}
\end{aligned}
\tag{3.1}
$$

着目バイト以外の15バイトはランダムとすべきであるが, 上記18パターンをランダムに割り当てている．これは，他のバイトを解析するときに，同じ波形を再利用して新たに波形を取得する手間を省くためである. バイト単位の偏りを持つ中間値は次のように, 二つの方法で作成する.

- 全バイトに同じ偏りのデータをランダムに配置する．以下ではこの手法をSAMEと記述する.

  $I_a = \mathrm{SHUFFLE}(HW_{0178})\ (a, b = 0 \cdots 15)$

  $I_a = I_b$ for $a \neq b$

- 各バイトに独立した偏りデータをランダムに配置する．以下ではこの手法をDIFFと記述する．

  $I_a = \mathrm{SHUFFLE}(HW_{0178})\ (a, b = 0 \cdots 15)$

  $I_a \neq I_b$ for $a \neq b$

表 3.1　秘密鍵のリスト

| No. | 秘密鍵 | 説明 | 表記 |
|---|---|---|---|
| 1 | 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F | 任意 1 の秘密鍵 | 0X_KEY |
| 2 | 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F | 任意 2 の秘密鍵 | 1X_KEY |
| 3 | 01 23 45 67 89 AB CD EF 12 34 56 78 9A BC DE F0 | ISO/IEC 17825 の秘密鍵 | ISO_KEY |
| 4 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 全ビット 0 の秘密鍵 | 00_RK0 |
| 5 | 62 63 63 63 00 00 00 00 00 00 00 00 00 00 00 00 | ラウンド鍵 1 が全ビット 0 になる秘密鍵 | 00_RK1 |
| 6 | 03 00 00 00 61 63 63 63 00 00 00 00 00 00 00 00 | ラウンド鍵 2 が全ビット 0 になる秘密鍵 | 00_RK2 |
| 7 | 64 63 63 63 61 63 63 63 67 63 63 63 00 00 00 00 | ラウンド鍵 3 が全ビット 0 になる秘密鍵 | 00_RK3 |
| 8 | 97 98 98 1C 0A 00 00 00 0C 00 00 00 6B 63 63 63 | ラウンド鍵 4 が全ビット 0 になる秘密鍵 | 00_RK4 |
| 9 | 7C 63 63 93 92 98 98 EC 0C 00 00 00 6B 63 63 63 | ラウンド鍵 5 が全ビット 0 になる秘密鍵 | 00_RK5 |
| 10 | A7 98 98 89 D1 FB FB 8F 94 98 98 79 6B 63 63 63 | ラウンド鍵 6 が全ビット 0 になる秘密鍵 | 00_RK6 |
| 11 | E8 97 6F DD 49 63 63 CA 2F 63 63 5F F3 FB FB 26 | ラウンド鍵 7 が全ビット 0 になる秘密鍵 | 00_RK7 |
| 12 | 2E D1 74 6D 5E F4 79 CF CC 00 00 3C 10 98 98 45 | ラウンド鍵 8 が全ビット 0 になる秘密鍵 | 00_RK8 |
| 13 | 73 97 D3 47 8F 25 23 25 38 F4 9E 9F 10 98 98 45 | ラウンド鍵 9 が全ビット 0 になる秘密鍵 | 00_RK9 |
| 14 | 15 F1 51 74 2E B2 0B 8A 1D D1 B6 6C E4 6C D3 89 | ラウンド鍵 10 が全ビット 0 になる秘密鍵 | 00_RK10 |
| 15 | FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF | 全ビット 1 の秘密鍵 | FF_RK0 |
| 16 | 9D 9C 9C 9C 00 00 00 00 00 00 00 00 00 00 00 00 | ラウンド鍵 1 が全ビット 1 になる秘密鍵 | FF_RK1 |
| 17 | FC FF FF FF 9E 9C 9C 9C 00 00 00 00 00 00 00 00 | ラウンド鍵 2 が全ビット 1 になる秘密鍵 | FF_RK2 |
| 18 | 9B 9C 9C 9C 61 63 63 63 98 9C 9C 9C 00 00 00 00 | ラウンド鍵 3 が全ビット 1 になる秘密鍵 | FF_RK3 |
| 19 | 4D 42 42 BE F5 FF FF FF F3 FF FF FF 94 9C 9C 9C | ラウンド鍵 4 が全ビット 1 になる秘密鍵 | FF_RK4 |
| 20 | A6 B9 B9 87 B7 BD BD 07 0C 00 00 00 6B 63 63 63 | ラウンド鍵 5 が全ビット 1 になる秘密鍵 | FF_RK5 |
| 21 | 7D 42 42 09 2E 04 04 70 B1 BD BD 06 6B 63 63 63 | ラウンド鍵 6 が全ビット 1 になる秘密鍵 | FF_RK6 |
| 22 | 20 5F 06 79 6C 46 46 6A F5 B9 B9 00 D6 DE DE 86 | ラウンド鍵 7 が全ビット 1 になる秘密鍵 | FF_RK7 |
| 23 | 25 DA 68 68 B3 19 DA 52 33 FF FF C3 EF 67 67 BA | ラウンド鍵 8 が全ビット 1 になる秘密鍵 | FF_RK8 |
| 24 | 78 9C 81 9D 69 C3 1B 02 2A E6 0B 9D 10 98 98 45 | ラウンド鍵 9 が全ビット 1 になる秘密鍵 | FF_RK9 |
| 25 | 15 F1 51 74 2E B2 0B 8A 1D D1 B6 6C E4 6C D3 89 | ラウンド鍵 10 が全ビット 1 になる秘密鍵 | FF_RK10 |

これらの値を T 検定で解析する各ラウンド 1~9 の中間値として，既知のラウンド鍵 RK1~RK9 を用いて AES を逆算して入力平文を求める．中間値は T 検定の Test に応じて SubBytes，MixColumns，AddRoundKey の出力となる．また，各ラウンドでラウンド鍵が特殊なパターンとなるようものを含めて，表 3.1 の 25 種類の秘密鍵を用いた．この方法で秘密鍵の値が情報漏洩への影響について確認する．

## 3.2 実験環境

3.1節で作成した偏りを持つデータをSAKURA-G上のAES回路に入力し，ISO/IEC 17825のセキュリティレベル3のT検定を行う．本章では偏ったデータセットと電圧波形の関係を1グループとして解析する. また, Test 0はいかなる実装に対しても, 全てのビットに対してT値が閾値4.5を超えることが確かめられており，評価に用いる意味がないため，本研究では実施していない.

図 3.1に電力解析実験環境を，図 3.2に実験の流れを，表3.2に実験の諸条件を示す. 暗号処理中の電力波形はGND線に挿入された1Ωシャント抵抗の電圧降下として観測される．PCで生成した平文をUSB経由でSAKURA-Gに送り，暗号化中の電力波形をオシロスコープで取得し，USB経由でPCに送信した波形を保存する．ノイズの影響を低減するため，電力波形は同じ平文を10回暗号化して平均化した．つまり，標準は1万波形を使うT検定に，実際には10万波形取得していることになる．波形取得プログラムはSASEBO_waveform_acquistion-limited.Rev891[24]を利用した.

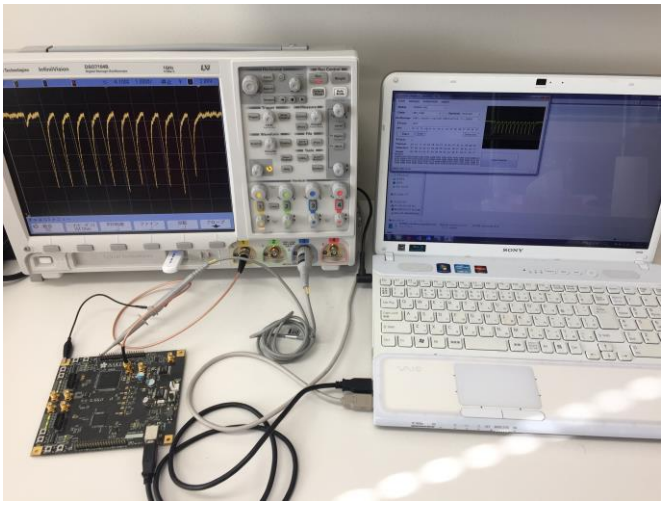

図 3.1　電力解析実験環境

表 3.2　電力解析実験の諸条件

| AES 回路 | ループアーキテクチャ，合成体 Sbox |
|---|---|
| 観測ポイント | GND側1Ωシャント抵抗 |
| 動作周波数 | 1.5 MHz |
| 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 |
| フィルタ | BWLimit 20MHz |

