令和 7 年度

修士学位論文

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

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

市ノ木 一希

指導教員　岩田 誠

2026 年 2 月 27 日

高知工科大学大学院 工学研究科 基盤工学専攻

情報学コース

要 旨

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

近年，IoT(Internet of Things) デバイスが様々な分野で活用されるに伴って，高いセキュリティも求められている．特に，電力解析攻撃等のサイドチャネル攻撃 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，電磁波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し，鍵推定により秘密鍵の取得が可能か検証することで，提案回路における電磁波解析攻撃耐性を確認した．

キーワード　IoT，AES, FPGA, サイドチャネル攻撃, 電磁波解析攻撃, 非同期暗号化回路

Abstract

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

Kazuki ICHINOKI

In recent years, as IoT (Internet of Things) devices have been widely deployed across various fields, stronger security measures have become increasingly important. In particular, there is an urgent need to develop circuit technologies that are resistant to side-channel attacks (SCAs), such as power analysis attacks, which attempt to extract secret cryptographic keys.

Meanwhile, to accommodate the diverse application requirements of IoT devices, they are often implemented using reconfigurable FPGA (Field-Programmable Gate Array) devices rather than dedicated ASIC (Application-Specific Integrated Circuit) chips. In this study, we focus on an AES (Advanced Encryption Standard) encryption circuit and investigate an FPGA implementation method that provides resistance against electromagnetic (EM) analysis attacks using EM probes.

The proposed circuit employs a self-timed data transfer control mechanism to realize asynchronous pipelined processing, thereby horizontally (temporally) concealing the execution timing of round operations. To evaluate the effectiveness of the proposed design, we conducted practical EM analysis attacks on both a conventional synchronous AES circuit without EM attack countermeasures and the proposed circuit. By attempting secret key extraction through key estimation, we verified whether the secret key could be successfully recovered. The experimental results confirm that the proposed

circuit demonstrates resistance against electromagnetic analysis attacks.

key words IoT, AES, FPGA, SCA, CEMA, Asynchronous cryptographic circuit

目次

目次

目次

図目次

図目次

表目次

第 1 章

序論

IoT(Internet of Things) デバイスが様々な分野で活用されるに伴い，高いセキュリティも求められている．特に，EM プローブを用いた電力解析攻撃等のサイドチャネル攻撃によって暗号鍵を盗み出す行為に対しても耐性を有する回路技術の開発が急務となっている．電力解析攻撃とは，消費する電力の違いから暗号鍵を推測する方法であり EM プローブを用いて波形の変化から鍵を取得する．セキュリティ対策を施していない AES 暗号回路では電力解析攻撃により 1bit あたり 0，1 の 2 回の攻撃により解析が可能であるため，128bit の場合は 256 回の解析により共通鍵の取得されてしまう．また，IoT デバイスの応用分野が多岐にわたるため ASIC(Application Specific IC) チップではなく，回路の書き替えが可能である FPGA デバイスによって実現されることが多い．そのため本研究では，身近な暗号であり Wi-Fi やファイルの暗号化などに使用されている AES(Advanced Encryption Standard) 暗号化回路を対象とし，電磁波 EM プローブによる電力解析攻撃に対する耐性を備える AES 回路の FPGA 実装法について検討した [1]，[3].

本研究では，第 2 章では AES の動作概要およびハードウェア AES 暗号回路の課題や主な対策方法について説明を行い，その後水平隠蔽を施した非同期 AES 暗号回路の設計方針について述べる．方針内容として，STP(Self-Timed Pipeline) を使用し，AES 暗号回路を非同期化することによってセキュリティ対策の一種である水平隠蔽を導入することを検討した．第 3 章では，FPGA に AES 暗号回路を実装した際の攻撃の種類および攻撃手法を説明する．本研究では，サイドチャネル攻撃の 1 種である，電磁波解析攻撃を用いて攻撃を行った．第 4 章では，第 2 章で検討した非同期 AES 暗号回路を実際に設計を行い，問題点を考察し改善案の提案および回路設計を行う．具体的には，設計回路構成を示すとともに各モジュー

ルについて説明を行う．また，改善した回路構成において変更点を示すことで提案回路の違いを明確化している．

第 5 章では，提案回路および比較対象として同期回路に対し，FPGA に実装した場合の回路規模・実行時間等の実装評価を行った．また，電磁波解析攻撃耐性を確認するため，電磁波解析攻撃を行う．結果として，提案回路にはセキュリティ対策が施されていない同期回路と比較して電磁波解析攻撃耐性を有している可能性が高いことを確認した．

第 6 章では，本研究で設計した提案回路についてのまとめおよび今後の課題と課題の解決策の構想について述べる．

第 2 章

電磁波解析攻撃を有する非同期 AES 暗号回路の設計方針

2.1 緒言

本章では，電磁波解析攻撃耐性を有する AES 暗号回路を IoT デバイスに実装することを目的とし回路設計を行う．そのため AES 暗号回路のセキュリティ対策として水平隠蔽を施すためのセルフタイム型パイプライン (Self-Timed Pipeline) を使用した非同期 AES 暗号回路を FPGA 向きに設計する．そこで本章では FPGA，AES およびハードウェア AES 暗号回路のセキュリティ対策や STP についての詳細を述べる．

2.2 FPGA

FPGA(Field Programmable Gate Array) とは特定の用途向けに設計されたものでなく，様々な用途に向け回路設計者が回路構成を変更することが可能である集積回路である．開発ツールを用いることにより容易に回路構成を変更することや新たな回路構成を設計することが可能であり，ASIC とは異なり設計期間の短縮が可能であり，回路設計のみの実装を行うことで，FPGA を購入する以外のコストを抑えることが出来る．本研究では，回路構成をする際には，ハードウェア記述言語により記述された RTL から開発ツールによって論理合成から配置配線が行われる．また，その後 FPGA に実装する前にシミュレーションを行うことが可能であるため，試験的な実装だけでなく実装前の動作確認をすることも可能であ

る．本研究では AMD 社の Zynq-7010 を使用する．LUT や FF 等から構成されるスライスとデータの保持が可能である BlockRAM から論理合成を行うことが可能であるため使用できる最大リソースまでであれば様々な複雑な回路の設計，構成が可能である．

2.3　AES

AES の暗号処理動作を図 2.1 に示す．AES は 128bit，192bit，256bit の 3 種類が存在するが基本的な動作は同じである．まず，暗号化を行う 4 つの処理を記述する．

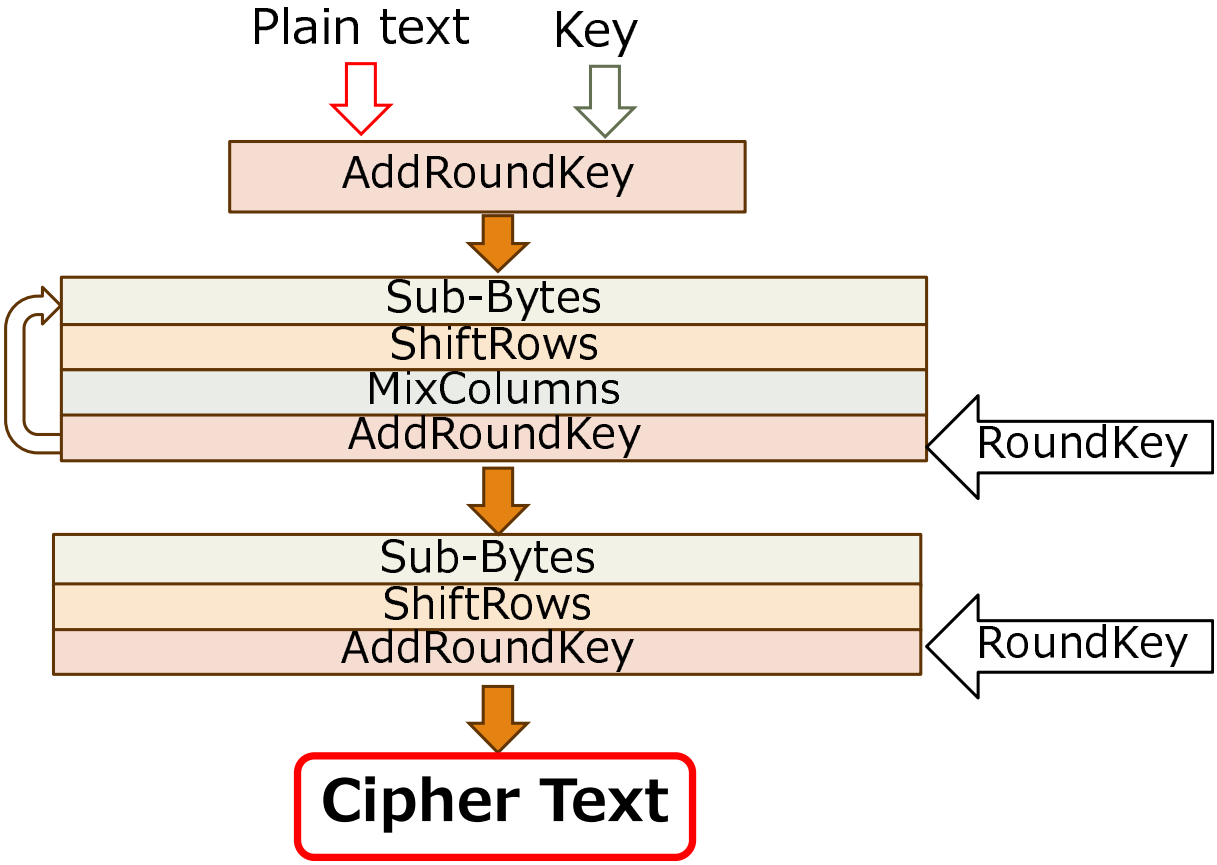

図 2.1　AES の暗号処理動作

- Sub-Bytes

  動作のイメージを図 2.2 に示す．各バイトを S-box というテーブルを用いて変換する．S-box は 0x00 から 0xff の入力された数字を 1 対 1 で対応する数字に変換を行うための

テーブルである．

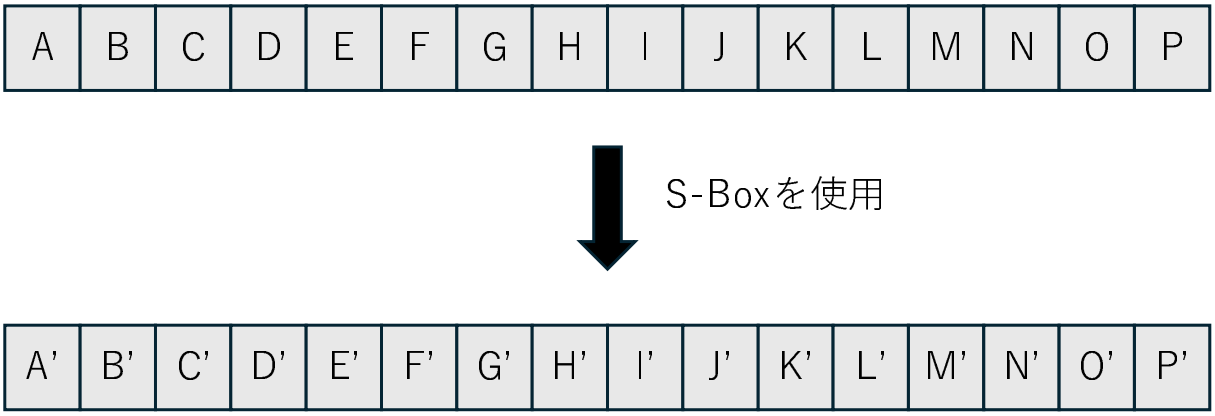

図 2.2　SubBytes の動作イメージ

また，以下に S-Box の変換テーブルの一部を図 2.3 に記載する．

	0	1	2	3	…	d	e	f
0	63	7c	77	7b	…	d7	ab	76
1	ca	82	c9	7d	…	a4	72	c0
2	b7	fd	93	26	…	d8	31	15
3	04	c7	23	c3	…	27	b2	75
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
d	70	3e	b5	66	…	c1	1d	9e
e	e1	f8	98	11	…	55	28	df
f	8c	a1	89	0d	…	54	bb	16

図 2.3　SubBytes の変換テーブル (S-Box) の一部

- ShiftRows

  各バイトの順番を入れ替える．4 × 4 の 2 次元配列に格納し，2 行目を 1byte，3 行目を 2byte，4 行目を 3byte 左にシフトする．動作方法を図 2.4 に示す．

