修士論文

順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析に関する研究

岡本 拓実
奈良先端科学技術大学院大学
先端科学技術研究科
情報理工学プログラム

主指導教員: 林 優一 教授
情報セキュリティ工学研究室（情報科学領域）

令和 2 年 3 月 13 日提出

本論文は奈良先端科学技術大学院大学先端科学技術研究科に
修士 (工学) 授与の要件として提出した修士論文である。

岡本 拓実

審査委員：

林 優一　教授　（主指導教員，情報科学領域）
岡田 実　教授　（副指導教員，情報科学領域）
藤川 和利 教授　（副指導教員，情報科学領域）
藤本 大介 助教　（副指導教員，情報科学領域）

順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析に関する研究*

岡本 拓実

内容梗概

暗号モジュールに対する故障利用解析は、意図的に外乱を与えることで一時的な故障を注入する故障注入と、それに伴う誤り出力の解析で構成される。クロックグリッチは従来研究で故障注入に頻繁に用いられているが、その多くは組み合わせ回路を対象としたセットアップタイム違反に限定されている。組み合わせ回路のセットアップタイム違反を引き起こすためには、データバス毎の遅延時間の微小な差異に合わせたタイミングでグリッチを挿入する必要がある。そのため、半導体のプロセス微細化技術の発展に伴う遅延時間の短縮により解析に適用可能な故障の注入は困難化する。

これに対し、本論文では遷移途中の不正な入力が取り込まれる順序回路への入力のタイミング違反による故障について検討し、故障により得られる誤り出力から秘密鍵の取得性について議論する。本論文で検討する故障は、値の遷移が行われる遅延時間中の適当なタイミングでグリッチを挿入することで注入可能であり、高度なタイミング制御が不要であるため、従来、故障利用解析の対象とならなかった暗号モジュールにも脅威が及ぶ可能性がある。実験では、広く利用されている共通鍵暗号である Advanced Encryption Standard（AES）を実装した暗号モジュールに対して提案手法を適用し、秘密鍵が取得可能であることを実証する。また、故障検知回路の追加による対策手法についても検討する。

キーワード

サイドチャネル攻撃，故障利用解析, 順序回路, タイミング違反

*奈良先端科学技術大学院大学 先端科学技術研究科 修士論文, 令和 2 年 3 月 13 日.

Fault Analysis Based on Timing Violation Fault in Sequential Circuit*

Takumi Okamoto

Abstract

The fault analysis for the cryptographic module consists of an injecting a transient fault based on an intentional disturbance, and analysis of a faulty output accompanying the fault injection. Clock glitches have been frequently used for fault injection in previous research, but these researches are limited to setup time violations for combinational circuits. In setup time violations for combinational circuits, to inject a transient fault applicable to the analysis, glitch insertion timing is required to correspond to a slight difference in delay time for each data bus. Therefore, under the situation of shrinking fabrication process dimensions of semiconductor, the difference of delay time in combinational circuits is decreasing, and it is difficult to apply conventional fault analysis to cryptographic modules.

In this research, faults due to timing violation of input to sequential circuits are focused. Then, the possibility to extract the secret key from the outputs containing faults is being discussed. Outputs with faults discussed in this paper can be injected by inserting glitches at appropriate timings during the delay time when value transitions occur, so precise timing control is not required. Therefore, there is a possibility that the proposed fault analysis method can be also applied to a cryptographic module even if the situation of shrinking fabrication process dimensions of semiconductor. In the experiment, the proposed method is applied to a cryptographic module that implements the Advanced Encryption

*Master's Thesis, Graduate School of Science and Technology, Nara Institute of Science and Technology, March 13, 2020.

Standard (AES), a widely used symmetric-key algorithm, and demonstrated that a secret key can be extracted. In addition, a countermeasure method by adding a fault detection circuit is also proposed and examined.

Keywords:

side-channel attack, fault analysis, sequential circuit, timing violation

目次

図目次

第 1 章　序論

1.1　研究背景

1.1.1　情報セキュリティと暗号技術

現代では、PC(Personal Computer) やスマートフォン、更にはネットワーク家電に至るまで、身の回りのあらゆる情報機器がネットワークに接続され、様々な用途で利用されている [1]。このように、情報通信技術への依存度が高まった現代社会において、情報セキュリティの確保は重要な課題である。