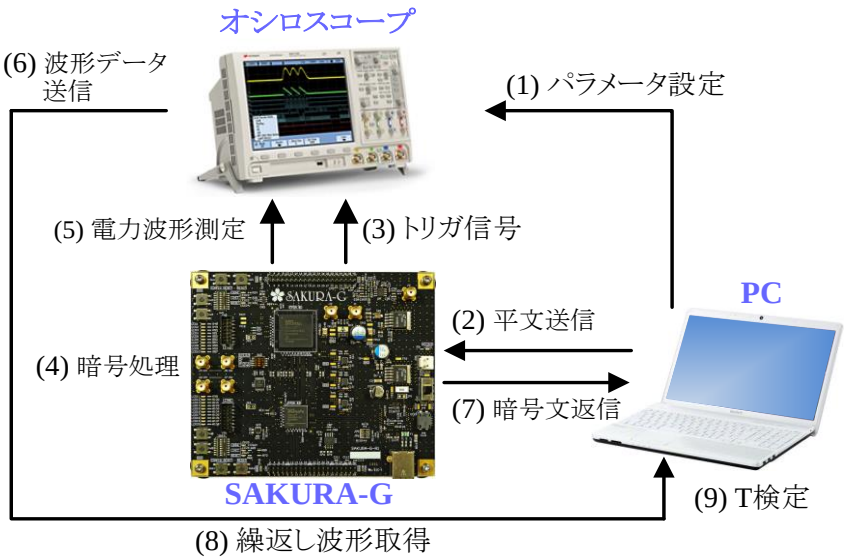


図 3.2　電力解析実験の流れ

図 3.2 に示した実験の流れは以下のとおりである．

(1) PC からオシロスコープに初期パラメータを設定．
(2) PC からボードに平文を送信．
(3) ボードからオシロスコープにトリガ信号を送信．
(4) 送信された平文を暗号化．
(5) 暗号化中の電力波形をオシロスコープで測定．
(6) 取得した波形データを，PC に送信．
(7) ボードから PC に暗号文を返信．
(8) (2)～(7)を 100,000 回繰り返し，波形を取得．
(9) 10,000 に平均化し，T 検定解析．

## 3.3　結果と考察

図 3.3にSAKURA-G上の未対策のAES回路の電力波形を示す．目盛りは縦軸が2mV，横軸は1μsである．電力波形に11のピークが見えるが，最後のピークはAESの10ラウンドの処理が終了して暗号文がレジスタに書き込まれたことで，その出力につながっているロジックが動作したことによるものである．

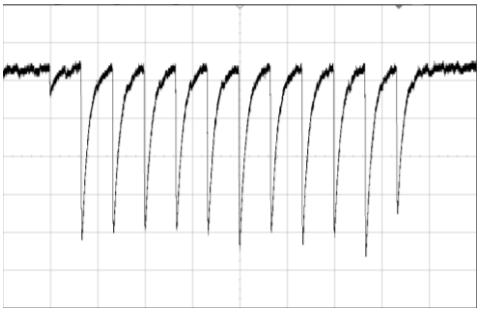

図 3.3　AES の電力波形

表 3.3は表3.1の0X_KEYの秘密鍵を用い，データを偏らせた解析結果の一部である．二行目の数値は偏らせた中間値のラウンドを意味する．SubBytesの出力を偏らせたものがTest 2，ラウンド出力の場合がTest 3で，着目ビットでT値の絶対値が4.5を越えた数(0~128)を記している．DIFFでは5ビット以下であるが，SAMEでは全てのビットで閾値4.5を越えており，他の秘密鍵でも同様になった．この結果から，SAMEのデータの方が秘密鍵の抽出に有利であると考えられる．これについては，第4章でサイドチャネル攻撃対策済の回路にDIFFとSAMEのデータを入力して検証する．

DIFF のデータを用いた解析では，秘密鍵を変更しても T 値が閾値 4.5 を越えるビット数はあまり変わらなかった．T 検定は中間値で母集団を分類するので，これは妥当な結果であると考えられる．偏った中間値による T 検定の全結果は付録に収めた．

表 3.3　偏ったデータによる T 検定の解析結果

| T検定 | Round | 0X_KEY_DIFF | | | | | | | | | 0X_KEY_SAME | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Test2 | 1 | 0 | 0 | 4 | 2 | 2 | 2 | 1 | 2 | 2 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 2 | 0 | 5 | 1 | 3 | 3 | 1 | 2 | 2 | 1 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 3 | 0 | 1 | 3 | 2 | 1 | 2 | 2 | 1 | 1 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 4 | 0 | 0 | 0 | 3 | 1 | 2 | 1 | 3 | 2 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 5 | 0 | 0 | 1 | 1 | 4 | 2 | 1 | 0 | 1 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 6 | 0 | 1 | 2 | 2 | 1 | 4 | 3 | 2 | 1 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 7 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 0 | 2 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 8 | 0 | 2 | 1 | 3 | 2 | 1 | 1 | 1 | 0 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 9 | 0 | 0 | 1 | 2 | 2 | 4 | 2 | 1 | 4 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 10 | 0 | 0 | 1 | 2 | 0 | 1 | 1 | 1 | 1 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| Test3 | 1 | 1 | 2 | 0 | 1 | 2 | 3 | 3 | 1 | 2 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 2 | 1 | 3 | 1 | 1 | 3 | 2 | 0 | 0 | 6 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 3 | 3 | 0 | 1 | 3 | 1 | 1 | 1 | 2 | 3 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 4 | 2 | 2 | 2 | 1 | 4 | 5 | 2 | 0 | 2 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 5 | 2 | 0 | 0 | 1 | 3 | 2 | 1 | 1 | 0 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 6 | 0 | 1 | 0 | 0 | 3 | 4 | 2 | 1 | 2 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 7 | 1 | 2 | 0 | 0 | 3 | 0 | 4 | 2 | 0 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 8 | 2 | 4 | 2 | 1 | 5 | 1 | 1 | 0 | 1 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 9 | 2 | 3 | 0 | 3 | 2 | 3 | 1 | 1 | 3 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |
| | 10 | 1 | 2 | 1 | 3 | 1 | 2 | 3 | 1 | 2 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 |

表 3.4　偏りデータによる RSL-2 対策の T 検定の解析結果

| T 検定 | Round | ランダム | DIFF | SAME |
|---|---|---|---|---|
| **Test 1** | **1** | 1 | 1 | 128 |
| | **2** | 2 | 0 | 128 |
| | **3** | 2 | 2 | 128 |
| | **4** | 2 | 1 | 128 |
| | **5** | 2 | 2 | 128 |
| | **6** | 2 | 1 | 128 |
| | **7** | 2 | 3 | 128 |
| | **8** | 0 | 0 | 128 |
| | **9** | 1 | 0 | 128 |
| | **10** | 0 | 2 | 128 |
| **Test 2** | **1** | 0 | 0 | 128 |
| | **2** | 0 | 0 | 128 |
| | **3** | 0 | 0 | 128 |
| | **4** | 0 | 0 | 128 |
| | **5** | 0 | 0 | 128 |
| | **6** | 0 | 0 | 128 |
| | **7** | 0 | 0 | 128 |
| | **8** | 0 | 0 | 128 |
| | **9** | 0 | 0 | 128 |
| | **10** | 12 | 31 | 128 |
| **Test 3** | **1** | 2 | 1 | 128 |
| | **2** | 0 | 0 | 128 |
| | **3** | 0 | 0 | 128 |
| | **4** | 0 | 0 | 128 |
| | **5** | 0 | 0 | 128 |
| | **6** | 1 | 0 | 128 |
| | **7** | 0 | 0 | 128 |
| | **8** | 0 | 0 | 128 |
| | **9** | 1 | 40 | 128 |
| | **10** | 12 | 31 | 128 |
| **Test 4** | **1** | 0 | 0 | 18 |
| | **2** | 0 | 0 | 18 |
| | **3** | 0 | 0 | 18 |
| | **4** | 0 | 0 | 18 |
| | **5** | 0 | 0 | 18 |
| | **6** | 0 | 0 | 18 |
| | **7** | 0 | 0 | 18 |
| | **8** | 0 | 0 | 18 |
| | **9** | 0 | 1 | 18 |
| | **10** | 0 | 1 | 18 |
| **Test 5** | **1** | 0 | 0 | 18 |
| | **2** | 0 | 0 | 17 |
| | **3** | 0 | 0 | 18 |
| | **4** | 0 | 0 | 18 |
| | **5** | 0 | 0 | 18 |
| | **6** | 0 | 0 | 17 |
| | **7** | 1 | 0 | 18 |
| | **8** | 0 | 0 | 18 |
| | **9** | 0 | 1 | 18 |
| | **10** | 0 | 1 | 18 |
| **B-DPA** | | 0 | 6 | 0 |
| **ZO-DPA** | | 0 | 6 | 0 |
| **CPA** | | 0 | 0 | 0 |

表 3.4 に，疑似 RSL による対策を施した AES 回路の T 検定の解析結果の一部を示す．Test1~5 の各ラウンドについて，ランダム，DIFF，SAME の各データで T 値が閾値 4.5 を超えたビットの数を記してある．DIFF と SAME はラウンド 9 の Addroundkey の出力を偏らせている．最下段の B-DPA，ZO-DPA，CPA の数字は，各攻撃で 16Byte の秘密鍵のうち求まった正解鍵の個数を表している．