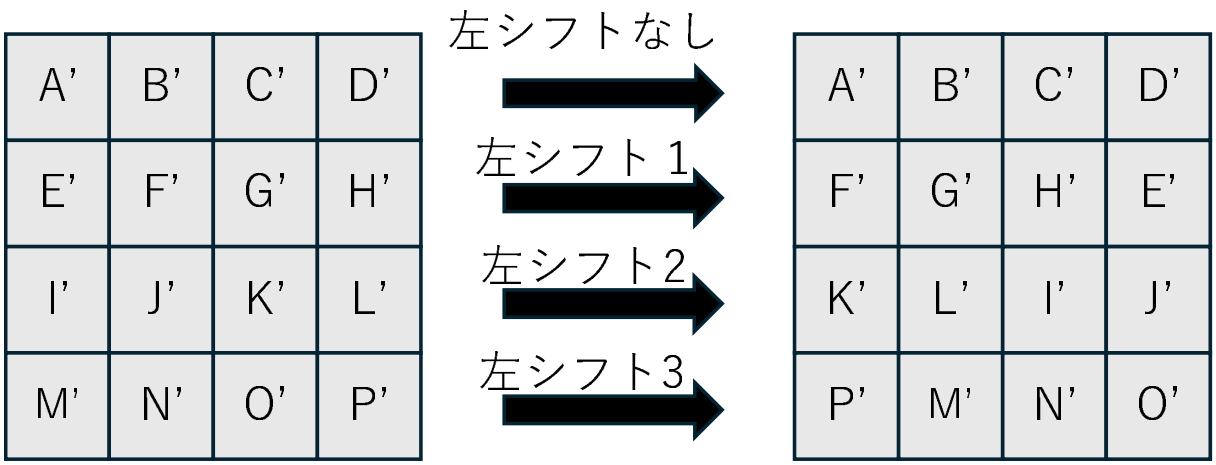

図 2.4　ShiftRows の動作イメージ

- MixColumns

  処理方法を図 2.5 に示す．ShiftRows の結果を用いて 4Byte 毎に行列演算を行う．

図 2.5　MixColumns の動作イメージ

- AddRoundKey

  ラウンド鍵を使用し変換する．MixColumns の計算結果を暗号化 bit と同じ bit 数のラウンド鍵を 4 × 4 の 2 次元配列にし，それぞれを排他的論理和を取る．処理方法を図 2.6 に示す．

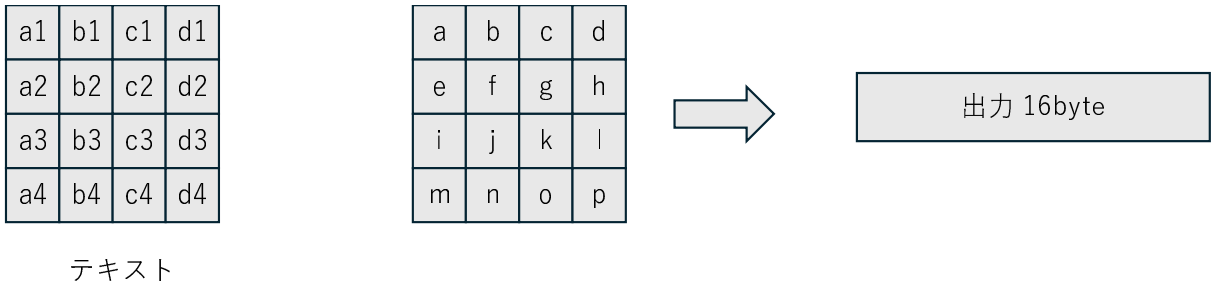

図 2.6　AddRoundkey の動作イメージ

Sub-Bytes，ShiftRows，MixColumns，AddRoundKey の順に処理を行い，4 つの処理をまとめてラウンドと言う．AES の暗号化の bit 数によりラウンドの処理回数が異なり，128bit，192bit，256bit それぞれ 9 回，11 回，13 回実行する．また，ラウンド処理が終了した後に MixColumns 以外の 3 つの処理を行い暗号化を行う．AES 暗号化の逆手順を行うことで復号となる．また，AddRoundKey に用いられるラウンド鍵は最初の 1 回は入力された鍵を用いて，その後鍵を変更しながらラウンド鍵を生成する．ラウンド鍵は拡張ルーチンにより生成される．処理を以下に記述する．

- RotWord

  入力された鍵を 4 バイト毎に分け，左方向に循環シフトさせる．
- SubWord

  4 バイトごとに S-Box 変換を行う．
- Rcon

  ラウンド毎に定められている定数を加算する．

ラウンド鍵の生成方法を図 2.7 に示す．この処理は鍵の 4Word 周期で行われるため 128bit の場合には最上位から 4byte のみをこの処理を行う．また，演算結果と直前の 4byte を排他的論理和を取ることを繰り返すことでラウンド鍵の生成を行っている．

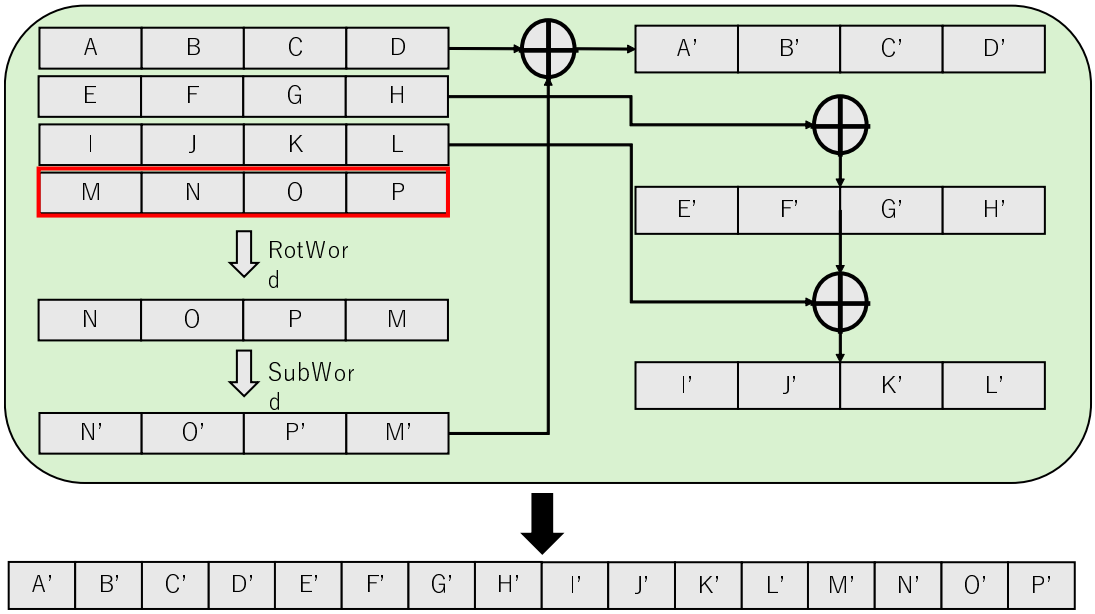

図 2.7　ラウンド鍵の生成方法

2.4　ハードウェア AES 暗号回路に施すセキュリティ対策

今回の AES 暗号に施すセキュリティ対策は IoT デバイス向けの実装となるためハードウェアに実装した AES 暗号回路となる．そのため，実装可能となる対策としてマスキングと隠蔽の手法が主に用いられる．

2.4.1　マスキング

この対策法は元の文字や数字を変更し，データを隠すプロセスである．しかし，問題点としてマスクのランダム性を保証する真の乱数発生器が必要となることに加え複雑であり高いオーバーヘッドが発生することが挙げられる．

2.4.2　隠蔽

この対策法は対策目的となる電力解析攻撃のターゲットである物理漏洩情報 (PLI) を均一化またはランダム化することで解析を不可能にする方法である．しかし問題点として面積及

びエネルギーのオーバーヘッドの抑制が必要となる．また，隠蔽方法として 2 種類あり，垂直隠蔽は図 2.8 のように，波形のハミング距離を一定にすることでどの bit を変更しているかを分からなくする手法である．この方法の問題点として，不均衡なルーティングが発生することに加えハードウェア暗号を脆弱にする早期伝播効果 (EPE) が大きくなりやすいことが挙げられる．また，水平隠蔽の手法では図 2.9 のように，PLI を時間内にランダムにすることによる非同期化を行うことで，暗号化のタイミングを分からなくする方法である．この方法の問題点としてタイミングをずらすために暗号化に不必要な回路を実装するため，面積やエネルギーのオーバーヘッドが大きくなりやすいことが挙げられる．本研究では，IoT デバイス向けとして回路のみの実装が可能である水平隠蔽を対象とした．

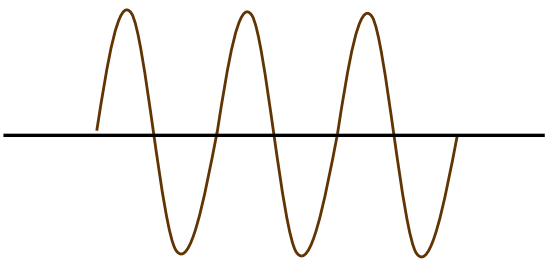

図 2.8　垂直隠蔽を施した波形のイメージ図

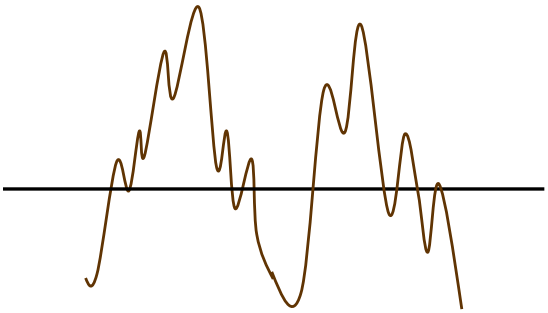

図 2.9　水平隠蔽を施した波形のイメージ図

2.5　STP

STP の構成を図 2.10 に示す．STP は非同期回路であり，パイプラインステージのデータ転送にデータ転送制御回路 (以下，C 素子：Coincidence flip-flop) を用いる．STP では，パイプライン構成として，C 素子，データラッチ (DL)，データ処理回路 (Logic) からなる．図にパイプライン構成を示す．パイプラインステージ構成の i 段目の Logic の処理と並行して同段の C 素子 C_i が，後段の C 素子 $C_{\{}\ i+1\}$ に対してデータ転送要求信号 Send を送信する．その後, 後段の DL にデータ転送が可能である場合は $C_{\{}\ i+1\}$ から C_i に対して転送許可信号 Ack を返信する．Ack を受信した場合もう一度 C_i から $C_{\{}\ i+1\}$ に向け Send 信号が送られ，$C_{\{}\ i+1\}$ はデータラッチ解放信号である CP 信号を立ち上げ DL にデータが

転送される．このように動作することでクロックによる動作でなく，隣接する C 素子同士が Send 信号および Ack 信号によるハンドシェイクを行うことでデータ転送が必要なパイプラインステージのみの動作が可能となるため低消費電力を実現している．

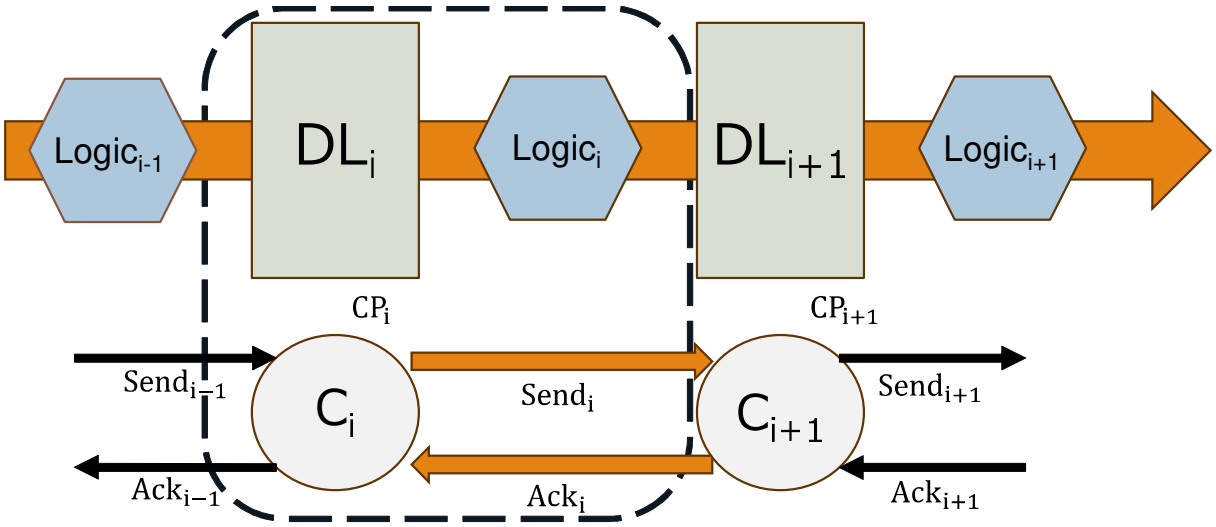

図 2.10 セルフタイム型パイプライン (STP) の構成

本研究では，データ転送制御回路に加え非同期回路内において様々な処理を行うことを可能にするためデータ転送の他に動作することが可能である複合データ転送制御回路 (以下：複合 C 素子) を使用している．使用した複合 C 素子について以下に記述する．

2.5.1 データ転送制御回路 (C 素子)

複合 C 素子の前に STP について説明した際に動作方法を記述した C 素子についてのゲートレベルの回路図を図 2.11 に記載する．本回路では，隣接する C 素子とデータ転送制御を行う．