暗号技術は、情報セキュリティの 3 大要素である、情報の機密性 (Confidentiality)・完全性 (Integrity)・可用性 (Availability) の維持を担う基盤技術である。現代の暗号技術は、公開鍵暗号方式と共通鍵暗号方式の 2 つに大きく分類できる。公開鍵暗号方式は、暗号化と復号に使用する鍵が異なる方式で、暗号化に使用する公開鍵は一般に公開し、復号に使用する秘密鍵は第三者に知られないように復号者の下で管理する。これにより、事前の鍵共有が不要という特徴を持つ。代表的な公開鍵暗号アルゴリズムとしては RSA(Rivest-Shamir-Adleman)[2][3]、楕円曲線暗号 [4] が知られている。共通鍵暗号方式は、暗号化と復号に同様の秘密鍵を使用する方式で、秘密鍵は第三者に知られないように両者で別個に管理される。共通鍵暗号方式は事前に両者で秘密鍵を共有する必要があるが、一般的に公開鍵暗号方式に比べ高速に動作可能という特徴を持つ。代表的な共通鍵暗号アルゴリズムとしては Camellia[5]、AES(Advanced Encryption Standard)[6]、KChiper-2[7] が知られている。上述した 2 つの暗号方式を用途により使い分ける形で情報セキュリティが確保されている。また、現代の暗号技術は秘密鍵が第三者に知られないことを前提に設計されており、仮に秘密鍵の情報が漏れた場合には暗号技術は完全に無効化され、重大なセキュリティ低下を招く。

1.1.2　暗号モジュールに対するサイドチャネル攻撃

暗号技術の実装形態のひとつとして、暗号化処理の高速化や省電力化、安全性の向上を目的とした、ASIC (Application Specific Integrated Circuit) や FPGA

(Field-Programmable Gate Array) などを用いたハードウェア実装がある。USB (Universal Serial Bus) トークンや RFID (Radio-Frequency Identification) タグ、IC(Integrated Circuit) を内蔵したスマートカードなど、比較的計算資源が潤沢でない機器においては、小型で消費電力が小さいハードウェア実装が適している。また、PC やオーディオ・ヴィジュアル機器、ネットワーク機器など比較的大型の情報機器においても、処理の高速化などを目的にハードウェア実装が利用されている。本論文では暗号アルゴリズムをハードウェア実装したモジュールを暗号モジュールと呼ぶ。

暗号モジュールにおいて、秘密鍵情報を含む物理情報の漏えい等のハードウェアレベルでの脆弱性があった場合には、ファームウェアのアップデート等のソフトウェアレベルの施策では対策が困難である場合が多い。対策のためには、暗号モジュールに対して物理的に変更を加えるハードウェアレベルでの修正が必要となる。しかし、流通後の製品に対してハードウェアレベルの修正を加えることは現実的でなく、ハードウェアレベルでの脆弱性の存在は重大なセキュリティ低下を引き起こす。このような背景から、情報セキュリティ確保のためには、ハードウェアレベルでの脆弱性の存在しない暗号モジュールを設計する必要がある。

暗号モジュールのハードウェアレベルでの脆弱性を利用した脅威として、サイドチャネル攻撃 (Side-Channel Attack) が知られている。サイドチャネル攻撃とは、暗号モジュールの正規の入出力情報である平文・暗号文ではなく、消費電力や処理時間などの非正規の入出力情報 (サイドチャネル情報) を、攻撃者が不正に利用することで秘密鍵を取得する脅威の総称である。このサイドチャネル攻撃は図 1.1 に示すようにパッシブな攻撃とアクティブな攻撃の 2 種類に分類できる。パッシブな攻撃では、攻撃者は暗号モジュールの動作に伴い生じる、消費電力の変動、漏えい電磁波の変動、処理時間などの非正規の出力をサイドチャネル情報として利用し、解析を実施することで秘密鍵を取得する。代表的な解析手法としては、タイミング解析 (Timing Analysis)[8]、差分電力解析 (Differential Power Analysis)[9][10]、相関電力解析 (Correlation Power Analysis)[11] 等が挙げられる。一方、アクティブな攻撃では、暗号モジュールに対して、非正規の入力である外乱を与え、それに伴う不正な動作や誤り出力を利用し、解析を実施することで秘密鍵を取得する。一般的に、アクティブな攻撃は機器に対して手を加えるため、パッシブな攻撃に比べて

強力であることが知られており、このような攻撃は故障利用解析 (Fault Analysis) と総称され、多くの検討が行われている [12]-[28]。

1.1.3 暗号モジュールに対する故障利用解析

故障利用解析では、暗号モジュールに対して意図的に物理的な外乱を与えることで、一時的な故障 (Transient Fault) を発生させる。ここで一時的な故障とは、暗号モジュール全体の動作を停止させるような永続的な故障 (Permanent Fault) ではなく、一時的にビット誤りなどの誤動作が発生し、その後正常な動作に回復する程度の故障を指す。攻撃者は、一時的な故障により得た誤り出力等の情報を元に、解析を実施することで秘密鍵情報を取得する。故障利用解析に関する研究は、特定の故障モデルが注入可能であると仮定した上で、秘密鍵を取得する解析手法について検討する「秘密鍵解析」に関する研究と、実際にそのような故障を発生させる手法について検討する「故障注入」に関する研究がそれぞれ並列に行われてきた。

故障利用解析に関する両研究を元に、セキュリティ確保のため暗号モジュールの故障利用解析に対する耐性を高めるには、適切なセキュリティ境界の設定が必要である。この場合のセキュリティ境界とは、暗号モジュールが故障利用解析の脅威対