表 3.4 の Test 3 に注目すると，ラウンド 9 と 10 で，ランダム入力よりも提案手法 DIFF と SAME が明らかに高い閾値を示したビット数が多いことがわかる．特に提案手法 SAME では 128 ビット中，全ビットの T 値が閾値 4.5 を超えている．しかし，B-DPA と ZO-DPA 解析の結果をみると，提案手法 SAME では部分鍵が一つも求まっていない．一方，DIFF では複数の部分鍵が求まっている．従って，全てのバイトパターンを同じにしたデータ SAME は，秘密鍵に依存した中間値のパターンとは別の要因で T 値が高くなったと考えられ，以降の実験ではランダムと DIFF のデータを用いて解析を進める．また，秘密鍵についてはあまり情報漏洩に影響しないと考えられる．

# 4 サイドチャネル攻撃対策済暗号 LSI 上の AES 回路の評価

本章では， 130nm (MAHS)，90nm (CHAR)と 65nm (RAY)の 3 つの CMOS スタンダードセルライブラリで製造された 3 つ暗号 LSI 上の 5 種類の DPA 対策，MAO, WDDL, MDPL，疑似 RSL-1，疑似 RSL-2 が施された AES 回路に，3 章で述べた偏りを持つデータを用いた安全性評価を行う．なお，3 つの暗号 LSI に対して同じ実験を行ったが，全て傾向は同じであったため，本章では解析のためのグラフが最もきれいであった 90nm の暗号 LSI の結果だけを示す. 他の 2 つの暗号 LSI の結果についてはまとめて付録収めた. 偏りを持つ中間値は Test 3 のラウンド出力で, 全ラウンドに対して DIFF を用いた. なお疑似 RSL-1 も-2 も同じ図 2.12 の疑似 RSL ゲートを用いているが，疑似 RSL-2 は FPGA に実装した AES 回路と同じ回路ノードを持つように制限を加えている．

## 4.1 実験環境

図 4.1 に電力解析実験環境を，表 4.1 に実験の諸条件を示す．暗号 LSI は SASEBO-W 上のドータボード SASEBO-RII に搭載され，その電力波形は GND 線に挿入された 1Ω シャント抵抗の電圧降下として観測した．PC で生成した平文を USB 経由で SASEBO-RII に送り，暗号化中の電力波形を 20dB および 17dB のアンプで増幅した後にオシロスコープで取得し，USB 経由で PC に送信した波形を保存する．解析に用いる波形数はセキュリティレベル 3 では 1 万，レベル 4 では 10 万であるが，ノイズの影響を低減するため，同じ平文を 10 回暗号化して電力波形を平均化したものを 1 波形としている．つまり，標準の T 検定に対しては各レベルで 10 万および 100 万の波形を取得している. また, データを偏らせた提案手法に対しては 10 波形を平均化した 1 万波形, つまりレベル 3 と同様に 10 万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 B-DPA，ZO-DPA および CPA を行ない，鍵の導出を試みた．

ISO/IEC 17825 は元からランダムデータに対する波形を使うので，着目ビットが変わっても同じ波形を用いることができる．しかし，提案手法は各 1~10 ラウンドで偏ったパターンを作るので，解析精度が標準の T 検定に対して向上しなければ，10 倍の波形が必要となってしまう点に注意が必要である．

Test 2 では，Sbox の出力ビットで分類を行う．したがって Sbox 出力にも上記 18 パターンの偏りを持たせたデータで波形を取得すべきであるが，これには Test 3 と同じもの，つまりラウンド出力に偏りを持つものを用いることとした．これは，今回使用した暗号 LSI の AES 回路は，ループアーキテクチャを採用しており，ラウンド出力の偏りを持ったバイトパターンが次のラウンドの Sbox 入力となるため，その電力波形を用いても効果が期待できるためである．

ところで，実験に用いた暗号 LSI 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“000102030405060708”に固定されており，ユーザは下

位 56 ビットのみ設定が可能である．このため実験には ISO/IEC 17825 で指定された鍵ではなく，表 4.1 に示した値を用いた．

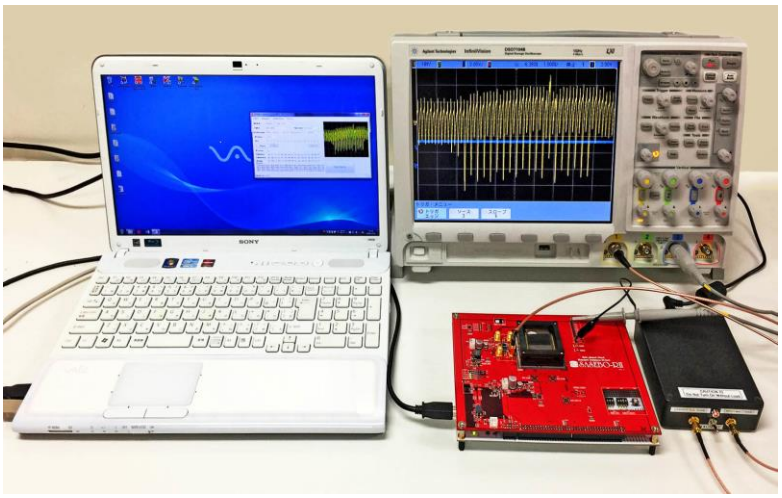

図 4.1　電力解析実験環境

表 4.1　電力解析実験の諸条件

| | 実験条件 | | |
|---|---|---|---|
| AES 回路 | ループアーキテクチャ，合成体 Sbox | | |
| 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 | 130nm CMOS<br>スタンダードセル | 90nm CMOS<br>スタンダードセル | 65nm CMOS<br>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),<br>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 | | |

## 4.2　90nm 暗号 LSI の結果と考察

図 4.2～図 4.6 にそれぞれ MAO，WDDL，MDPL，疑似 RSL-1 および-2 の各 AES 回路の電力波形を示す．目盛りのスケールは縦軸が 50mV，横軸が 1μs である．図 4.3 と図 4.4 は 22 のピークの波形が見えるが，これは WDDL と MDPL の 2 線のロジックはプリチャージと演算のためのディスチャージによって，1 ラウンドが 2 サイクルで動作するためである．

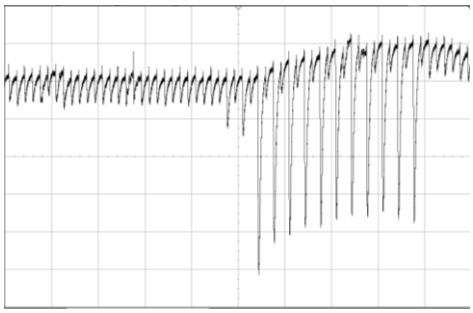

図 4.2　MAO の電圧波形

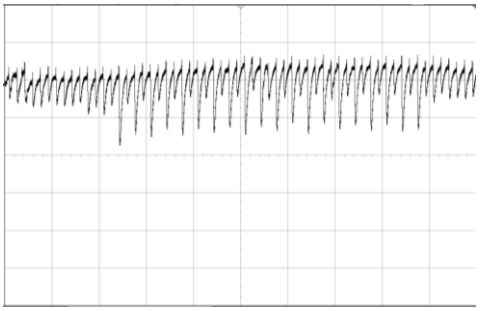

図 4.3　WDDL の電圧波形

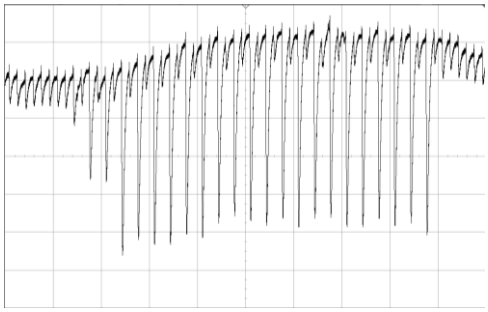

図 4.4　MDPL の電圧波形

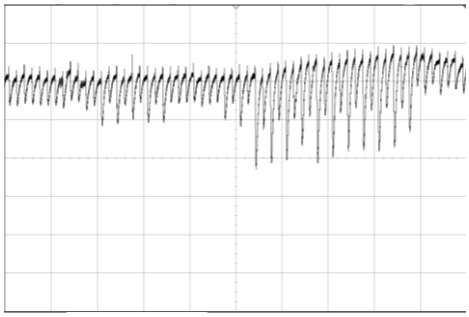

図 4.5　疑似 RSL-1 の電圧波形

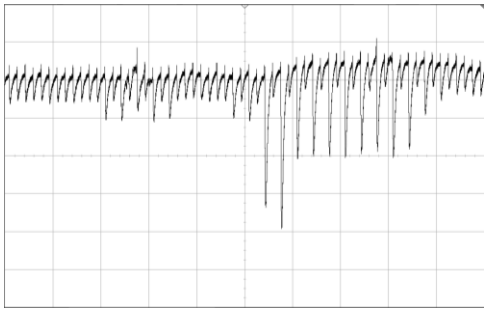

図 4.6　疑似 RSL-2 の電圧波形

図 4.7～4.12 にそれぞれ, WDDL, MDPL の各 DPA 対策を施した AES 回路に対する Test 3 の T 検定の結果を示す．各対策に対して 1 万波形のセキュリティレベル 3，10 万波形のレベル 4, そしてデータを偏らせた 1 万波形の提案手法 DIFF の 3 つのケースで評価を行った. 縦軸は解析しているラウンド, つまり波形の分類に用いた着目ビットを含むラウンドである. 各図では T 値が大きかった着目ビットを選んで示しており, WDDL は bit 27, MDPL は bit 66 である．また，横軸は時間（ラウンド）による T 値の変化を示している.