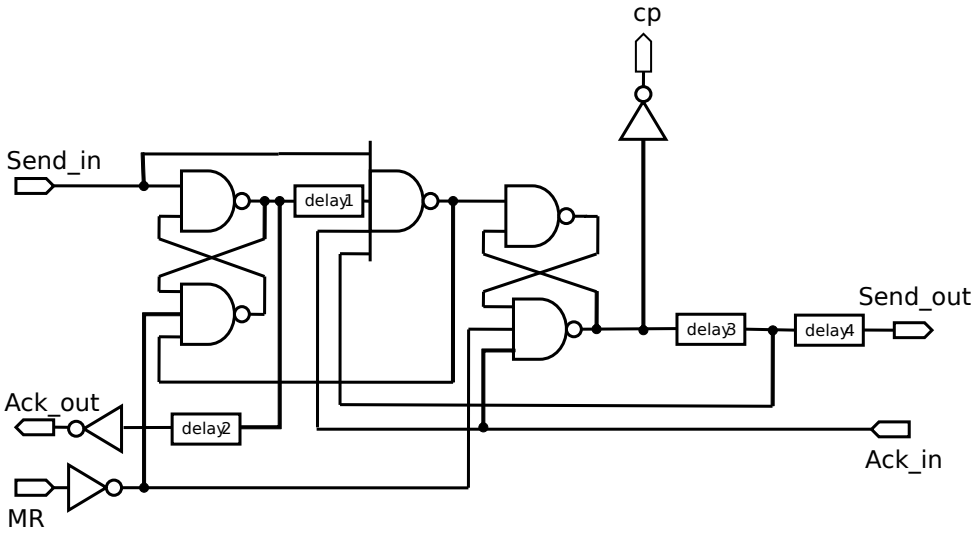

図 2.11 データ転送制御回路

2.5.2 データ転送合流調停制御回路 (CM 素子)

CM 素子の構成を図 2.12 に示す．本回路では，上下に 2 つの C 素子を使用し構成している．2 つの C 素子を用いることで転送されてくるデータを 2 つに増加させることが可能である．そのためデータの衝突が起こらないようにするために，ga, gb 信号によってどちらの Send 信号が先に入力されたかを確認することでデータ転送される入力先を決定することが可能である．また，2 つから送られる信号から返信する信号を決定するため，ハンドシェイクを行っている前段を明確にしている．

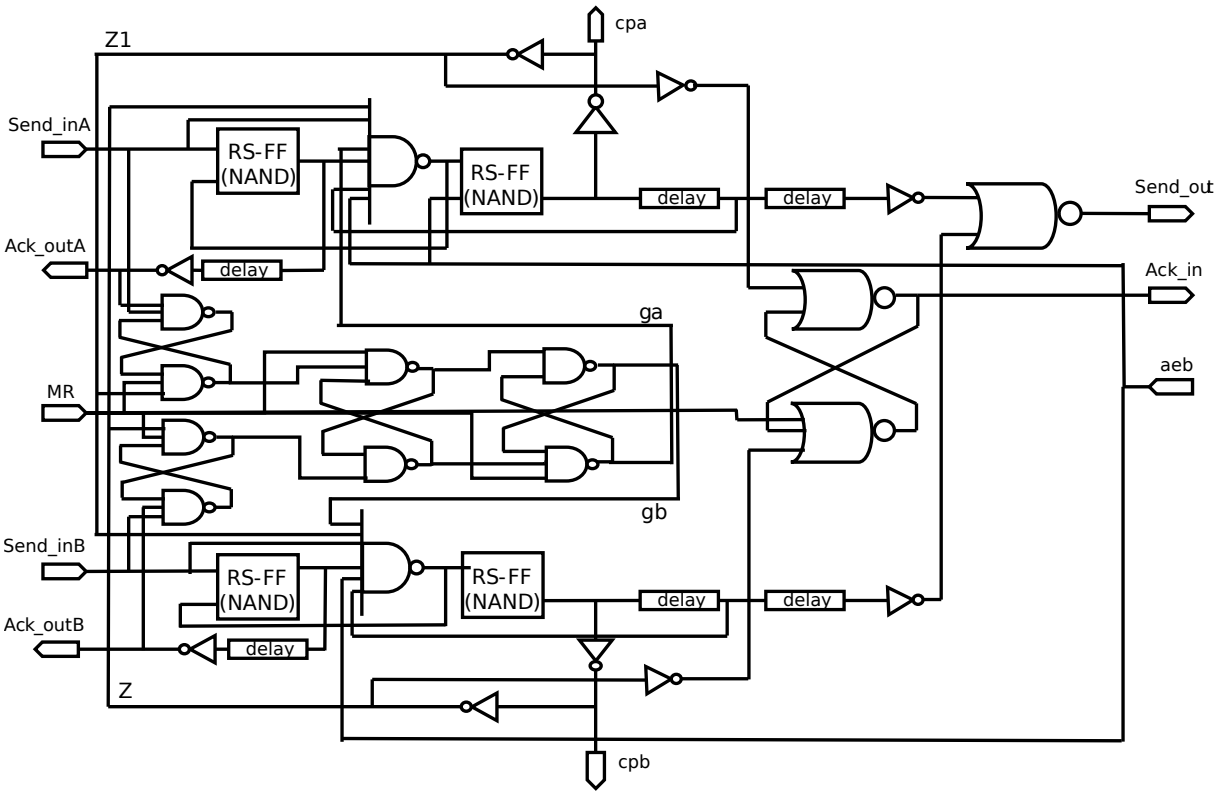

図 2.12　データ転送制御合流調停回路

図 2.12 に記載している RS-FF の構成を図 2.13 に示す.

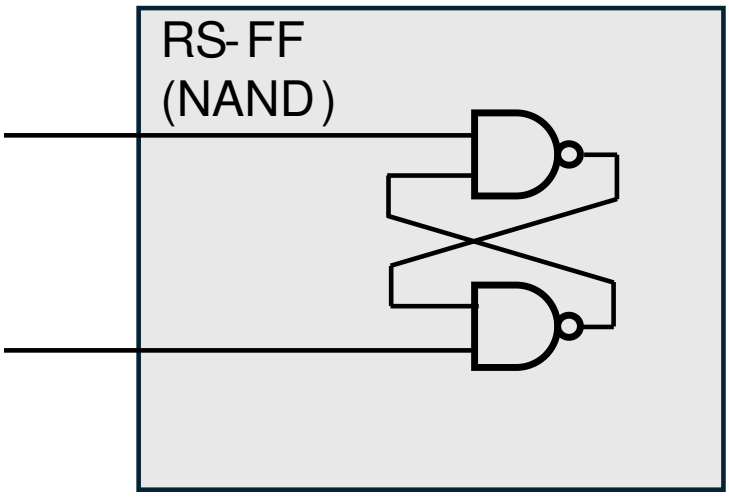

図 2.13　RS-FF 構成図

2.5.3 データ転送削除制御回路 (CE 素子)

CE 素子の構成を図 2.14 に示す．本回路では，データの削除を行うことが可能であり，exb 信号において削除機能の制御を行っている．削除機能が動作する場合には，後段との Send/Ack のハンドシェイクを行わず前段のみとデータ転送の制御を行うため，後段にデータが転送されずに前段のデータが転送されてくることにより DL に格納されているデータが上書きされることで，削除機能が動作したデータを削除することが可能となる．

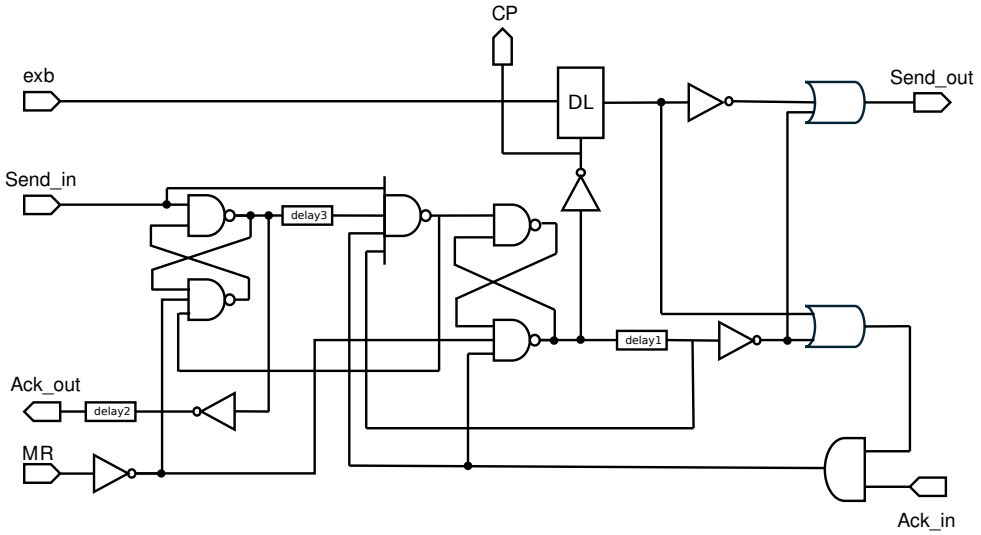

図 2.14 データ転送削除制御回路

2.5.4 データ転送分岐制御回路 (CB 素子)

CB 素子の構成を図 2.15 に示す．本回路では，データの出力を分岐させることが可能である．図より br 信号により転送先の分岐制御を行っている．この方法により 2 つの Send 信号から 1 つを選択し送信することが可能であるためどちらか一方とハンドシェイクを行うことで分岐を行いデータの出力を決定している．

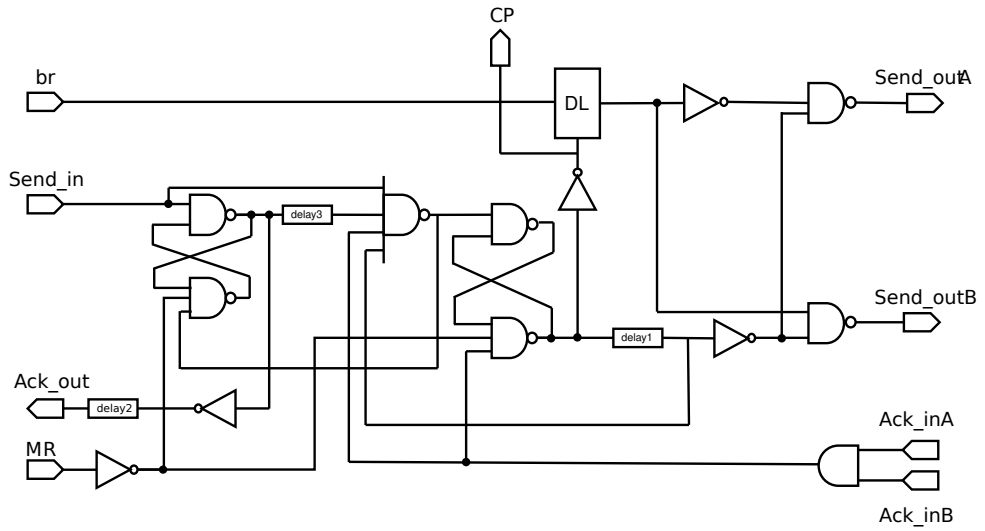

図 2.15　データ転送分岐制御回路

2.5.5　データ転送同期回路 (CS 素子)

CS 素子の構成を図 2.16 に示す．本研究では，AES 暗号回路を非同期にする際にラウンド数の調整が必要となるため回路全体を簡単な同期をとる必要が生じた．そのため，新たな複合 C 素子として CS 素子を設計した．上記で説明した C 素子を元に，同期させた信号を前段の Send 信号のみでなく，同期させたいものから出力される信号の入力により動作する．前段の Send 信号と同期信号が同時に入力状態になった時のみハンドシェイクがハンドシェイクを行う．

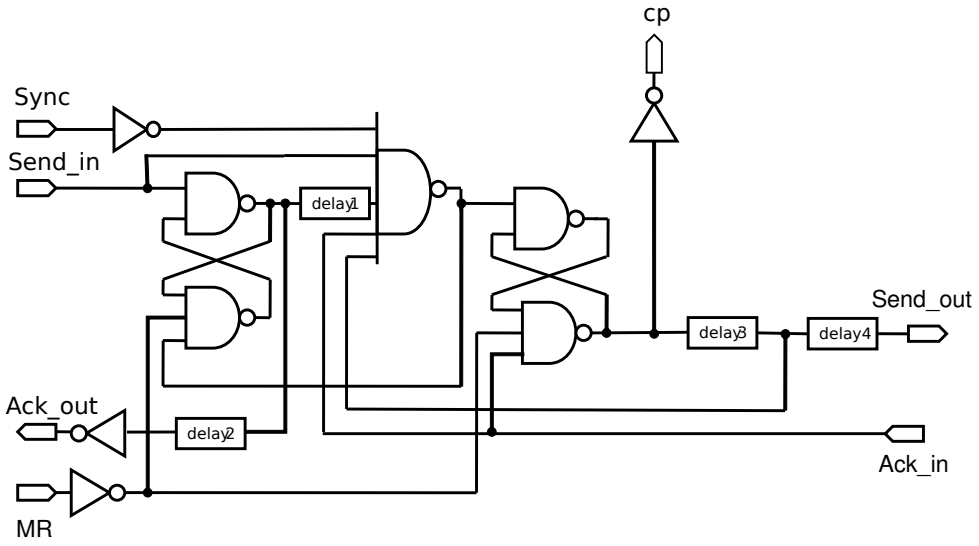

図 2.16　データ転送同期制御回路

2.6　非同期 AES 暗号回路の設計の課題

本研究の目的は，IoT デバイスに実装する AES 暗号回路へのセキュリティ対策である．そのため，真の乱数発生器を導入する必要があるマスキングはコスト面等を考慮し導入せず，STP による FPGA 向きの AES 暗号回路設計を行うことから水平隠蔽の導入を行った．そのため，水平隠蔽の課題である面積およびエネルギーのオーバーヘッドを考える必要がある．エネルギー面に関しては STP による導入であるため，低消費電力での動作が可能であることから面積を評価指標として回路設計を行う．