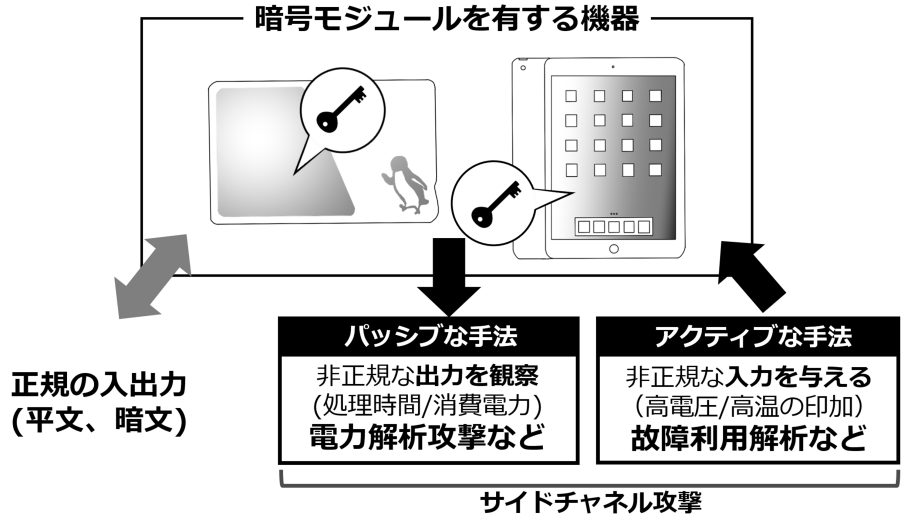


図 1.1 サイドチャネル攻撃の分類

象となるか否かの境目のことであり、脅威対象である場合には、対策を実施することでセキュリティを確保する必要がある。セキュリティ境界を適切に設定するためには、対象の暗号モジュールが実際に運用される状況を考慮し、その状況下で実際に故障が注入され、秘密鍵が取得される可能性について考える必要がある。

過去の検討により、攻撃者が利用可能な故障注入手法として、暗号モジュールの電源電圧を低下させる手法 [12][13]、白色光やレーザーを暗号コアのメモリに照射する手法 [14][15]、X 線を照射する手法 [15]、IC 近傍で強力な電磁波パルスを印加する手法 [16]、クロックにグリッチ (Clock Glitch) を挿入する手法 [17] などが報告されている。これらの手法のうち、レーザーや、X 線を照射する手法は、暗号モジュールに対して侵襲し、特殊なセットアップを用いて故障注入を行うため、高度な専門知識が必要であり攻撃コストが高い。それに対して、クロックにグリッチを挿入する手法は、安価な機器のみで比較的容易に実行が可能であるため、攻撃コストの低い故障注入法として知られている。近年では、暗号モジュールへの接近が困難である場合にも、暗号モジュールの電源線に電磁プローブをクランプし、電磁波印加を行うことで、遠方から非侵襲にクロックにグリッチを挿入し故障を注入可能であることも示されている [18]。このように、クロックグリッチを用いた故障注入法は攻撃コストが低い上、暗号モジュール遠方から非侵襲に実行される可能性があり、非常に多くの暗号モジュールが脅威の対象になると考えられる。そこで、安全な暗号モジュールを実現するためには、クロックグリッチを用いた故障注入に基づく故障利用解析の脅威に対する議論が求められる。

1.1.4 クロックグリッチを用いた故障利用解析

クロックグリッチとは、クロックに生じるパルス状のノイズであり、クロック入力を受信する回路において、立上りとして認識される場合がある。攻撃者はこれを意図的に発生させることでクロックの立上りタイミングでデータ取込みを行っている暗号モジュールに対して故障を注入する。

従来の検討において議論されているクロックグリッチを用いた故障注入のイメージを図 1.2 に示す。図 1.2 は演算を行う組み合わせ回路 (Combination Circuit) とクロックの立上りでデータ取込みを行う順序回路 (Sequential Circuit) からなる一