WDDL と MDPL はいずれも，着目ビットを含むラウンド処理時の T の絶対値に 4.5 以上のピークが見られ，リーク情報が検出されている．なお，ISO/IEC 17825 では，波形をラウンド出力 $R$ のビットパターンで振り分けているが，$R$ は次のラウンド入力となって電力波形が影響を受ける．したがって，1 ラウンド目の出力で振り分けた場合，そのリークを示す T 値のピークは次の 2 ラウンド目に出ており，全ての T 値が 1 ラウンドずつずれているように見える点に注意する.

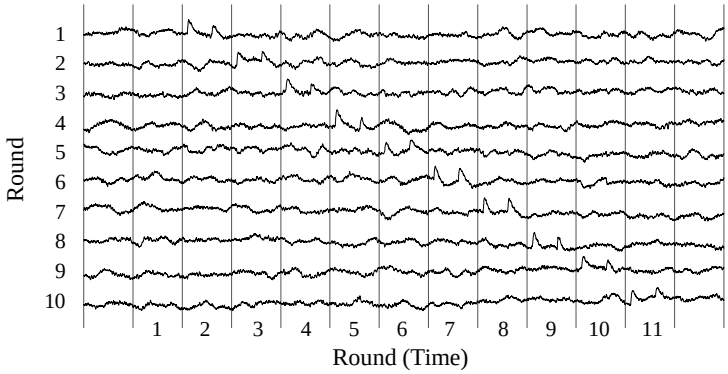


図 4.7 WDDL (Level 3, bit 27)

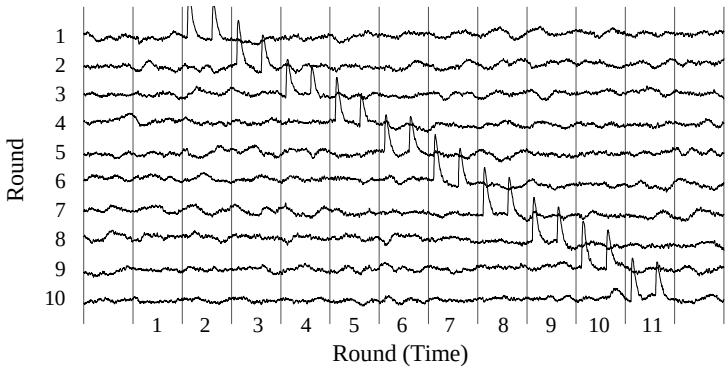


図 4.8 WDDL (Level 4, bit 27)

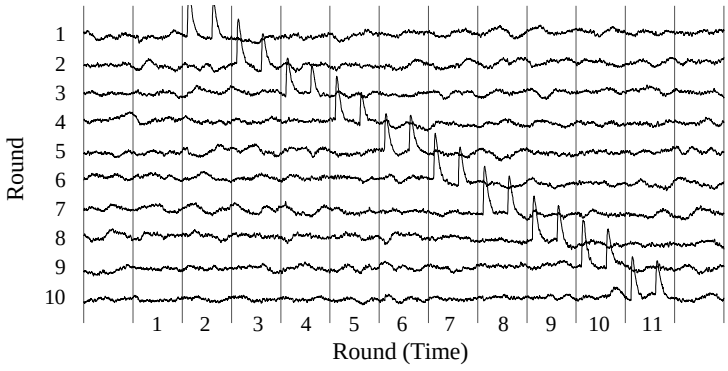


図 4.9 WDDL (DIFF, bit 27)

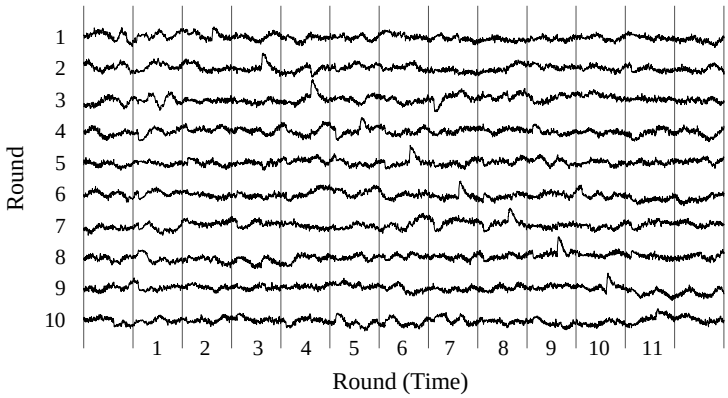


図 4.10 MDPL (Level 3, bit 66)

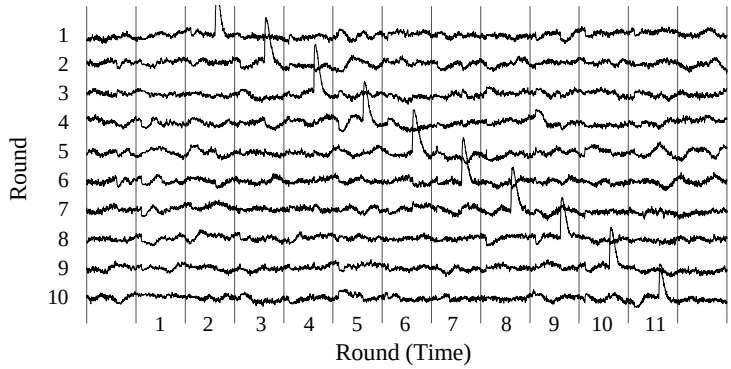


図 4.11　MDPL (Level 3, bit 66)

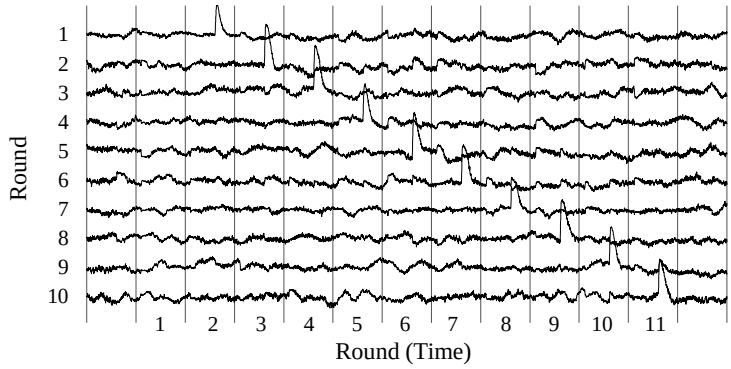


図 4.12　MDPL (DIFF, bit 66)

CPA では鍵は求まらなかったが，B-DPA と ZO-DPA では WDDL と MDPL いずれも全ての部分鍵が求まった．図 4.13 と図 4.14 は WDDL 対策済 AES 回路の ZO-DPA において，正しい部分鍵の電力波形との相関値が $2^8$=256 個の鍵候補の中で何番目に高いかを示している. 図 4.13 は ISO/IEC 17825 の T 検定に用いたランダム平文入力で, 図 4.14 は DIFF の偏りをもつ平文入力である．波形数が増えるに従って解析精度が上がり順位が上昇しているが，偏りを持たせたデータでは上昇がより速いことがわかる．これは図 4 の T 検定においてセキュリティレベル 3 よりも，波形数が 10 倍のレベル 4 の方が高いピークが表れていることと合致した結果と言える．なお，WDDL では T 値のピークが各ラウンドで 2 回見えるが，これは 2 線方式において演算で一方の線が放電されるときと，次のラウンドの演算に先立ってその線を充電するときの 2 回リーク情報が検出されるためである．

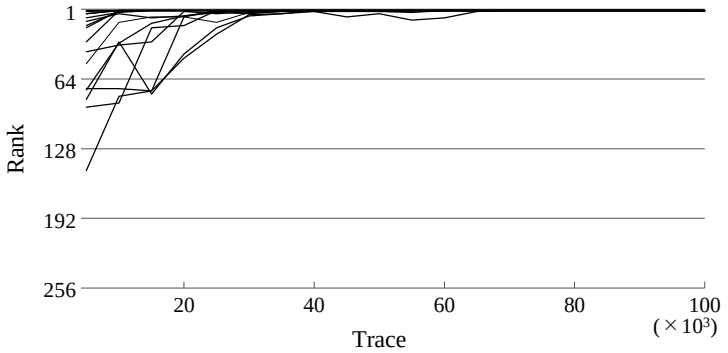


図 4.13　ランダム入力による WDDL への ZO-DPA による正しい部分鍵の順位

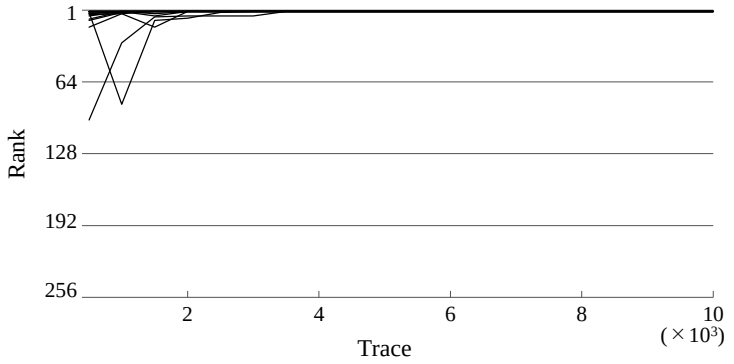


図 4.14　DIFF 入力による WDDL への ZO-DPA による正しい部分鍵の順位

図 4.14 のデータを偏らせた DIFF の ZO-DPA は，図 4.13 のランダム入力よりも少ない波形数で相関値が上昇している．したがって，T 検定も提案手法は少ない波形で高いリーク情報を検出でき，図 4.8 の 10 万波形を用いたセキュリティレベル 4 の検定とほぼ同等の精度が，図 4.9 のように 1/10 の 1 万波形で得られることがわかる．