2.7　結言

本章では，IoT デバイス向けに実装するためのセキュリティ対策を施した AES 暗号回路の設計方針を検討する際に必要となる AES，セキュリティ対策及び STP について述べた．また，設計する際の課題と評価指標について述べ，設計方針を示している．

本研究では，電磁波解析攻撃耐性を有する非同期 AES 暗号回路の検討として水平隠蔽によるセキュリティ対策を採用しているが垂直隠蔽のみの場合や両者の隠蔽を施した場合等のセ

キュリティの強度面，回路面積，実行時間等を評価及び比較する必要があり，IoT デバイスに実装する最適な実装手法を検討する必要がある．

第 3 章

サイドチャネル攻撃

3.1　緒言

本章では，IoT デバイスに施される AES 暗号回路における秘密鍵を推測する方法の一つであるサイドチャネル攻撃について示す．本研究の実験で使用した攻撃手法である相関電磁波解析攻撃についても述べる．

3.2　サイドチャネル攻撃とは

サイドチャネル攻撃とは暗号アルゴリズムそのものではなく，暗号処理時に副次的に漏れる物理情報（電力，時間，電磁波，音，故障挙動など）を解析して秘密鍵を推定する攻撃のことであり，主な攻撃対象として暗号機能を内蔵した IC カードなどの電子機器や半導体製品が挙げられる．また，それに対する攻撃方法が複数存在する．主要な攻撃方法を図 3.1 に提示する．

3.2　サイドチャネル攻撃とは

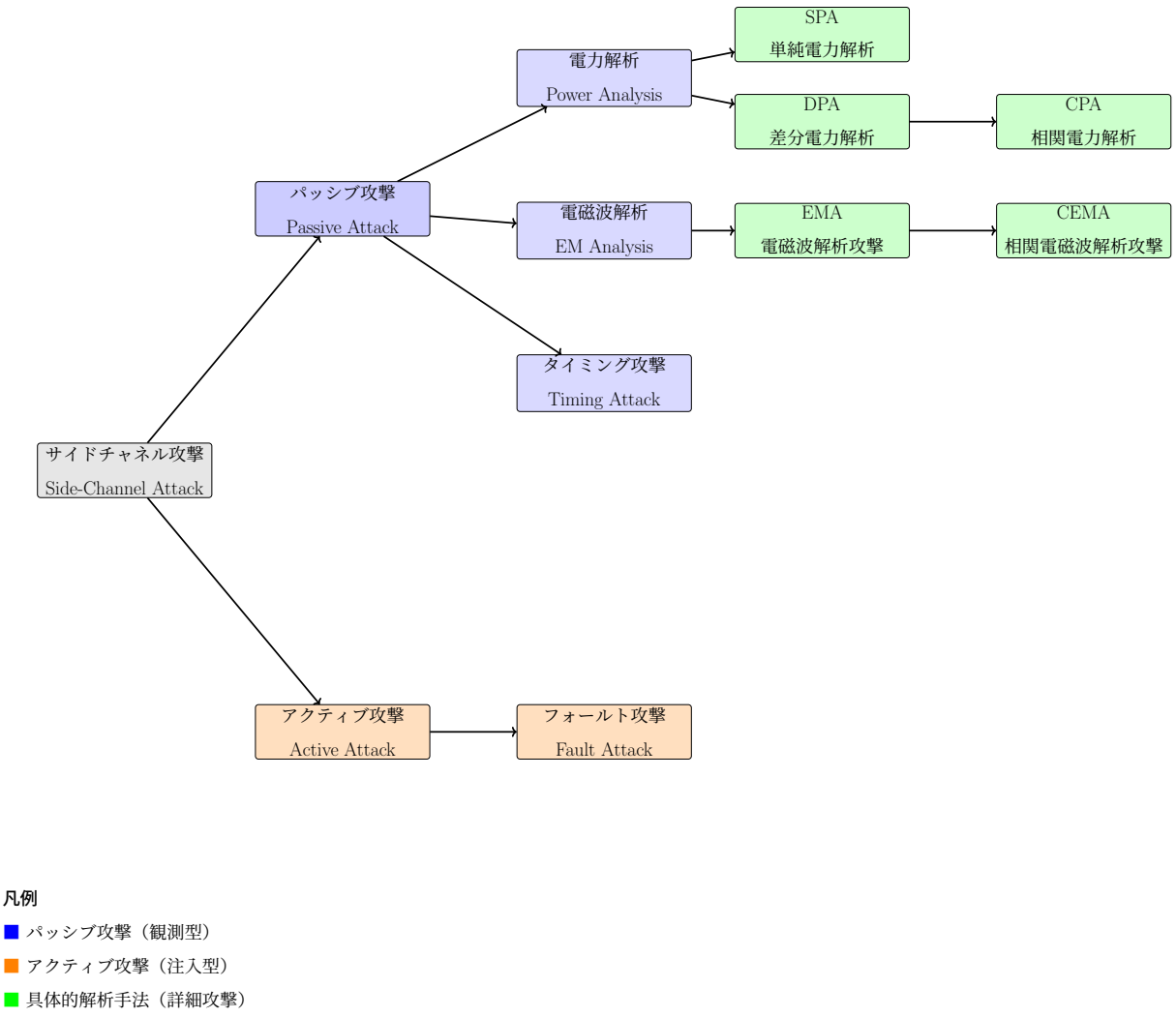

図 3.1　サイドチャネル攻撃の分類）

また，それぞれの攻撃手法について説明する [5].

- 電力解析攻撃

  暗号回路の動作時における消費電力の変動を測定・解析することで秘密鍵を推定する攻撃である．単一の電力波形から処理内容を推測する単純電力解析（Simple Power Analysis: SPA）と，多数の電力波形を統計的に解析する差分電力解析（Differential Power Analysis: DPA）が存在する．DPA の代表的手法として，相関電力解析（Correlation Power Analysis: CPA）が知られている．CPA は，鍵の仮説に基づいて算出した暗号処理中の中間値のハミング重みやハミング距離を電力モデルとし，測定した電力波形と

の相関係数を計算することで秘密鍵を推定する手法である．このような相関解析はノイズ耐性が高く，実用的な攻撃手法として広く用いられている．

- 電磁波解析攻撃

  暗号処理中に回路から放射される電磁波を測定・解析する攻撃である．電磁波解析は非接触で測定可能であり，さらに回路の局所的な情報を取得できることから，電力解析攻撃よりも高い分解能を有する場合がある．電力解析と同様に，単一の電磁波波形を用いる単純電磁波解析（Simple Electromagnetic Analysis: SEMA）と，多数の波形を統計的に解析する差分電磁波解析（Differential Electromagnetic Analysis: DEMA）が存在する．DEMA の代表的手法として，相関電磁波解析（Correlation Electromagnetic Analysis: CEMA）があり，電力解析における CPA と同様に，相関係数を用いて秘密鍵を推定する．FPGA や LSI を対象とした攻撃として有効であり，近年多くの研究が報告されている．

- タイミング攻撃

  暗号処理に要する時間の差異を測定することにより秘密鍵を推定する攻撃である．条件分岐やメモリアクセスの違いに起因する処理時間のばらつきが情報漏洩の原因となる．特にソフトウェア実装において問題となりやすく，定数時間で処理を行う実装が対策として有効である．

- フォールト攻撃

  暗号処理中に意図的に誤動作を引き起こし，正常な出力と誤った出力との差分を解析することで秘密鍵を推定する攻撃である．フォールト注入の手法としては，クロックや電圧のグリッチ注入，レーザ照射，電磁パルス注入などが知られている．ハードウェア実装に対して強力な攻撃手法である一方，エラー検出や冗長計算による対策が可能である．

3.3　本研究で用いるサイドチャネル攻撃

本研究では特に電磁波解析攻撃（EMA）に焦点を当てる．理由は主に以下の三点である．

- 非接触で測定可能であること

  電磁波解析攻撃は，回路の近傍から放射される電磁波を非接触で取得できるため，物理的な改造や接触を必要とせず，IoT デバイスや FPGA 実装回路のようにアクセスが制限される環境においても成立しやすい．
- 局所的な情報取得が可能であること

  EM プローブを用いることで，回路の特定の部位やラウンド単位で放射される信号を観測できる．これにより，鍵に依存した微細な情報が電磁波波形として抽出可能であり，統計的解析（差分・相関解析）により秘密鍵の推定が実施されやすい．
- 従来手法との比較で有効性が明確に評価できること

  電力解析攻撃やタイミング攻撃は，ソフトウェア実装や同期回路において特に有効である一方，FPGA 上の非同期回路に対しては自然にタイミングばらつきが生じるため，耐性評価の効果が見えにくい場合がある．一方で，電磁波解析攻撃は非同期回路でも局所信号の観測に基づき鍵推定が可能であるため，提案回路の耐性向上を明確に示す指標として適している．

以上の理由から本研究では電磁波解析攻撃を対象とし評価を行い，タイミング攻撃，フォールト攻撃，および電力解析攻撃については評価対象外とする．以下にその理由を述べる．まず，タイミング攻撃は暗号処理に要する時間の差異を利用する攻撃であり，主にソフトウェア実装において問題となることが多い．本研究で対象とする AES 暗号回路は FPGA 上に実装されたハードウェア回路であり，処理フローが固定されているため，ソフトウェア実装と比較してタイミング情報のばらつきは限定的である．また，本研究の主眼は処理タイミングを時間的に隠蔽する非同期回路構成による電磁波解析耐性の評価であることから，タイミング攻撃は本研究の評価対象外とした．次に，フォールト攻撃は暗号処理中に意図的な誤動作を注入することにより秘密鍵を推定する攻撃であり，クロックや電圧のグリッチ注

入，レーザ照射などの専用装置を必要とする．本研究では，非同期回路を用いた暗号回路構成が電磁波解析攻撃に与える影響を明らかにすることを目的としており，フォールト耐性を考慮した回路設計や評価は研究対象を大きく拡張するため，本研究では扱わず，今後の課題として位置付ける．また，電力解析攻撃は暗号回路の消費電力変動を解析する攻撃であり，電磁波解析攻撃と類似した解析手法が用いられる．しかしながら，FPGA 実装においては電源ネットワークが広範囲に共有されており，消費電力波形には複数の回路動作が重畳されることから本研究に対する攻撃として適さないと考え対象外とした．また，本研究にて行う攻撃手法として，電磁波解析攻撃の中でも，本研究では相関電磁波解析（Correlation Electromagnetic Analysis: CEMA）を用いて耐性評価を行った．CEMA は，鍵の仮説に基づいて算出した中間値モデルと測定した電磁波波形との相関係数を用いる手法であり，ノイズ耐性が高く，安定した解析が可能である．FPGA 実装回路から取得される電磁波信号は，周囲環境や回路配置の影響を受けやすいが，CEMA は統計的解析によりこのような条件下でも攻撃成立の可否を評価できる．また，AES 暗号回路に対する攻撃手法として広く用いられていることから，先行研究との比較が容易である点も利点である．以上の理由から，本研究では相関電磁波解析攻撃を実施し，AES 暗号回路の FPGA 実装における電磁波解析攻撃耐性を評価した．

3.4　相関電磁波解析による攻撃手法

相関電磁波解析攻撃（Correlation Electromagnetic Analysis: CEMA）は，暗号処理中に回路から放射される電磁波を測定し，鍵の仮説に基づいて算出した理論モデルとの相関を解析することで秘密鍵を推定する攻撃手法である．CEMA は，以下の手順により実施される．

- 平文の選択と暗号処理の実行

  攻撃者は，暗号回路に対して既知の平文を複数回入力し，暗号処理を実行させる．AES 暗号の場合，通常は攻撃効率の高い 初段（1st round） または 最終段 の中間値が解析

対象として選択される．

- 電磁波波形の測定

  暗号処理の実行中に，EM プローブを用いて回路近傍から放射される電磁波を測定する．各暗号処理に対して 1 本の電磁波波形を取得し，これを多数回繰り返すことで，平文と電磁波波形の対応関係を持つデータ集合を得る．