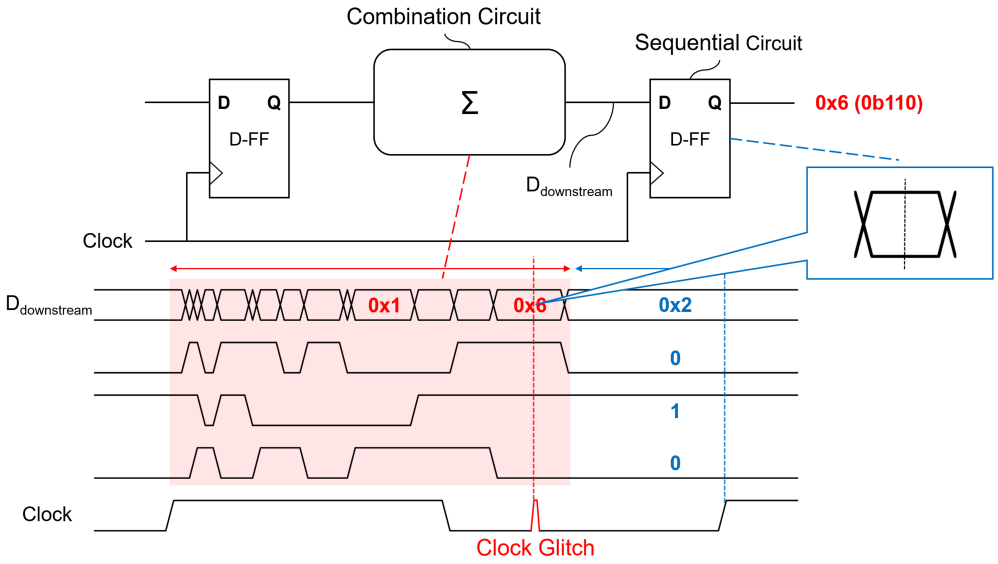


図 1.2　組み合わせ回路のセットアップタイム違反による故障

般的なクロック同期式回路のデータフローを示している。組み合わせ回路が正規の演算結果を出力する定常状態に至るまでには、図中に赤い領域で示したような伝搬遅延時間が存在する。定常状態に至る伝搬過程では、組み合わせ回路の実装に依存し、正規の出力とは異なる値を取る。図中に青い点線で示したように、通常は組み合わせ回路の出力が定常状態となった後に、データ取込みが行われるよう十分余裕を確保したクロック周期が設定されている。図 1.2 の場合では、正規のクロックタイミングでの取込みでは正規の演算結果である 0x2(0b010) が順序回路のフリップフロップ (FF: Flip Flop) によりビット単位で取込まれる。

しかし、クロックグリッチによる故障注入が行われた場合、図中の赤い点線に示したように取込みタイミングが早まり、組み合わせ回路が正規の値に落ち着く前にデータ取込みが行われ、セットアップタイム違反による故障が生じる。図 1.2 の場合では、遷移過程の非正規の演算結果である 0x6(0b110) が取込まれる。このとき、図中に青い枠で示したように、順序回路のフリップフロップにおける値取込みでは、どのビットの取込みにおいても違反は生じおらず、値を正常に取込んでいる。そのため、本論文ではこの故障を「組み合わせ回路のセットアップタイム違反による故障」と呼ぶ。

従来のクロックグリッチによる組み合わせ回路のセットアップタイム違反を対象

とした故障注入では、解析に適用可能な誤り出力を得るために、クロックに同期して並列に行われる演算毎の組み合わせ回路の伝搬遅延時間の差異を利用して、特定の演算のみが伝搬過程にあるタイミングでグリッチ挿入を行っていた。

しかし、半導体集積技術の進歩に伴うプロセスの微細化・高速化により伝搬遅延時間が縮小してきており、テクノロジの発展と共に組み合わせ回路の伝搬遅延時間の差異に着目した従来の故障注入は困難化し、それを利用した故障利用解析の脅威は縮小すると考えられる。

一方、クロックグリッチによりデータ取込みを担う順序回路の値取込みに対して故障注入が可能であり、その誤り出力に対して故障利用解析が適用できる場合には組み合わせ回路の伝搬遅延時間の差異を狙ったグリッチの挿入は不要となる。そのため、テクノロジの発展と共に攻撃範囲が縮小すると考えられていた故障利用解析の適用範囲が再び拡大する可能性がある。そこで、安全な暗号モジュールを設計するためには順序回路の故障に着目した故障利用解析について検討を行うことでセキュリティ境界を明らかにし、対策手法を適用していくことが求められる。

1.2 本研究の目的

前節で述べた背景を踏まえ、本論文では攻撃者が暗号モジュールのクロックに対してグリッチを挿入可能である状況を想定し、順序回路の値取込みに生ずる故障に着目した故障利用解析の実現可能性について検討すると共に、その脅威範囲と対策手法について議論することを目的とする。

具体的には、図 1.3 に示すように、遷移途中の不正な入力が順序回路のフリップフロップで取り込まれる入力タイミング違反 (本論文では、以後これを「順序回路の入力タイミング違反」と呼ぶ。) を対象とした故障注入に着目し、故障により得られる誤り出力から秘密鍵の取得性について検討すると共に、追加回路による対策手法についても議論する。