図 4.15 と図 4.16 の MDPL に対する ZO-DPA は，いずれも直ちに全ての部分鍵が求まっており，ランダムと偏りを持ったデータの違いはこの図からはわからない．しかし，図 4.11 および図 4.12 の T 検定のピーク波形から，提案手法では WDDL と同様に，セキュリティレベル 4 の検定と同等の精度を 1 万波形で得られることがわかる．

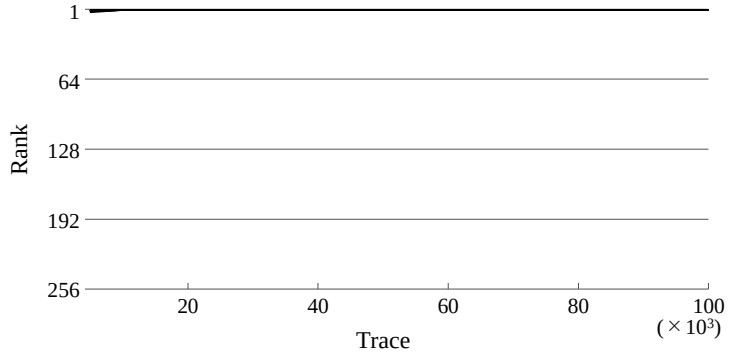


図 4.15　MDPL への ZO-DPA による正しい部分鍵の順位

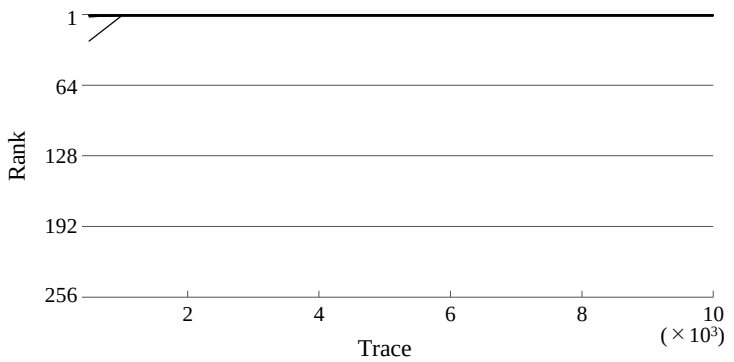


図 4.16　DIFF 入力による MDPL への ZO-DPA による正しい部分鍵の順位

図 4.17～図 4.19 に MAO の T 検定結果を示す．標準の T 検定ではレベル 3, 4 ともにリーク情報が見られず，ランダムな平文入力では CPA でも図 4.20 に示した ZO-DPA でも鍵が求まらなかった．それに対し，図 4.19 の提案手法 DIFF は，着目ビットを含むラウンド処理時の T 値にピークが見られ，リーク情報が明確に検出されていることがわかる．そしてデータを偏らせた DIFF の ZO-DPA では，図 4.21 に示したように 1 万波形で多くの鍵が求まっている．このように提案手法は，少ない波形数で解析精度を高められるだけでなく，標準の T 検定では得られなかったリーク情報を検出できることがわかる．

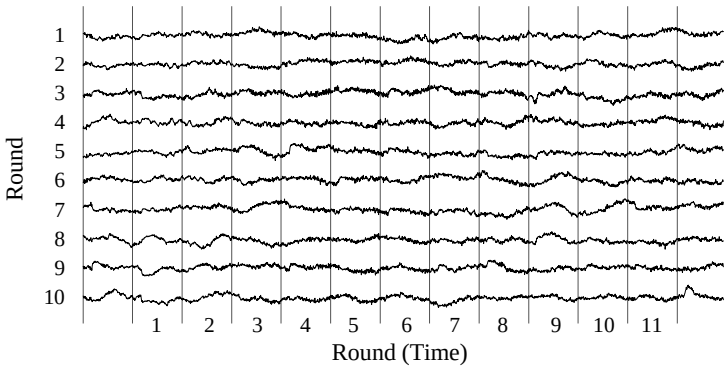


図 4.17　MAO(Level 3, bit 111)

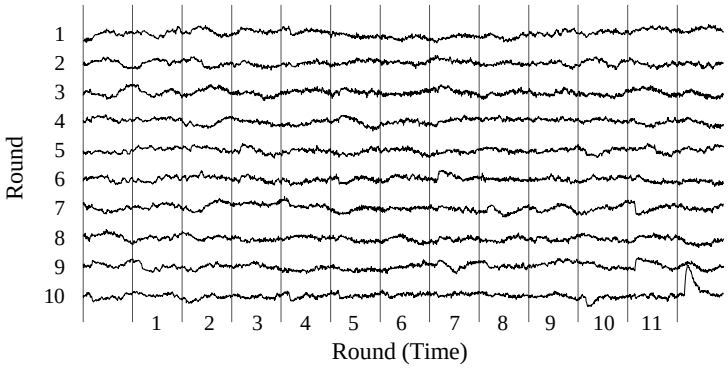


図 4.18　MAO(Level 4, bit 111)

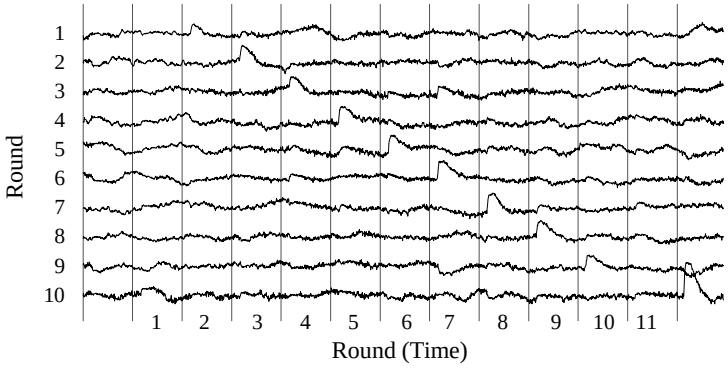


図 4.19　MAO (DIFF, bit 111)

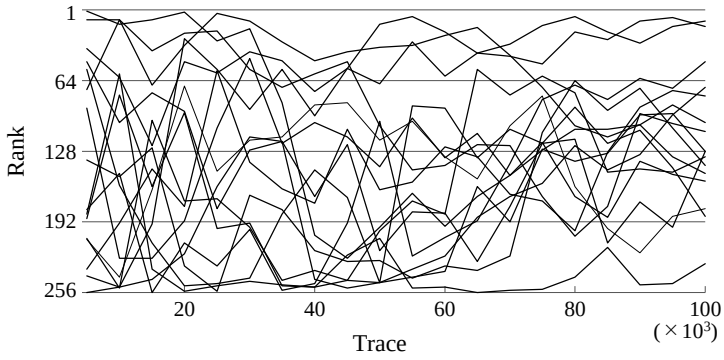


図 4.20　MAO への ZO-DPA による正しい部分鍵の順位

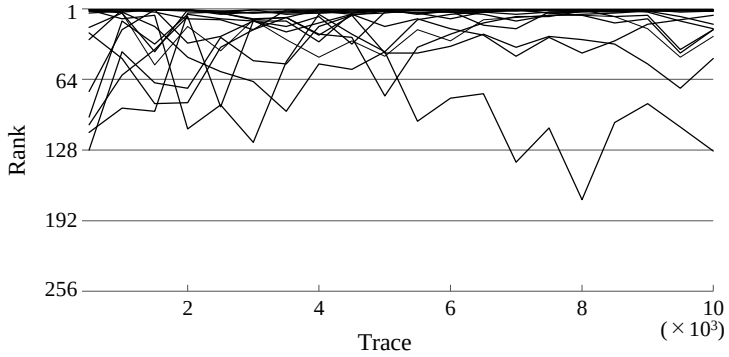


図 4.21　DIFF 入力による MAO への ZO-DPA による正しい部分鍵の順位

図 4.22～4.24 は疑似 RSL 方式による AES 回路で，比較的高い T 値が表れた bit 5 の結果である．全てのビットに対して bit 5 と同様に，セキュリティレベル 3, 4 および提案手法 DIFF のいずれでも，ラウンド処理に依存した T 値のピークを検出することができなかった．またランダムな入力に対して ZO-DPA でも CPA でも鍵は求まらず，図 4.25 と図 4.26 の ZO-DPA でも部分鍵の順位を示す線が全体にばらついていることからも，情報のリークは検出できていないことがわかる．