- 解析対象中間値の選択

  AES の内部演算における中間値のうち，秘密鍵に依存する値を解析対象として選択する．代表的な例としては，SubBytes 演算の入力または出力が挙げられる．

- 鍵仮説の設定

  解析対象となる鍵バイトについて，取り得るすべての鍵候補（例：8 ビット鍵であれば 0〜255）を仮定する．各鍵候補に対して，中間値を計算する．

- 電磁波モデルの計算

  各鍵仮説に基づいて算出した中間値に対し，ハミング重みモデルやハミング距離モデルを用いて理論的な漏洩モデルを計算する．このモデルは，暗号処理時の電磁波強度が論理値の遷移やビット数に依存するという仮定に基づいている．

- 相関係数の算出

  測定された電磁波波形と，鍵仮説ごとに算出した理論モデルとの間で，相関係数を計算する．一般に，ピアソンの積率相関係数が用いられる．この計算を，時間サンプルごとに実施することで，相関値の時間変化を得る．

- 鍵候補の推定

  各鍵候補に対して得られた相関係数の最大値を比較し，最も高い相関値を示す鍵候補を正しい鍵として推定する．正しい鍵が存在する場合，特定の時間位置において他の鍵候補よりも顕著に高い相関値が観測される．

また，攻撃の流れを図 3.2〜図 3.4 に示す．

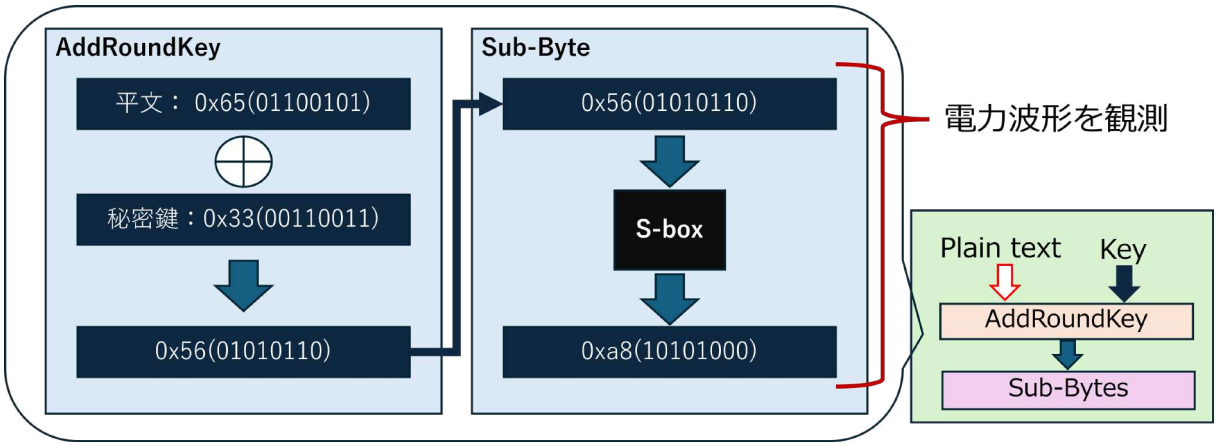

図 3.2　攻撃の流れ (漏洩電磁波計測)

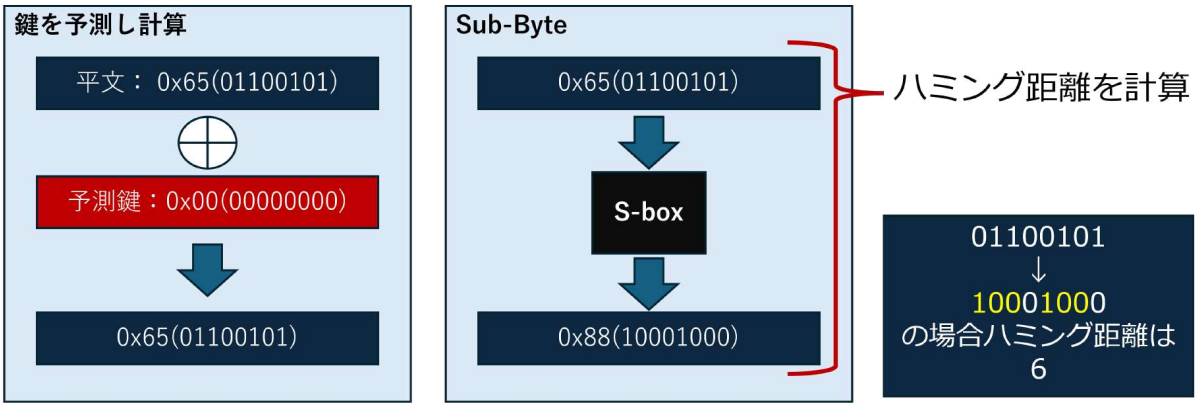

図 3.3　攻撃の流れ (ハミング距離計算)

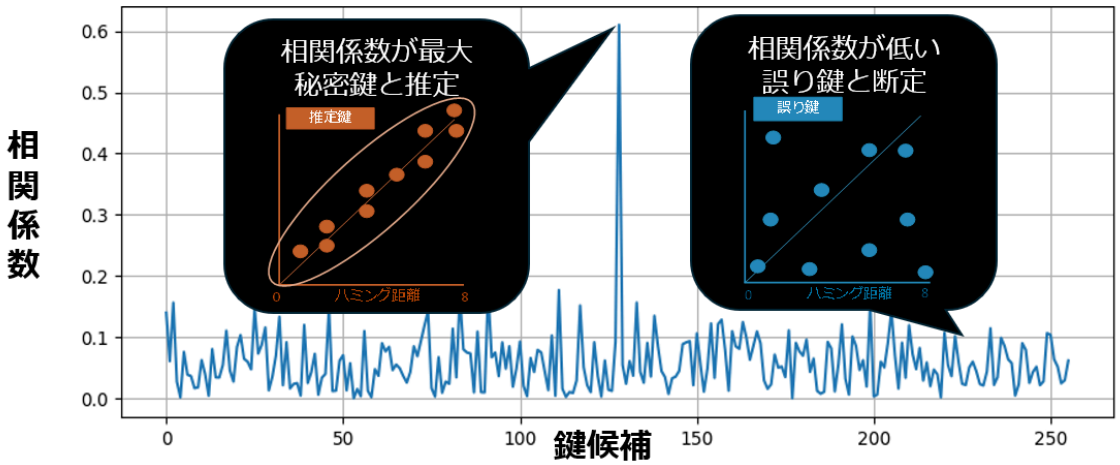

図 3.4　攻撃の流れ (漏洩電磁波とハミング距離相関)

本研究では，この攻撃手法を用いて漏洩電磁波から鍵の推定を行い，提案非同期 AES 暗号回路における電磁波解析攻撃耐性を検証する．

3.5　結言

本章では，IoT デバイスに搭載されている AES 暗号回路の攻撃手法の 1 つであるサイドチャネル攻撃について述べた．また，本研究で実施した攻撃手法として電磁波解析攻撃の 1 種である相関電磁波解析攻撃について，この手法を選択した理由および攻撃手順を説明した．

第 4 章

提案回路

4.1　緒言

本章では，第 2 章で述べた方針をもとに先行研究にて設計された非同期 AES 暗号回路の回路構成について示す．非同期 AES 暗号回路は 3 つのパイプラインから構成されており，各モジュールの回路構成についても述べる．また，先行研究で提案した回路に基づき実装可能であり，オシロスコープによって計測可能となる回路を設計した [4]

4.2　提案回路

本回路での暗号化回路の全体図を図 4.2 に示す.

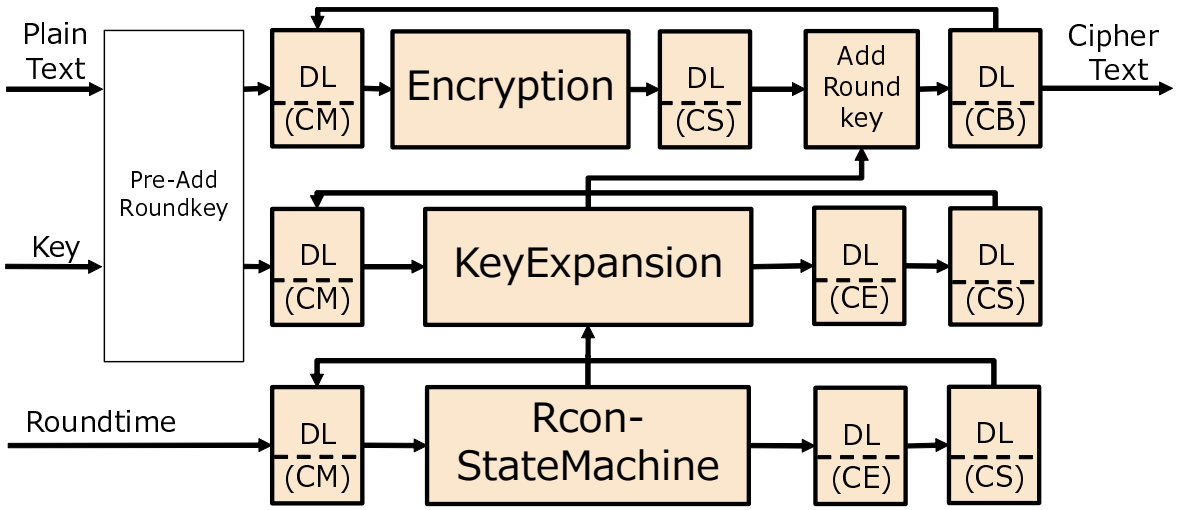

図 4.1　提案非同期 AES 暗号回路構成

また，暗号化処理を行う Encryption モジュールの構成を図 4.2 に示す.

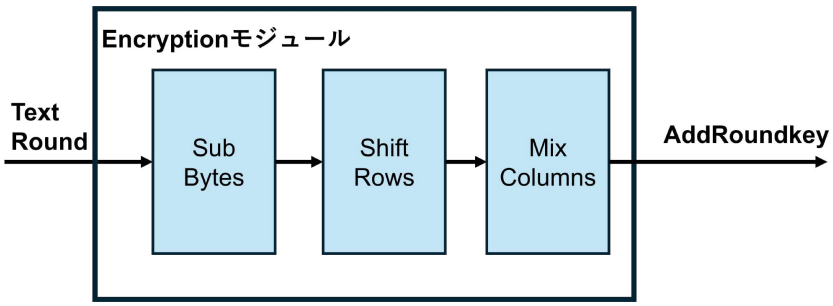

図 4.2　Encryption モジュールの構成

- Encryption モジュール

  本モジュールでは AES 暗号化の処理である SubBytes，ShiftRows，MixColumns3 つの処理を行っている．また，ラウンド数を同時に受け取ることで最終ラウンドの時の MixColumns の処理を行わないようにしている．また，Encryption モジュールから AddRoundkey のみを AES 暗号処理から切り離すことで，下のパイプラインで生成される RoundKey による動作によって遅延させることなく処理が進む．これにより,Encryption パイプラインステージが早くラウンドが循環してしまうのに対し，AddRoundkey において RconStateMachine および KeyExpansion の処理を待つ必要を削減することが可能となり，暗号処理の実行を行う際の，不必要な遅延を失くしている．

本回路では，図 4.2 より，Encryption モジュールにおいて AES の暗号化，KeyExpansion モジュールにてラウンド鍵の生成，RconStateMachine においてラウンド数の管理を行っている．暗号化の流れとして，左の DL に付随する CM 素子が外部との転送制御を行い転送可能である場合には平文と鍵およびラウンド数が入力される．その後，最初の AddRoundKey を実行する．STP 部分の処理は RconStateMachine によるラウンド数の加算が行われた後に，KeyExpansion へラウンド数を渡しラウンド鍵の生成が行われる．その後，生成されたラウンド鍵を AddRoundkey へ渡し，AddRoundkey まで実行されることで 1 ラウンドの暗号化が行われる．本研究は 128bit のみの暗号化回路となっているため，10 ラウンド目

の動作において Encryption モジュールにおいて MixColumns の処理を行わないようにし，CE 素子が付随している DL においてラウンド鍵とラウンド数のデータを消去している．また，ラウンド数を利用して CB 素子からラウンド数が 10 となった場合には暗号化終了として暗号文の出力を行っている．本回路ではパイプライン同士のデータのやりとりが行われることから周回数を同じにする必要があるため CS 素子を用いて簡易的な同期をとる．ラウンド数からラウンド鍵を生成し，AddRoundKey を実行するため Encryption のパイプラインは下のパイプラインの処理が終了することで実行可能な動作が存在するため，実行時間が最も長くなる．そのためデータ転送が最も遅い Encryption パイプラインの 3 つ目の DL にデータが転送されたことをトリガーとすることですべてのラウンドごとの暗号化処理が終了したと判断することが出来るため，3 つ目の CB 素子から出力される Send 信号を CS 素子に入力することで，パイプラインの転送制御を開始させている．また， Encryption パイプラインステージの DL のみ設計段階で場所が他パイプラインステージと異なる理由として，DL に付随するデータ転送制御回路は C 素子であったが暗号化処理を一時停止させ，ラウンド鍵のデータが転送される必要があるため KeyExpansion パイプラインステージの 2 つ目の DL にラウンド鍵のデータが入力された時点でラウンド鍵の生成が終わっていることを意味する．そのため Send 信号を同期信号として Encryption パイプラインステージの CS 素子に入力することで暗号化処理を再開させるように設計した．