1.3 本論文の構成

本論文の構成は以下の通りである。

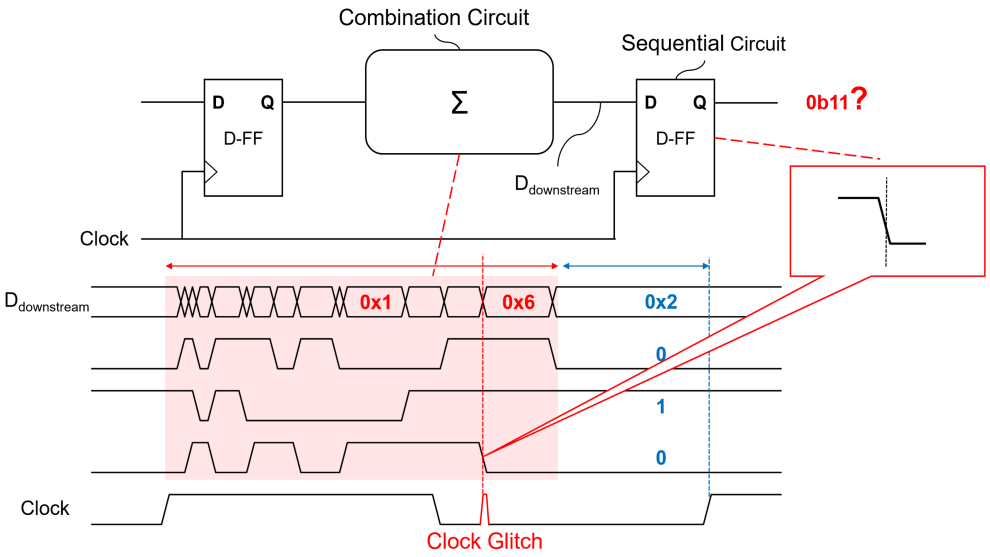


図 1.3　順序回路の入力タイミング違反による故障

第 2 章では、順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析手法を提案する。提案手法は故障注入と秘密鍵解析で構成され、故障注入では暗号文の持つ頻度分布の一様性の低下を誘発し、秘密鍵解析では、その一様性の低下を利用して秘密鍵を取得する。

第 3 章では、第 2 章で提案した故障注入の有効性を示すため、順序回路の入力タイミング違反により取込まれた値の一様性が低下することを基礎実験により実証する。

第 4 章では、第 2 章で提案した手法を組み合わせ回路の実装が異なる 3 つの AES 暗号モジュールに対して適用し、秘密鍵の取得性から提案手法の実現可能性について議論する。また、対策手法についても論ずる。

第 5 章では、本論文の結論を述べる。

第 2 章　順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析手法の提案

本章では、順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析手法を提案する。提案手法は故障注入と秘密鍵解析で構成され、故障注入では暗号文の持つ頻度分布の一様性の低下を誘発する。秘密鍵解析では、その一様性の低下を利用して秘密鍵を取得する。

2.1　順序回路の入力タイミング違反に着目した故障注入

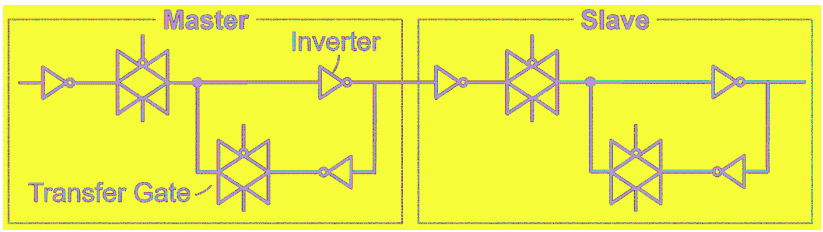
本節ではまず、順序回路における値取込み原理と入力タイミング違反により生ずる可能性のある準安定状態 (Metastable) について概説する。次に、順序回路の入力タイミング違反が引き起こされた場合に、物理的な特性により取込まれる値が High/Low のいずれかに偏る原理について述べる。最後に、クロックグリッチを用いて順序回路の入力タイミング違反による故障を注入し、一様性の低下を誘発する手法について述べる。

2.1.1　順序回路における値取込みと準安定状態

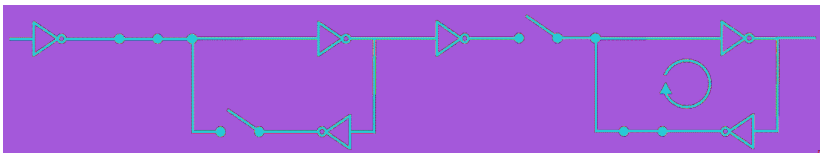
順序回路における値取込み原理と入力タイミング違反によりに生じる可能性のある準安定状態について概説する。

順序回路の値取込み・保持は、クロック信号の立上がりで入力データを取込み、次の立上がりまでその値を保持する機能を持つポジティブエッジ型の D フリップフロップ (D-FF) と呼ばれる 1 ビットの記憶素子が担っている。図 2.1 にその回路構造と動作を示す。D-FF は、図 2.1(a) のように、スイッチの役割を果たすトランスファーゲート (Transfer Gate) とインバータ (Inverter) を 2 個使用したラッチ回路が前後に接続されたマスタースレーブ (Master-Slave) 構成である。図 2.1(b) のように、クロック信号が Low の時は、前段のラッチ回路に入力値を格納し、後段のラッチ回路では前のサイクルの値を保持し出力する。このとき前段と後段を接続するトランスファーゲートはオフであるため信号は伝わらない。図 2.1(c) のように、