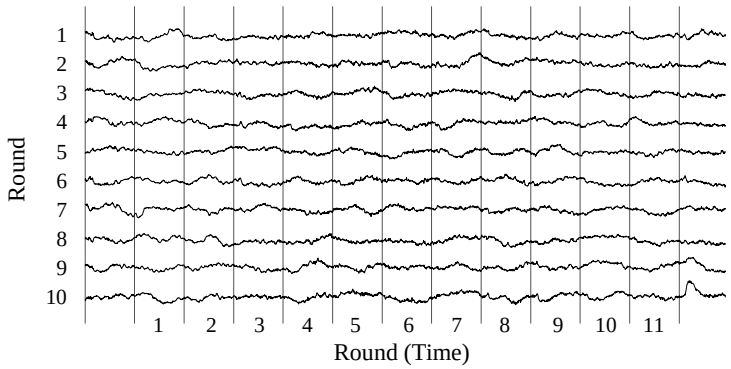


図 4.22　疑似 RSL-1 (Level 3, bit 5)

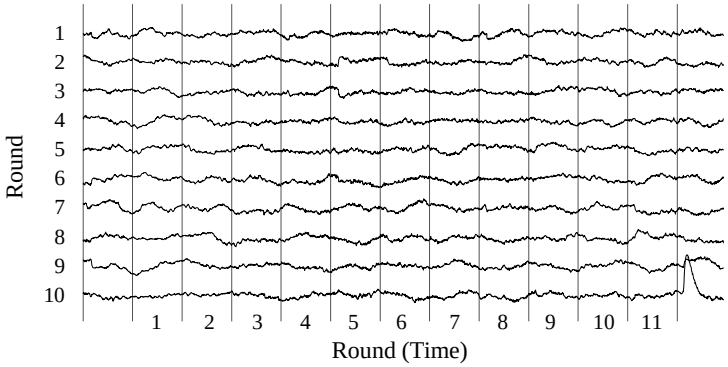


図 4.23　疑似 RSL-1 (Level 4, bit 5)

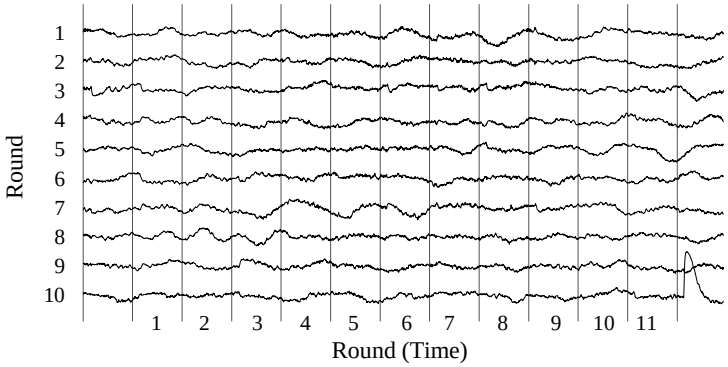


図 4.24　疑似 RSL-1 (DIFF, bit 5)

なお，11 ラウンド以降に T 値のピークが見られるが，これは 10 ラウンドの出力である暗号文のビットによる振り分けによって生じたものと考えられる．AES 回路のデータパスは 10 ラウンド終了後にレジスタに保存されたデータが外部に出力されるが，そのデータによってラウンド関数ブロックの回路がスイッチングすることになる．暗号文は内部変数のようにマスク処理したり，それによって生じる消費電力パターンを隠す必要もない．したがって，その消費電力を秘密でない暗号文データで振り分けた結果で T 値にピークが見られるのは当然のことであり，秘密情報がリークしているわけではない．したがって，最終ラウンド出力である暗号文で T 検定を行ってはいけないことに注意が必要である．

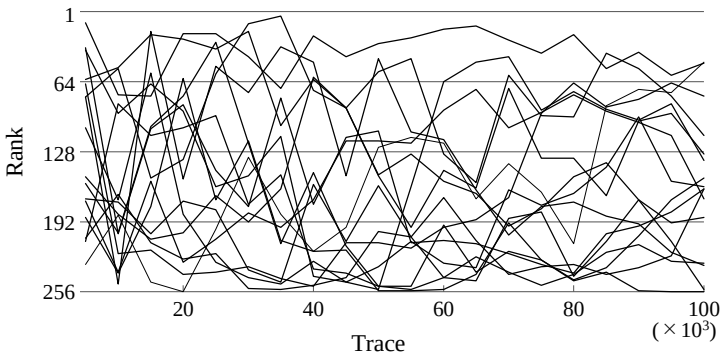


図 4.25　疑似 RSL-1 への ZO-DPA による部分鍵の順位

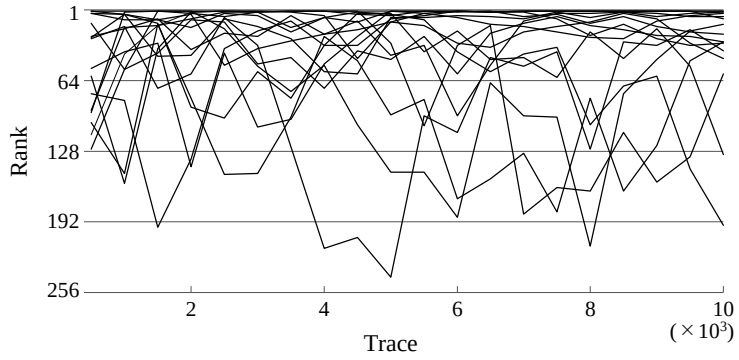


図 4.26　DIFF 入力による疑似 RSL-1 への ZO-DPA による部分鍵の順位

図 4.25 と 4.26 の疑似 RSL への ZO-DPA では，データを偏らせることで乱高下はあるものの正しい部分鍵の順位が上位に偏っており，何らかの情報のリークがあると見られる．それでいながら同じデータセットを用いた図 4.24 の T 値にピークが観測されないのは，T 検定が 1 bit の情報を用いているのに対して，ZO-DPA はハミング重みを偏らせた上で 8 bit の情報を集めているためと考えられる．したがって，提案手法による T 検定は今回 1 万波形であったが，10 万波形に増やすことでリークが検出できる可能性がある．

図 4.27~4.29 は，FPGA に実装した AES 回路と同等のノードを持つよう制約が与えられた疑似 RSL 回路に対する T 検定の結果である．WDDL，MDPL，MAO に比べてピークが低く，またビットやラウンドによってピークが出たりでなかったりしていた．そこで一番高いピークが表れたビット（グラフ右に数字で表示）を選び，10 ラウンド分表示している．全ての着目ビットに対して対応するラウンドにピークが出るわけではない．しかし図 4.28 や 4.29 のように，それらを集めると連続してピークに移動のあることがわかる．

ところで図 4.28 では，9 ラウンドの出力による振り分けで，1 ラウンドに高いピークが現れている．原因は不明だが，明らかに誤ったピークである．しかし ISO/IEC 17825 の評価手順では，このような誤ったピークが生じてもテストは Fail となってしまう．したがって，T の絶対値が閾値の 4.5 を超えたかどうかだけでなく，その T 値のピークが着目ビットのラウンドまたは次のラウンドに出ているかどうかを調べる必要がある．さらにループアーキテクチャであれば，同じラウンド関数ブロックを繰り返し使用する処理の中で，着目ビットによる波形の振り分けを行うのであるから，リーク情報があるならば図 4.28 のようなピークの移動が生じるはずで，そのチェックも不可欠である．

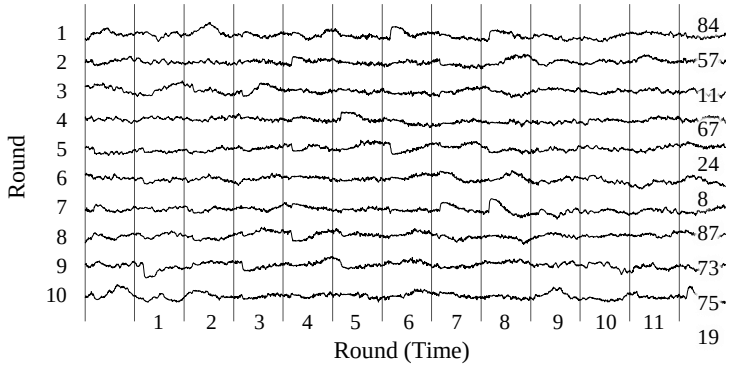


図 4.27　疑似 RSL-2(Level 3, Test 3)

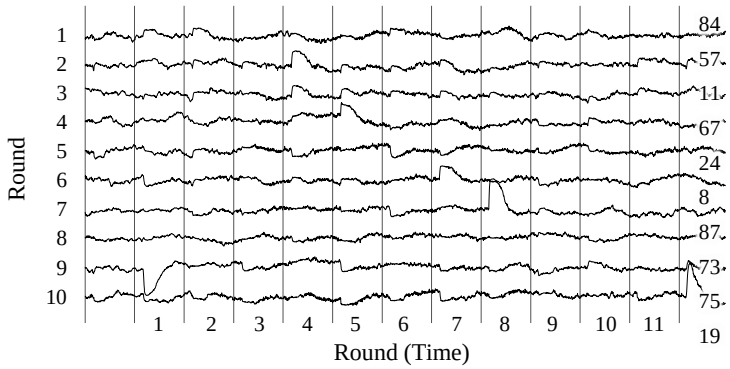


図 4.28　疑似 RSL-2(Level 4, Test 3)