4.3 結言

本章では，第 2 章で取り上げた問題点および AES 暗号回路のセキュリティとして STP を利用し水平隠蔽を施した非同期 AES 暗号回路を設計した．提案回路において暗号化処理の途中で一時停止させることにより不必要な遅延を失くし配置配線を変更による影響を受けない安定した動作を行うことが出来る非同期 AES 暗号回路の設計を行った．

第 5 章

提案回路の実装評価および攻撃実験

5.1 緒言

本章では，本研究で設計した非同期 AES 暗号回路を配置配線後の実遅延シミュレーションから正しく動作することを確認し，回路規模および実行時間を評価指標とする．また，比較対象として，セキュリティ対策を施していない提案回路と同様の動作を行う AES 暗号回路を同時に評価している．その後，FPGA に実装し電磁波解析攻撃を AES 暗号回路に対して行い，それぞれの電磁波解析攻撃耐性の有無について確認する．

5.2 前提条件

本研究での実装評価指標として，回路規模，実行時間および電磁波解析攻撃耐性の確認としている．また，解析実験では，攻撃者が任意のタイミングで好きな平文を送信することが可能であり，FPGA が AES を実行しているタイミングにおいて漏洩電磁波を傍受することが可能であることを前提とする．

5.3 基本 AES 暗号回路

セキュリティ対策を施していない提案回路とほぼ同じ動作を行う AES 暗号回路として同期 AES 暗号回路の回路構成を図 5.1 に示す．本研究における二つの提案回路は水平隠蔽の導入を行っている AES 暗号回路である．そのため，導入したセキュリティ対策の具体的な回路規模および実行時間の増加量が分からず評価が難しい．そのため，比較対象とし提案回

路と同様の動作を行うセキュリティ対策がない AES 暗号回路もまとめて評価を行っている．提案回路との相違点として，最初の AddRoundkey を含めすべてのラウンドを環状パイプラインを周回させるように設計している．また，ラウンド鍵の作成およびラウンド数の管理までを 1 つのパイプラインステージで処理を行い，1 クロックにつき 1 ラウンドの処理を行っている．まず外部から平文と鍵およびラウンド数として 0 が入力され，暗号化処理を実行する前に転送するデータを DATA として全て結合を行い，AES 暗号回路内においてラウンド数の加算，ラウンド鍵の生成，暗号化処理を実行している．AES 暗号回路から DL への返還である Pre-DATA は今回処理を行った DATA を次ラウンドのための事前データとしている．また，最初の暗号化処理のためラウンドが 0 の場合には AddRoundkey 以外を実行，ラウンドが 10 の場合には MixColumns 以外の処理を実行させるようにしている．出力の管理は最上位モジュールにおいてラウンド数が 10 の時に出力を行うように設計した．

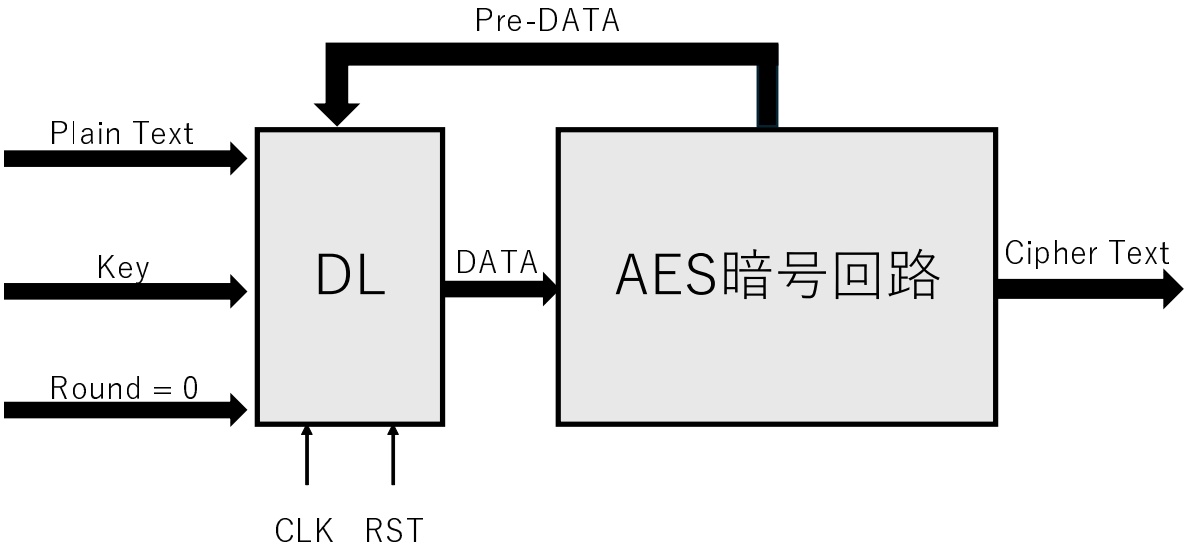

図 5.1　基本 AES 暗号回路構成

5.4　回路規模の評価

今回の回路評価に用いた評価方法を以下に記述する．

5.4.1　評価対象 AES 回路の仕様

- 入力：平文 (128bit)
- 出力：暗号文 (128bit)
- 秘密鍵 (128bit)

5.4.2　FPGA 回路実装環境

- FPGA チップ：AMD 社 Zynq-7010
- EDA ツール：AMD 社 Vivado 2023.1

5.4.3　評価指標

- 暗号化に要する時間

  平文と鍵が入力された時刻から暗号文が出力されるまでの時刻
- FPGA 回路の規模

  LUT および FF の使用数，使用率

上記の評価基準を用いて 3 つの暗号回路の評価を行った結果を以下に記載する．

表 5.1　AES 回路の回路規模・使用率

回路	LUT	FF	実行時間 (ms)
基本 AES 暗号回路	2680(15.23%)	390(1.11%)	0.42
提案回路 2	4727(26.86%)	1191(3.38%)	1.50

この結果から STP を用いて水平隠蔽を導入した本回路においては LUT の使用数が約 2000，FF の使用数が約 800 個の増加が見られた．また，実行時間が約 1ms 増加することで処理性能が約 3 分の 1 程に低下した．増加した要因としてパイプラインステージを 1 つから 3 つに分離させたことに加え DL の増加と C 素子の使用が考えられる．

5.5　電磁波解析攻撃耐性の評価

5.5.1　実験環境

本研究で行った相関電磁波解析攻撃における実験の実行環境を以下に記述する．

- オシロスコープ (Agilent 社 DSO9104A)
- EM プローブ (テクシオテクノロジー社 GKT-008)

実装する FPGA については上記に記述した FPGA 回路実装環境と同様の環境で攻撃を行った．以下に計測環境の提示する．

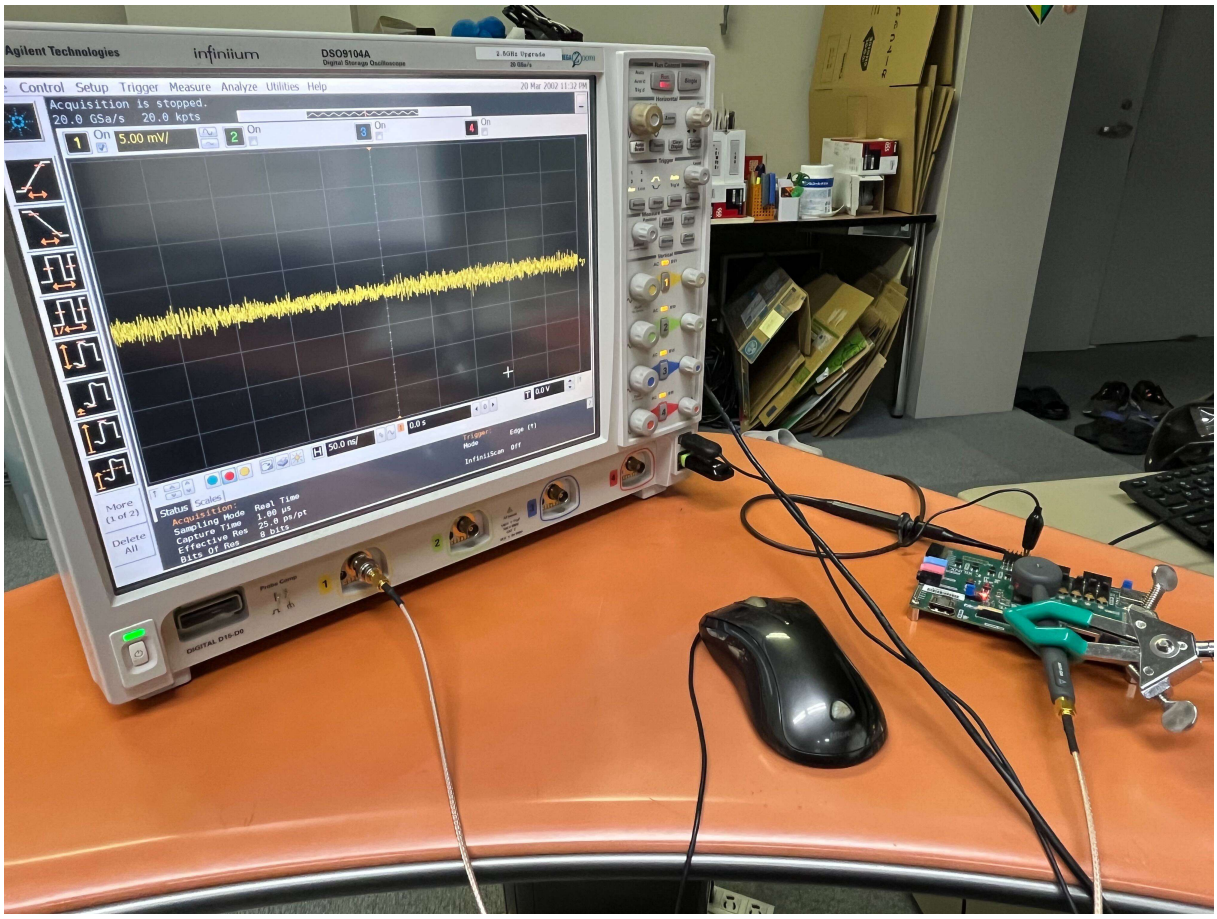

図 5.2　実験環境

5.6　予備実験

本実験では，オシロスコープに FPGA から AES 暗号回路が動作を開始させる際に，トリガ信号を送信することで必要なタイミングの漏洩電磁波を計測する．オシロスコープはトリガ信号を外部配線を FPGA からオシロスコープに流すことによって立ち上がりを検出し，波形データを取得することにしているため，外部配線の遅延があるためシミュレーション上で確認する時間とオシロスコープで計測した時間に誤差が生じる．そのため，適切なタイミングを計測することを可能にするために，予備実験としてトリガ信号遅延の計測を行った．実験方法は，FPGA のボタンを押下した際にトリガ信号を立ち上げた後，発振する回路を任意のタイミングおよび時間によって動作させる．実際に計測する前に，配置配線を行った後の実遅延シミュレーションを行い，シミュレーションでの遅延を記録する．その後，実際にオシロスコープで計測し，発振を観測出来た地点とシミュレーションでの遅延の差からトリガ信号を送信するための外部信号遅延を推定した．以下に実験方法を図 5.3 に示す．

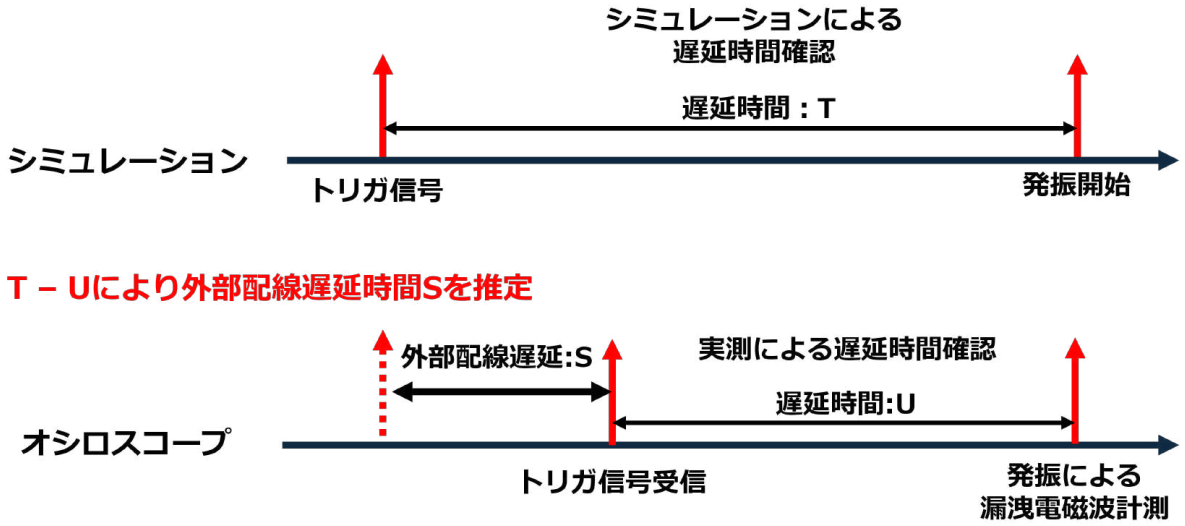

図 5.3　予備実験によるトリガ遅延取得

オシロスコープの計測結果から発振回路の発振開始時刻を確認する方法として，クロックと発振を同期させることで通常時よりも強い漏洩電磁波を計測可能である．そのため，本実験の実行環境である 50MHz の周波数においてピーク値を確認可能な計測時間を調査するこ