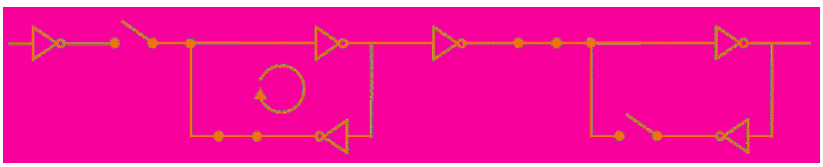
クロック信号が High の時は、前段のラッチ回路で保持した値を後段へ伝送する。このときデータ入力のトランスファーゲートはオフであるため、D-FF へデータは入力されない。これによりクロックの立上がりで値を取込み、次の立上がりまで保持する機能を実現している。しかし、入力データの到達が遅く入力データが前段のループを 1 周していない場合には、出力値が Low と High の間で揺れる準安定状態となる問題が知られている [29][30]。また、次のデータ入力の到達が速すぎた場合にも、ループを 1 周する前に次のサイクルで取込むべき値を取込み、同様に準安定状態となる可能性がある。図 2.2 に入力タイミング違反による準安定状態のイメージを示す。図 2.2 に示したように、準安定状態は極めて稀な場合を除き、High または Low のいずれかに落ち着くことが知られており、どちらに落ち着くかは温度、電源電圧等から決定される確率に従う [30]。このように、正しい値取込みのためにはクロックの立上がり前後で値を確定・保持していなければならない。立上り前の時間はセットアップ時間 (Setup Time)、立上がり後の時間はホールド時間 (Hold Time) と呼ばれる。



(a) 回路構成



(b) Master 動作時 (クロック信号が Low の時)



(c) Slave 動作時 (クロック信号が High の時)

図 2.1　ポジティブエッジトリガ型 D フリップフロップの回路構成と動作

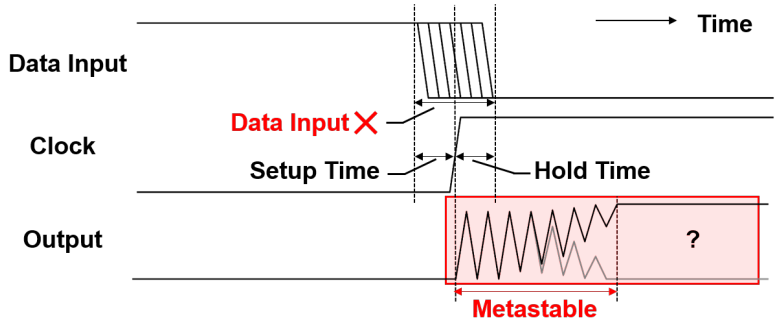


図 2.2　準安定状態のイメージ

2.1.2　順序回路の入力タイミング違反時の取込み値に生ずる偏り

順序回路において値取込み・保持を担うフリップフロップへの入力タイミング違反が引き起こされた場合、つまり遷移中の電気信号が任意のタイミングで取込まれた場合に、取込まれる値に偏りが生じる原理ついて述べる。

入力タイミング違反時には以下の 2 つの要因から High/Low のいずれかが取込まれる確率が高くなる。

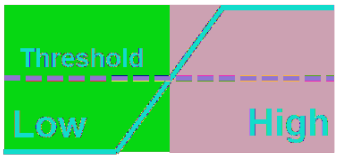
(1) 遷移中のアナログの電気信号を、デジタル回路において High/Low として認識する場合の境界に偏りがある。
(2) 準安定状態を経て、定常状態で落ち着く値が、High/Low のいずれかに偏りがある。

ここで、(1) は電気信号であるデータ信号をデジタル値で認識する際の閾値設定に関する要因である。図 2.3 に High/Low の境界が Low に偏るイメージを示す。図 2.3 の (a) は理想的な場合、(b) は閾値が中央に設定されていない場合、(c) は立上がり波形が非線形な場合のイメージをそれぞれ表している。(a) では、遷移途中の電気信号が High とみなされる範囲と Low とみなされる範囲は等しい。それに対して (b)、(c) では、Low とみなされる範囲が広くなっている。そのため、(b)、(c) のような要因が存在する場合に、入力タイミング違反により遷移途中の値取込みが行われると Low に偏りやすくなる。

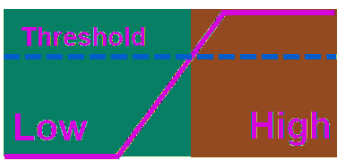
それに対して、(2) は 2.1.1 節で述べた準安定状態に関する要因であり、値取込

みを行う 2 つのインバータで High/Low の異なるデータが取込まれた際に生じる。前述したように、準安定状態が High/Low のどちらに落ち着くかは、温度や電源電圧等に依存する確率に従うため、この確率に偏りがある場合には取込まれる値の偏りの要因となる可能性が考えられる。

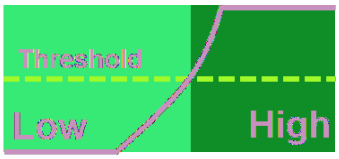
以上の 2 つの要因を考慮して、フリップフロップへの入力タイミング違反による値取込みについて考える。図 2.4 に (1) および (2) の要因により、取込み値に偏りが生ずるイメージを示す。この図に示したように、内部のアナログ値のデータ信号は、内部閾値で引かれる境界により High/Low のデジタル値として解釈される。このとき、(1) の要因により偏りが生じ、図中①に示したように、Low が取込まれる確率が高くなる。更に、図中に②で示したように、その境界で値が取込まれる場合には、準安定状態が生じる可能性がある。このとき、(2) の要因により偏りが生ずる可能性がある。このように、(1) と (2) の要因は分離して考えることは困難であり、両者が同一の値へ偏るようにバイアスをかけている場合および、打ち消す方向にバイアスをかけている場合の両方が考えられる。ここで、(2) の要因となる準安定状態は稀な場合であるため、(1) の要因が取込まれる値の偏りに対してより支配的になると考えられる。このように、入力タイミング違反が引き起こされ、遷移途中の不正な値が取込まれた場合には取込まれる値は、High/Low のいずれかに偏ると考えられ、この偏りを決定する要因はいずれも順序回路の物理的な特性に依存している。