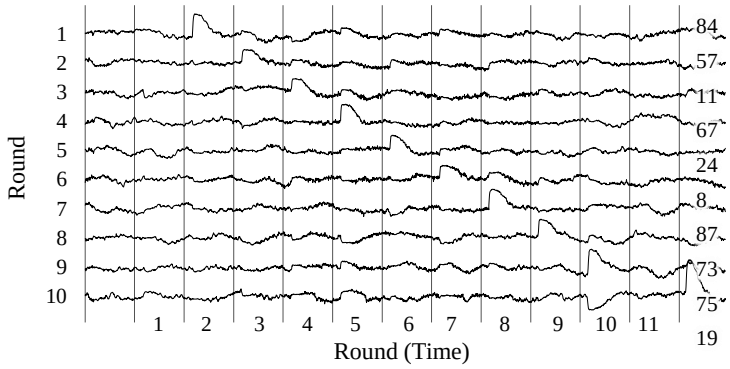


図 4.29　疑似 RSL-2(DIFF, Test 3)

図 4.30 と図 4.31 は ZO-DPA の結果で，ランダムデータと偏りを持たせたデータいずれにおいても，全ての鍵の順位が高いことは，T 検定で正しいリーク情報が捉えられることを裏付けている．

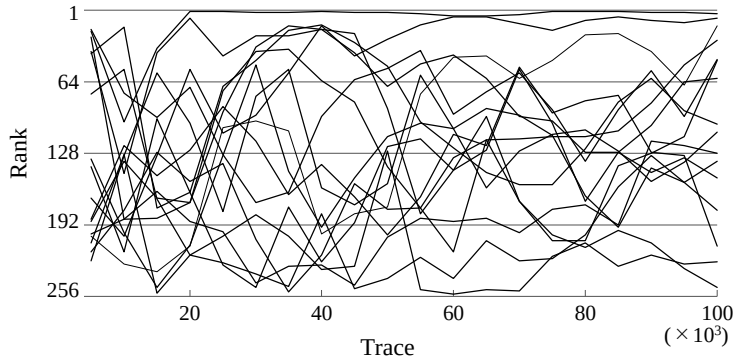


図 4.30　RSL-2 への ZO-DPA による正しい部分鍵の順位

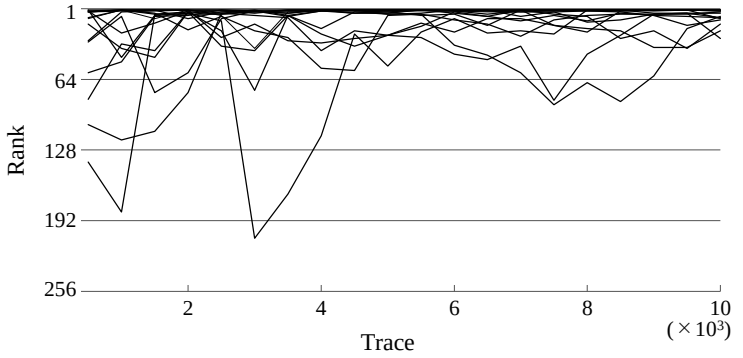


図 4.31　DIFF 入力による RSL-2 への ZO-DPA による正しい部分鍵の順位

図 4.32～4.34 は，Sbox の出力ビットで波形を振り分ける Test 2 に対する疑似 RSL-2 の T 検定結果である．提案手法では Test 3 のラウンド出力 $R$ を偏らせたデータを用いているが，それは次のラウンドの Sbox 入力となるため，結果としてリーク情報が強調され，T 値のピークがラウンドに依存して移動している様子が図 4.33 や 4.34 で見られる．したがって，提案手法で Test 3 のためにデータを偏らせて取得した波形は，Test 2 にも有効であるということがわかる. しかし, 図 4.35 と 4.36 に示したように, Sbox 出力で振り分ける ZO-DPA では，正しい部分鍵の順位の推移に何らかの傾向が見られるものの鍵は求まらなかった．これは，最終ラウンドは MixColumns がスキップされるため Sbox 出力が影響を与える回路が AddRoundKey だけで，十分なリーク情報が得られないためではないかと考えられる．また図 4.33 と 4.34 でも，10 ラウンドには T 値のピークは見られなかった.

以上の実験結果から，T 検定だけ，あるいはサイドチャネル攻撃だけではなく，双方によって総合的に情報の有無を判断することが不可欠であると言える.

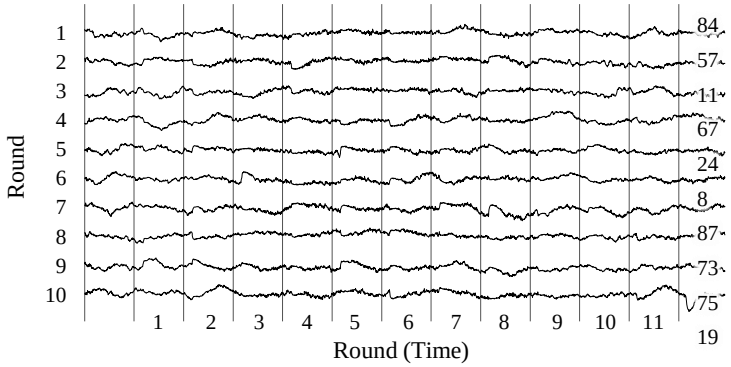


図 4.32　疑似 RSL-2(Level 3, Test 2)

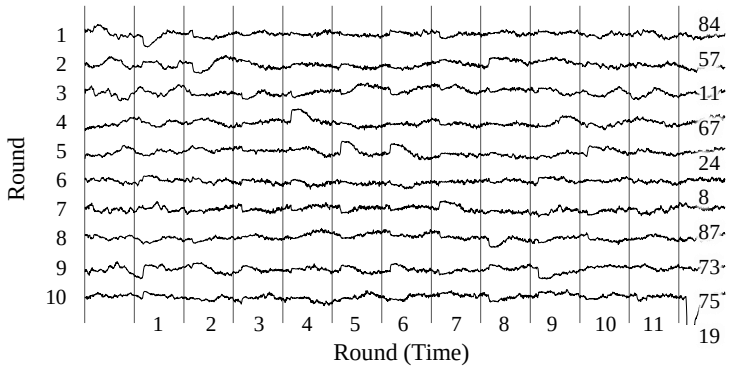


図 4.33　疑似 RSL-2(Level 4, Test 2)

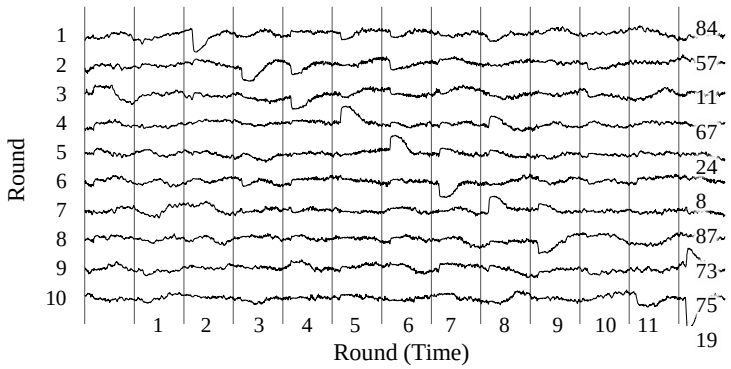


図 4.34　疑似 RSL-2(DIFF, Test 2)

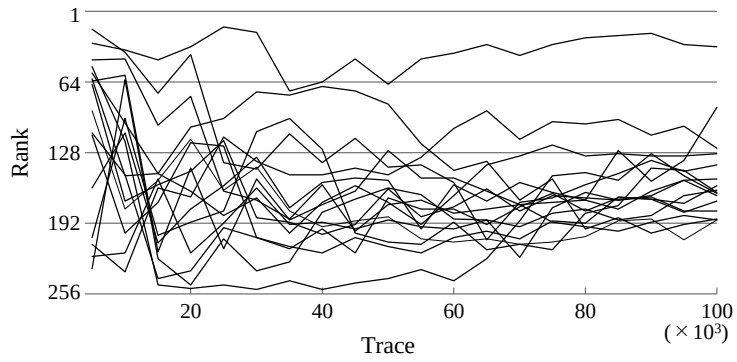


図 4.35　RSL-2 への ZO-DPA による正しい部分鍵の順位（Sbox 出力）

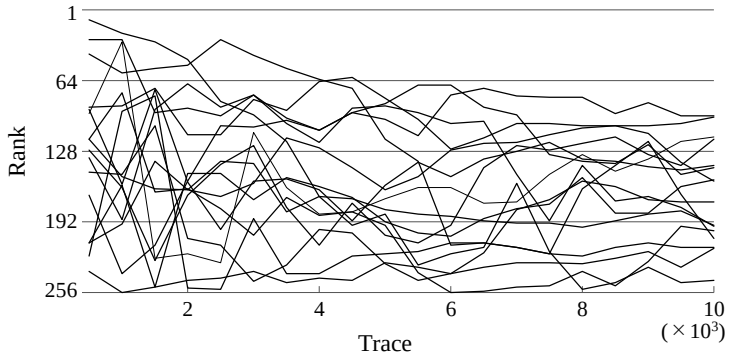


図 4.36　DIFF 入力による RSL-2 への ZO-DPA による正しい部分鍵の順位
（Sbox 出力）

# 5 結論

本研究では，暗号モジュールのサイドチャネル攻撃に対する安全性評価の，高精度化と低コスト化を目的に新たな評価手法を提案し，暗号ハードウェアを用いた実験でその有効性を検証した．