とで，確認を行う．計測結果例を以下に提示する．

5.6.1　予備実験結果

予備実験として行った結果を図 5.4 に記載する．

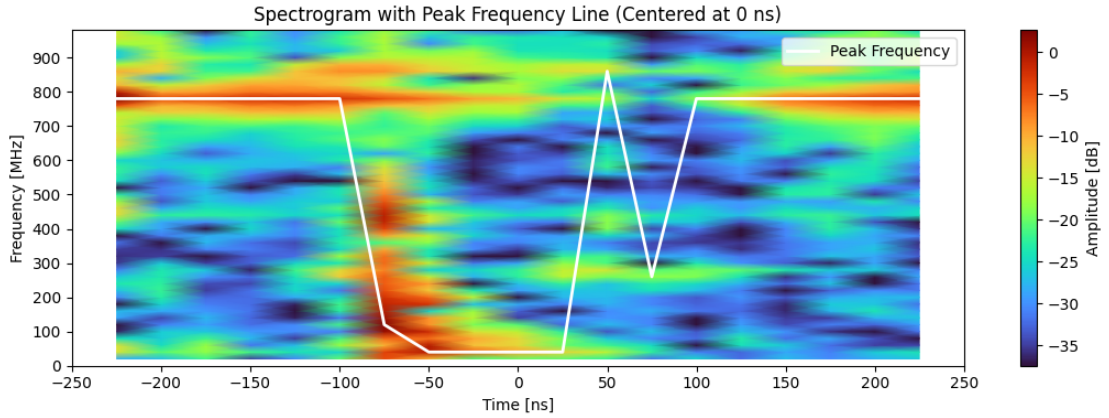

図 5.4　発振回路によるピーク値確認

この結果から約 - 50ns ～ 40ns 程度から開始していると推測することが可能である．また，シミュレーション上での遅延時間トリガ信号を 0ns した際の結果を表 5.3 に記述する．

表 5.2　トリガ信号遅延の推測結果

回路	trigger	動作開始時間 (ns)
シミュレーション	0	34 ～ 35
実測	0	-50 ～ -40

窓幅およびオーバーラップ時間を変更し，より明確な遅延時間を計算した結果を予備実験としてのトリガ信号遅延時間を約 80ns ～ 約 75ns と推定した．

5.7　本実験

5.7.1　鍵解析試行実験

予備実験を基に，提案非同期 AES 暗号回路および同期 AES 暗号回路に対し，3 章で説明した電磁波解析攻撃を実行する．以下に実行条件を記載する．

- 平文：128bit(256 回以上)
- 秘密鍵：128bit
- 測定回路：同期型 AES 暗号回路，提案非同期 AES 暗号回路
- 鍵解析：自作 Python コード

また，送信する平文は攻撃者が FPGA に搭載されているボタンを押下することで 1 回ずつ送信し，それぞれの回路が動作した際にトリガ信号を立ち上げることで漏洩電磁波を計測する．本研究では，1Byte ごとに秘密鍵を推定する最も容易である手法を用いる．平文は求めたい Byte の部分を 0x00 ～ 0xFF に変更し，残りは全て 0xFF となる平文を送信する．また，オシロスコープで計測する箇所を 1 ラウンド目の SubByte とし，対応する平文と計測した漏洩電磁波から相関を求め，取りうる全ての場合となる 0 ～ 255 までを確認し，SubByte が実行されているとされる時間において推測された推定鍵が正解鍵と一致するか確認した．例として解析対象となる秘密鍵の 1Byte 目を 0x00 とし，実験を行った結果となる相関係数のグラフである図 5.5 を示す.

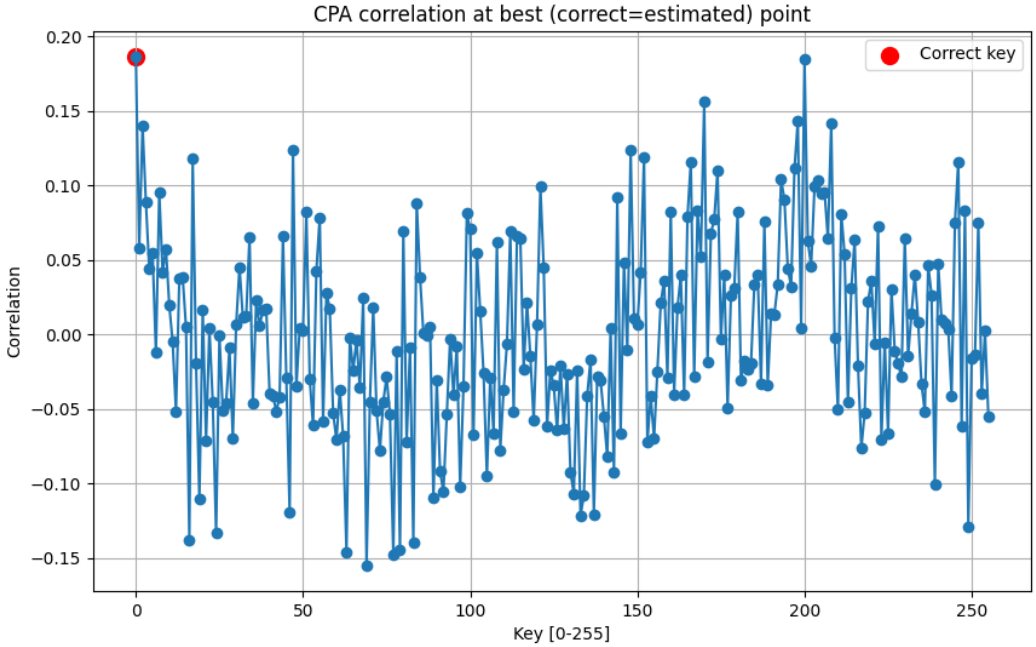

図 5.5　正解鍵 0x00 とした際の CEMA により求めた相関係数

実行環境が回路以外の FPGA からの漏洩電磁波や周囲の電波等のノイズの影響により明確な差が出ていないが，推定鍵として特定することが出来る可能性を確認した．この結果を基に，複数パターンの鍵をそれぞれの回路に導入し，同様の方法により相関電磁波解析攻撃を実行した．以下に試行した提案回路および同期回路における解析結果を表 5.3 に記載する．

表 5.3　鍵解析の試行結果

回路	秘密鍵	観測窓	推定鍵 (相関係数)	相関係数
提案非同期回路	0x00	—	0x10(0.160)	0.077
	0x36	—	0xF6(0.217)	0.114
	0x56	—	0xE8(0.187)	0.130
	0x98	—	0x11(0.157)	0.134
	0xAA	—	0x0B(0.284)	0.174
	0xDC	—	0xAE(0.187)	0.124
	0xFF	—	0x11(0.217)	0.099
同期回路	0x00	-12.9 ～ -6.9	成功	0.186
	0x36	—	0x3D(0.125)	0.104
	0x56	—	0x6b(0.161)	0.132
	0x98	—	0xEF(0.210)	0.186
	0xAA	-19.2 ～ -13.2	成功	0.162
	0xDC	—	0xB3(0.162)	0.157
	0xFF	—	0x7F(0.122)	0.093

結果から，同期回路は成功，失敗したとしても推定鍵との相関係数に大差は見られなかったが，提案非同期 AES 暗号回路はすべての鍵解析において失敗し，推定鍵との相関係数の差が同期 AES 暗号回路と比較して大きいことが分かる．この結果から提案非同期 AES 暗号回路には電磁波解析攻撃に対する耐性を高めることが出来る可能性があると考えられる．しかし，鍵解析の試行回数が限定的であり，提案回路に電磁波解析攻撃耐性があると結論づけることが難しいため，現在より多くの試行実験を行い，電磁波解析攻撃耐性の強度を確認する必要がある．また，同期 AES 暗号回路において相関電磁波解析による鍵解析は成功したが，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り，確実に推定できたという確証は持てない値である．理由として，FPGA 周辺のノイズや計測時間のばらつきの影響が大きいのではないかと考えられる．そのため，今後の実験において試行回数の増加や周

囲からのノイズを遮断するよう工夫し，より正確な値を取得可能な実験環境により計測する必要がある．

5.7.2　追加実験

試行回数が限定的であったため，秘密鍵が 0x00, 0xAA の 2 種に限定し，漏洩電磁波の計測回数を増加させ検証を行った．条件は本実験と同様にし計測回数のみを平文一つあたり 10 回に増加させ，平文 256 個による鍵解析を 10 回行い，それぞれの鍵解析の成功確率および秘密鍵の平均相関係数を求めた．以下に試行した提案回路および同期回路における解析結果を表 5.4 に記載する．

表 5.4　追加実験の試行結果

回路	秘密鍵	成功確率	平均相関係数 (秘密鍵)
提案非同期回路	0x00	0％(0/10)	0.13
	0xAA	0％(0/10)	0.14
同期回路	0x00	30％(3/10)	0.15
	0xAA	30％(3/10)	0.13

この結果から同期 AES 回路はそれぞれ 30%の確率で鍵解析に成功したが，提案非同期 AES 回路については一度も成功しなかった．また，平均相関係数は提案回路と同期回路において大差がないことから，提案非同期 AES 回路については，S-box を実行している際に他の回路が動作することで隠蔽され，他の値がピーク値として推定されたからと考えられる．このことから追加実験で行った複数回の試行実験においても提案非同期 AES 暗号回路に水平隠蔽が施されたと考えられる．

5.8　結言

本章では，提案非同期 AES 暗号回路の評価を行うためとして，同期 AES 暗号回路と提案回路を評価し比較した．回路規模の観点では LUT が約 1.76 倍，FF が約 3.05 倍，実行時

間が約 3 倍であった．また電磁波解析攻撃の実験では，同期 AES 暗号回路の鍵解析は成功し，提案非同期 AES 暗号回路は鍵解析の取得に失敗した．このことから，提案非同期 AES 暗号回路には電磁波解析攻撃耐性を高める効果がある可能性があると考えられる．しかし，限定的な試行回数やノイズの影響等で確証を持てる結果であるとは言い切ることが出来ないため，今後はより多くの試行実験を行うことで電磁波解析攻撃耐性の強度を確認する必要がある．また，IoT に活用する条件として，一般的なセキュリティ強度との比較が求められるため，信頼性モデルを設計し定量的な評価を行う必要がある．

第 6 章

結論

近年，IoT デバイスの普及に伴い，様々な分野で活用することが出来るとして FPGA への実装が進んでいる．また，IoT デバイスの暗号化処理として AES が実装されているが電力解析攻撃への脆弱性が存在する．そのため，ハードウェア AES 暗号回路へのセキュリティ対策が求められており，STP を用いて水平隠蔽を施した非同期 AES 暗号回路を設計し，相関電磁波解析攻撃から鍵解析実験を行った．提案非同期 AES 暗号回路は同期 AES 暗号回路と比較し，回路規模では LUT が約 1.76 倍，FF が約 3.05 倍，実行時間が約 3 倍となった．また，相関電磁波解析攻撃による鍵解析の実験では，同期 AES 暗号回路は特定の時間における鍵解析が可能であったが，提案非同期 AES 暗号回路は特定の時間帯において相関係数の最大値が正解鍵と推定鍵が等しくなることがなかった．このことから，先行研究？において提案した非同期 AES 暗号回路による電磁波解析攻撃耐性は同期 AES 暗号回路と比較し，セキュリティ強度を高める効果が期待できると考えられる．考えられる理由として，提案回路による SubByte の実行時間に他のパイプライン処理が実行されるため，オシロスコープによる漏洩電磁波の計測値が相関値を取りやすい値ではなくなった可能性が考えられる．また，本研究を一般的な IoT デバイスに応用可能とするために必要となる課題を以下に記述する．

6.1 提案非同期 AES 暗号回路の改良

- 192，256bit への応用

  本研究の回路構成は 128bit の平文および共通鍵のみによる設計である．しかし，現在の

IoT デバイスに実装されている AES 暗号回路は暗号性能が高い AES-192，AES-256 の使用が増加している．そのため，現在の 128bit のみから 192，256bit までの暗号化が可能である回路設計を行う必要があると考えている．