(a) 理想状態



(b) 閾値が中央でない



(c) 非線形な立上がり波形

図 2.3　取込み値の偏りの要因となる閾値

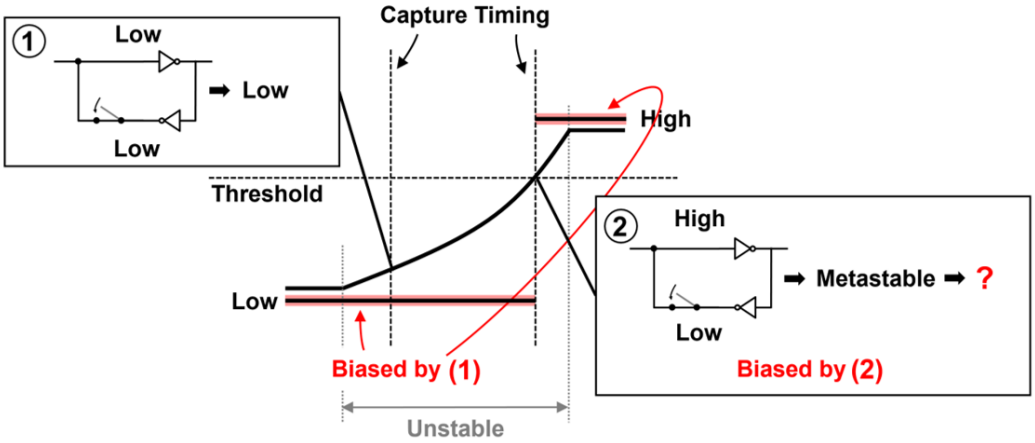


図 2.4　順序回路の入力タイミング違反により取込み値に偏りが生じる原理

2.1.3　クロックグリッチを用いた順序回路の入力タイミング違反による故障の誘発

本節では、クロックグリッチを用いて順序回路の入力タイミング違反による故障を注入し、誤り出力の一様性の低下を誘発する手法について述べる。

順序回路の入力タイミング違反は、従来クロックグリッチによる故障注入で対象としていた、組み合わせ回路のセットアップタイム違反の特殊な例である。組み合わせ回路のセットアップタイム違反時には、順序回路のフリップフロップによりビット単位で正常に値が取込まれているのに対して、順序回路の入力タイミング違反時には、順序回路のフリップフロップでの取込みそのものに故障が生じている点で異なる。

前述したように、順序回路の入力タイミング違反は、組み合わせ回路の伝搬過程における遷移タイミングで値取込みが行われた場合に生じる。この組み合わせ回路における定常状態に至るまでの不要な値の遷移はハザード (Hazard) と呼ばれ、消費電力の大きな要因となることから暗号モジュールの回路設計の観点からも議論されている [34]。後方にハザードが伝搬しにくい AND 回路を入力側に実装する等、回路設計を工夫することでハザードの抑制は可能であるが、ハザードの全く生じない回路設計は困難である。そこで、暗号モジュールの組み合わせ回路におけるハザードを利用した順序回路の入力タイミング違反の誘発のイメージを図 2.5 に示