従来のサイドチャネル攻撃の研究は，暗号モジュールの外部から電力・電磁波等を観測して，そこに漏れている情報から内部状態を統計解析して暗号の秘密鍵を推定するものであった．しかし，暗号モジュールの開発者あるいは善意の第三者による安全性評価という立場においては，攻撃者のように秘密鍵を盗み出すことが目的ではなく，秘密鍵やモジュールの内部状態がサイドチャネル情報として洩れているかどうかを調べることが重要となる．つまり攻撃は漏れている情報から鍵を求めるのに対して，安全性評価は鍵の情報が洩れているかどうかを調べるという逆のことを行う．もちろん，攻撃によって鍵が求まればそれは情報が漏れていたことを意味するが，多くの鍵候補の中から正解の秘密鍵を導出するため，電力波形・電磁波形の計測および鍵候補との相関値の計算に大きなコストが必要とされる．そこで，評価者の立場から秘密鍵および，それ用いて処理されるモジュール内部のデータを把握した上で，それと波形データとの間の相関値を調べることで無駄な計算を削減することが可能となる．これ ISO/IEC 17825 に採用されたウェルチの T 検定を用いた評価手法である．

本研究の提案手法はこれをさらに一歩進め，サイドチャネル情報が漏洩しやすいように内部状態を制御しようというものである．消費電力や放射電磁波は，暗号モジュール内部のトランジスタがスイッチングすることによって生じ，そのスイッチングは演算データのパターンに応じて発生し，その演算データとして秘密鍵が用いられるため，それがサイドチャネル情報として漏洩する可能性が生じる．しかしその情報は弱く，時として周辺回路が発生するノイズに埋もれてしまい，そのため多数の電力波形や電磁波形を取得して統計解析する必要がある．そこで，より情報が漏洩しやすい，つまり演算によって生じる波形データの強弱が付きやすいようにモジュール内部のデータを制御することで，ノイズの影響を低減しようというものである．具体的には，16Byte の中間値で解析対象のバイト中の 1 の数（ハミング重み）が 0，1，7，8 の 4 種類に偏るように入力平文を選択した．

提案手法の有効性を示すために，様々なサイドチャネル攻撃対策を施した AES 回路を実装した FPGA ボード SAKURA-G および，それを 90nm スタンダードセルライブラリで実装した暗号 LSI を搭載した SASEBO-RII に対して，ランダムデータを用いた通常の T 検定および，中間値を偏らせた T 検定を実行した．その結果，提案手法は通常の T 検定に対して 1/10 程度の波形数でもリーク情報を検出でき，あるいは通常の手法では見えない情報も検出できることを示した．

ISO/IEC 17825 の T 検定では，暗号処理中の各ラウンドに，中間値の特定のビット

で波形を 2 つの母集団に分けて T 値を計算し，その絶対値が 4.5 を超えた時に中間値の情報が漏洩していると判断するものである．しかし，解析しているラウンド処理以外のラウンドで，T 値に 4.5 を超えるピークが見られることもあり，これは明らかに本来の情報漏洩とは別の原因によるものと言える．したがって，単に T 値の絶対値だけで判断するのではなく，ピーク値がラウンド処理の進行に合わせて，次第に移動していくことをグラフ上で確認することも重要であることを明らかにした．

また T 検定の他に，様々なサイドチャネル攻撃と波形数を順次増やしながら実施し，正しい部分鍵が $2^8$=256 個の鍵候補の中で何番目に高い相関値を有するかをグラフ化した．正しい部分鍵が 1 位となった場合に攻撃が成功したことになるが，たとえそうでなくても，安全性評価という立場からは部分鍵が高い順位にあれば何らかの情報が洩れていることを意味する．ここでもデータを偏らせることで正し鍵が上位に表れることが確認され，ランダムデータでは見えなかったリーク情報の検出に成功した．

対策手法に疑似 RSL を用いた暗号 LSI 上の AES 回路は，データを偏らせた T 検定でもサイドチャネル情報が検出できなかった．ランダムデータを用いたサイドチャネル攻撃（Zero Offset DPA）でも鍵は求まらなかったが，データを偏らせることで部分鍵の順位が上位側に寄るようになり，なんらかの情報がリークしている様子がうかがえた．T 検定よりもサイドチャネル攻撃のほうがリーク情報に敏感であったのは，前者が 1bit の中間値で波形を分けているのに対し，後者は中間値の 8bit を使って解析しており，その分情報が多いためと考えられる．したがって，T 検定でもさらに波形を増やすことで T 値にピークの移動が見られる可能性がある．

以上の結果から，ハミング重みを偏らせたデータを用いる提案手法は T 検定だけでなく，サイドチャネル攻撃にも有効であることが明らかとなった．ISO/IEC 17825 で採用された T 検定は，暗号アルゴリズムの構造を一切理解する必要がなく，機械的に中間値から判定基準の T 値を出力してくれるため，非常に汎用性の高い便利な解析手法である．しかしながら，情報のリークがないはずのラウンドに T 値のピークが出ることがあり，またサイドチャネル攻撃で検出できた情報も検出できない場合がある．また，T 検定は内部状態を全て把握できるという極めて有意な条件の下での解析のため，そこで情報のリークが見られたとしても，それが直ちに暗号モジュールが実用に耐えない脆弱性を有しているということにはならない．すなわち，T 検定は情報がリークする可能性があるという 1 次スクリーニングに用いるべきものである．したがって，サイドチャネル攻撃等と他の解析手法と合わせて，総合的な判断を行うことが暗号モジュールの安全性を担保するうえで不可欠であろう．

# 6　謝辞

本研究を進めるにあたり，指導教官の佐藤証教授から，丁寧かつ熱心なご指導を賜りました．また論文を何度も推敲していただき明確な文章にしていただきました．心より感謝いたします．

また，佐藤研究室の同期・後輩の方々，特に松林雅人氏と野亦優氏のご協力をいただいて心より感謝いたします．

# 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, J. Jaffe, and B. Jun, “Differential power analysis,” CRYPTO ’99, LNCS 1666, pp. 388-397, Aug. 1999.

[3] ISO/IEC 19790:2006, “Information technology – Security techniques – Security requirements for cryptographic modules.”

[4] ISO/IEC 24759:2008, “Information technology – Security techniques – Security requirements for cryptographic modules.”

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

[6] 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

[7] AIST, “Evaluation Environment for Side-Channel Attacks.”
http://www.risec.aist.go.jp/project/sasebo/

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

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

[10] 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.

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

[12] 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.

[13] 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.

[14] 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

[15] 産業技術総合研究所, “標準暗号LSI仕様書 ~サイドチャネル攻撃対策版~ [第1.0版]”, 2009年8月.

https://www.risec.aist.go.jp/project/sasebo/download_prev/CryptoLSI2_Spec_Ver1.0_Japanese.pdf

[16] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” in CHES 2004, Lecture Notes in Completer Science, vol. 3156, pp. 16–29, 2004.

[17] 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.

[18] ISO/IEC18033, “Information technology - Security techniques - Encryption algorithms” http://www.iso.org/iso/catalogue_detail.htm?csnumber=54530

[19] INSTAC, “平成 14 年度耐タンパー性調査研究委員会報告書.” http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/documents/INSTAC rep.pdf, 2003

[20] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton, “On the importance of checking cryptographic protocols for faults,” Advances in Cryptology - EUROCRYPT ’97, Vol. 1233, pp. 37–51, 1997. http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/AttaquesParFautes/boneh97importance.pdf

[21] P. Kocher, R. Lee, G. McGraw, and A. Raghunathan, “Security as a new dimension in embedded system design,” in DAAC ’04, Proceedings of the 41th annual conference on Design automation, New York, USA, pp. 753-760, ACM Press, 2004. https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/SecurityEmbeddedSystemsDAC.pdf

[22] R. Bevan and E. Knudsen, “Ways to Enhance DPA,” International Converence on Information Security and Cryptology (*ICISC 2002*), LNCS 2587, pp.32342, Springer-Verlag, Dec. 2003.

[23] J. Waddle and D. Wagner, “Towards Efficient Second-Order Power Analysis,” Cryptographic Hardware and Embedded Systems (*CHES 2004*), LNCS 3156, pp. 1-15, Springer-Verlag, Aug. 2004.

[24] “SAKURA hardware security project” http://satoh.cs.uec.ac.jp/SAKURA/tools.html

# 付録