- 垂直隠蔽の導入

  本回路構成は STP を用いた非同期 AES 暗号回路にすることにより水平隠蔽を施したが，垂直隠蔽を実装することが出来ていない．そのため，一つのセキュリティ対策ではどの程度の安全性があるのか比較することが不可能である．よって垂直隠蔽を施した AES 暗号回路，水平隠蔽を施した AES 暗号回路，両方の隠蔽を施した AES 暗号回路を設計および評価することにより隠蔽方法による安全性および回路規模等の比較・評価を行うことが可能になると考える．この評価結果を元に今後のハードウェア AES 暗号回路に組み込む最適なセキュリティ対策を推測することが可能となると推測している．また，セキュリティ強度，回路規模および実行時間はトレードオフの関係であるためそれぞれの IoT デバイスにおけるセキュリティ対策を考えた回路構成を柔軟に変更することが可能になると考えられる．垂直隠蔽の課題である配置配線が行われるごとにルーティングが変わるためデュアルロジックが安定しないことや動作する bit が 2 重になることから早期伝播効果の影響が大きくなることが課題である．この課題に対し，現段階での解決策として配置配線を固定することでその回路に合わせたデュアルロジックを構成することが可能であると考えていることに加え，早期伝播効果については水平隠蔽を施しているため垂直隠蔽単体の処理に比べ影響が減少されると考えている．

- 回路規模縮小・実行時間短縮

  本研究の回路構成においてより良い回路構成であると考えられる提案回路 2 の Zynq-7010 における LUT 使用率は約 27%であり，実行時間は 128bit あたり約 1.5ms と処理性能が約 85kbps 程度であった．このことから，FPGA チップを変更し，使用できる LUT 等の個数が減少した場合 IoT デバイスによっては本回路構成の実装が不可能となることも考えられる．また，上記の課題によって様々な追加仕様が存在するため現段階での 27%の使用率は大きすぎると推測できる．実行時間においては，処理性能約

85kbps は現在カード等に実装することが可能な処理性能であると考えている．この処理性能ではサイズが大きい IoT デバイスでの処理性能には届かないと考えているためより実行時間が短くなる回路構成の検討が必要である．現在の改善案として，本回路においては 128bit のラウンド数が 10 まで循環させ，MixColumns モジュールでは処理を行わないことによって暗号化処理を完了させている．そのため，最後の処理を行うまで次の平文と鍵の入力を受け付けることが出来ない．よって，図 5.1 に示したように処理動作が異なる最終ラウンドを分けることにより，前ラウンドが終了したタイミングから次の入力を受けることが可能となるため複数回の入力を必要とする場合は処理速度が 1 回の実行時間より早くすることが可能となる．また，図 5.2 に示したように提案回路 1 では DL を処理後に 2 段使用している構成を 1 段の DL のみにすることで処理速度の向上および回路規模の減少が可能であると考えている．しかし，前者の解決方法である最終ラウンドの処理を周回する部分とは別に行う方法では，回路規模が現在の提案回路より増加してしまい別の部分での回路規模縮小が望まれる．また，後者の解決方法である DL の個数を減少させる方法では，波形の動作回数が 9 回から 6 回まで減少してしまうためセキュリティ面での弱体化が考えられる．

上記では様々な課題を記述したが，処理性能と回路規模はトレードオフの関係であるため 2 つの課題を同時に性能を高めることは困難である．また，必要とされる処理性能および許容できる回路規模は IoT デバイスによって様々であるため，それぞれの課題を一つずつ解決する方法をとりデバイスごとに最適な段階を探すことが一般的な IoT デバイスに応用可能な電磁波解析攻撃耐性を高めることが可能であると考えられる．しかし，回路規模を縮小した場合，漏洩電磁波量が減少するため，本研究目的である電磁波解析攻撃耐性が減少する可能性が存在するため，改良した回路においても電磁波解析を行い鍵解析の試行が求められる．

6.2　電磁波解析攻撃実験および回路評価の改良

- 推定鍵のビット数の変更

  現在 S-box1 つとなる 8 ビットごとの鍵解析を実行している．しかし，ハミング距離が 0〜7 までの，8 通りしかないためハミング距離の差による漏洩電磁波量の差が小さく鍵解析が困難になった可能性がある．そのため，鍵解析を 8bit から 128 ビット全てに変更することでハミング距離を 0 から 127 までの 128 通りにすることでより顕著な相関がみられることが予想される．

- ノイズの減少

  本研究の電磁波解析の鍵解析試行実験において，正解鍵が顕著となる相関係数を得ることが出来ていない．理由として漏洩電磁波を計測する環境が FPGA の AES 暗号回路と関係ない箇所からの漏洩電磁波や周囲の電波等を傍受し，計測結果に影響を与えている可能性がある．そのため，本研究において FPGA は 50MHz の実行であるため，バンドパスフィルタ等から解析を行う周波数帯を制限することで，Wi-fi や携帯電話等の電波によるノイズを低減させることが可能になるのではないかと考えている．また，FPGA をシールドによって囲むことで周りの影響をゼロにする方法などが挙げられる．また，今回の EM プローブによる計測距離や角度が 1 種類のみの計測であったため，適切な距離や角度を模索することでより正確なデータを入手することが考えられる．よって，同じ秘密鍵の試行実験での取得方法の違いから得られる結果の比較等を行い適切な入手方法を検討することが必要である．

- 試行回数の増加

  ノイズの影響と同様に限定的な試行回数が相関係数の値を低くした原因であると考えられる．そのため，現在 1Byte あたりの試行回数が 256 回を増加させる必要があると考えられる．現在の方法は，1 つの平文につき 1 つの波形の対応させているため，同様の平文を繰り返し AES 暗号回路に送信することでより高度な鍵推定を行う必要がある．電磁波解析による鍵推定の際に，閾値を設定し相関係数が閾値を超える試行回数を調査

することで，今後の信頼性モデルを作成する際に定量化を行いやすくすることが可能であると考える．また，AES 暗号回路を 192，256bit と拡張した際に，回路規模が増加し実行時間が長くなることが予想されるため，鍵解析が現在より困難になることが考えられる．そのため，それぞれの bit に適切な試行回数を実験結果から推定することで，今後の評価指標を明確化する必要がある．

- 電磁波解析攻撃耐性の定量化

  本研究では，提案非同期 AES 暗号回路および同期回路にたいし，限定的な鍵解析の試行から電磁波解析攻撃耐性の評価を実施した．しかし，電磁波解析攻撃耐性およびセキュリティ強度に対し確証を持つことは出来ない．そのため，定量化指標として非同期 AES 暗号回路における信頼性モデルを作成する必要がある．これにより，現在の一般的に活用されている IoT デバイスに搭載されている暗号回路と比較することを可能にし，より明確な利点を挙げることが出来ると考える．信頼性モデルの作成には，鍵解析の実験から必要試行回数や実験環境から設定し，bit 幅を拡張した AES 暗号回路に対しても定量化を可能とする必要がある．

- 信頼性モデルの作成

  本研究では，Advanced Encryption Standard（AES）暗号回路を対象として，セルフタイム型データ転送制御回路を用いた非同期パイプライン構成により，電磁波解析攻撃に対する耐性向上を実験的に確認した．しかしながら，本研究で得られた結果は主として実測波形に基づく攻撃実験による評価であり，耐性を理論的・定量的に保証する信頼性モデルの構築には至っていない．

  今後は，電磁波解析攻撃に対する回路の安全性を定量的に評価するための信頼性モデルを構築する必要がある．具体的には，まず攻撃者モデルを明確化し，取得可能なトレース数，測定帯域幅，ノイズ環境などの攻撃条件をパラメータとして整理することが重要である．これにより，攻撃成功確率を攻撃条件の関数として定式化することが可能となる．

  次に，回路側の設計パラメータとして，ラウンド処理時間のばらつき，タイミングジッ

タの分布，パイプライン段数，ハンドシェイク遅延特性などを定量化し，これらが漏洩強度に与える影響を明らかにする必要がある．特に，非同期化による時間的ランダム性が信号対雑音比（SNR）や相関係数にどの程度影響を与えるかを解析することが重要である．

さらに，漏洩モデルとして Hamming Weight や Hamming Distance に基づく仮定を用い，Guessing Entropy，Success Rate，必要トレース数などの統計指標を導入することで，攻撃成功確率を定量的に評価する枠組みを構築できると考えられる．最終的には，回路の信頼度を「信頼度 ＝ 1 − 攻撃成功確率」として定義し，設計パラメータと耐性指標との関係を体系的に整理することが望まれる．

また，提案回路はセキュリティ向上を目的としている一方で，回路規模，消費電力，スループットといった実装コストとのトレードオフが存在する．そのため，耐性指標と実装コストを統合的に評価する指標を導入し，セキュリティ効率の観点から最適設計を検討することも今後の重要な課題である．

以上のような信頼性モデルを構築することで，本研究で提案した非同期 AES 回路の電磁波解析攻撃耐性を理論的に裏付けることが可能となり，IoT 機器における物理攻撃耐性設計の体系化へと発展することが期待される．

- 攻撃の種類増加

  本研究では，ブロック暗号に対する効果的な攻撃方法の一つとして，電磁波解析攻撃を実行した．しかし，IoT デバイスは他にも電力解析攻撃等に対する耐性を持ち合わせることも必要である．そのため，実際に電力を計測による鍵解析や，電磁波解析攻撃とは全く異なる攻撃に対しても実行し，信頼性モデルから耐性があるか確認することで，提案非同期 AES 暗号回路における総合的なセキュリティ強度を決定づけることが出来ると考えている．また，他攻撃により鍵解析が可能となる脆弱性が確認されれば対策する必要が生じるため，現在確認されている解析手法により鍵解析を確認することが求められる．

6.3　将来の展望

本研究では，Advanced Encryption Standard（AES）暗号回路を対象として，セルフタイム型データ転送制御回路を用いた非同期パイプライン構成により，電磁波解析攻撃に対する耐性向上を図った．将来の展望として，以下の発展が期待される．

まず，提案手法を AES 以外の暗号アルゴリズムへ拡張することである．例えば，軽量暗号や公開鍵暗号へ適用することで，IoT 機器全般におけるサイドチャネル攻撃耐性設計の一般的な手法を確立できる可能性がある．また，電磁波解析攻撃だけでなく，電力解析攻撃や故障注入攻撃など他の物理攻撃手法に対する耐性評価を実施することで，より包括的なハードウェアセキュリティ設計手法の構築が期待される．

次に，FPGA 実装における設計自動化手法の確立である．非同期回路設計は設計難易度が高いという課題があるため，ソフトウェア等の設計ツールとの連携や設計テンプレート化を進めることで，実用的な設計フローの確立が求められる．これにより，SCA 耐性を考慮した暗号 IP コアの標準化および産業応用が現実的となる．

さらに，IoT 機器やエッジデバイスへの実装実証を通じて，実環境下でのセキュリティ評価を行うことが重要である．実運用環境における攻撃シナリオを想定した評価を実施することで，社会インフラや産業機器など高い信頼性が要求される分野への応用が期待される．

以上より，本研究は暗号アルゴリズムの安全性のみならず，物理実装レベルにおける安全性確保という観点から，実装暗号技術の発展に寄与するものであり，今後の IoT 社会におけるセキュアハードウェア基盤技術として発展する可能性を有している．

謝辞

本研究を行うにあたり，ご指導頂いた岩田誠教授には深く感謝申し上げます．お忙しい中様々な場面で助言を下さり，相談に乗って頂いたため研究を進めることが出来ました．

また，本研究の副査を引き受けてくださり，貴重なご意見および疑問点を指摘して頂きました，吉田真一教授，福本昌弘教授に深く感謝申し上げます．

研究室の先輩である，Tamnuwat Valeeprakhon 氏には研究活動を進めるにあたりアドバイスを下さり，時には相談に乗って頂きました．深く感謝いたします．

研究室の同期である岡村健勝氏，山下拓巳氏には心から感謝いたします．お互いに研究の意見交換や息抜きとしての会話や食事を行ったことが心の支えとなりました．

研究室の後輩である大崎綾斗氏，門屋陽丈氏，苅田 勇人氏，小松 憲生氏，長崎 雅季氏にはご支援いただきました．深く感謝いたします．

最後になりますが，岩田誠教授，同期，後輩の皆様改めてありがとうございました．また，今まで支援してくださった家族，友人にも心から感謝申し上げます．皆様の支えのおかげで本論文を完成させることができました．

参考文献

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

[2] 中井綱人，他. “電力・電磁波解析攻撃におけるオンチップ・キャパシタの影響評価” SCIS2013

[3] 川西紀昭 株式会社ゴフェルテック ACRi FPGA で作る暗号は危険？ https://www.acri.c.titech.ac.jp/wordpress/archives/8171 2024 年 12 月閲覧

[4] 市ノ木一希. “電力解析攻撃耐性を有する非同期 AES 回路の検討”, 高知工科大学 学士学位論文, 2024.

[5] 崎山一男，他.『暗号ハードウェアのセキュリティ』，コロナ社，2014.