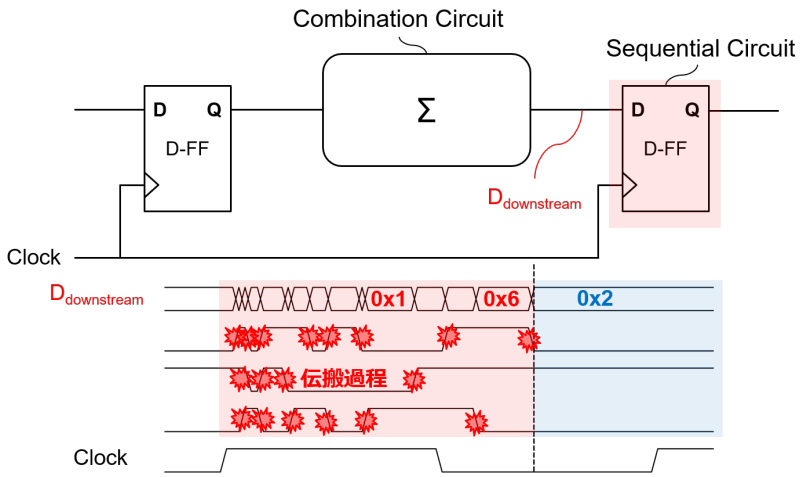


図 2.5　クロックグリッチを用いた順序回路の入力タイミング違反による故障の誘発イメージ

す。ハザードが生じるタイミングに合わせてグリッチを挿入し、順序回路の入力タイミング違反による故障を確実に引き起こすのは困難であるが、図 2.5 に示したように、クロック同期回路ではクロックの立ち上がりタイミングで複数のビットの取込みが各フリップフロップで行われるため、全ビットが伝搬過程にあるような適当なタイミングでクロックにグリッチを挿入することで、いずれかのビットにおいて入力タイミング違反を誘発できる可能性が高い。そのため、このような故障注入を複数回実施し、得られた誤り値をビット単位で統計的に調査することで、High または Low への偏りが確認できると考えられる。

以上より、全ビットが伝搬過程にある適当なタイミングでグリッチを挿入する故障注入を複数回行うことで、誤り出力のハミング重み (HW:Hamming Weight) の平均値を増加または低下させることができ、一様性の低下が誘発可能である。

2.2　順序回路の入力タイミング違反に着目した秘密鍵解析

本節では、前節で述べた順序回路の入力タイミング違反により生ずる誤り出力の一様性の低下を利用した秘密鍵解析手法について述べる。

通常の暗号化処理においては、任意の平文を暗号化した際、中間値や暗号文の頻

度分布は一様性を持ちランダムな値が出力される。一方、故障注入時には中間値や出力の一様性が低下する場合がある。こうした一様性の低下を用いて秘密鍵を取得する SFA(Statistical Fault Analysis) と呼ばれる統計的な解析手法が提案されている [24]-[28]。本提案手法である順序回路の入力タイミング違反に着目した故障利用解析における秘密鍵解析では、SFA を使用する。

図 2.6 に、故障注入による誤り出力の HW の低下を利用した SFA のイメージを示す。SFA では、(1) 部分鍵に依存した演算の入力となる中間値において、故障注入で生じた誤りによって HW が低下することを仮定する。この時、部分鍵の鍵空間は全探索可能な広さである必要がある。次に、誤り出力値の集合に対し、(2) ある部分鍵を用いる演算において、出力値から部分鍵の候補全てに対する中間値の逆算を行い、候補鍵毎の中間値集合を得る。そして、(3) 中間値集合において誤った部分鍵で逆算した中間値は暗号アルゴリズムの特性上、一様性を有するのに対して、正しい部分鍵を用いた中間値は (1) の仮定から HW の低下により一様性が低下することを利用し、秘密鍵を推定する。図 2.6 では、試行回数を重ねて適用する誤り暗号文数を増やした場合、誤った鍵 (鍵 B-Z) を仮定した場合の中間値の平均 HW は一様性から一定の値に収束する。対して、正しい鍵 A を仮定した場合には、中間値の平均 HW の低下が有意にみられるため部分鍵が取得可能である。図 2.6 ではビットが Low に偏ることを仮定し HW の低下を利用したが、High に偏る場合も同様の手法で鍵推定が可能である。また、図 2.6 では部分鍵の 1 つを推定する手順を示したが、全ての秘密鍵を取得するには中間値全ての HW を操作する必要がある。

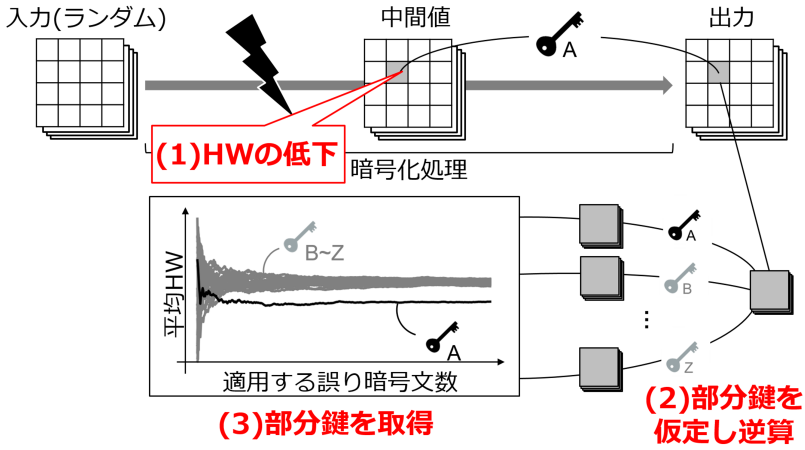


図 2.6　HW の低下を利用する SFA のイメージ

第 3 章　順序回路の入力タイミング違反時の取込み値に生ずる偏りの検証

本章では、2.1 節で提案した故障注入による一様性低下誘発の有効性を示すため、2.1.2 節で述べたように遷移中の電気信号を順序回路のフリップフロップにおいて任意のタイミングで取込んだ場合に、取込まれる値が High/Low の境界等の物理的特性により High/Low のいずれかに偏ることを実証する。

具体的には、順序回路のフリップフロップに対してクロック信号とデータ入力信号を外部機器から入力し、信号間の遅延時間を高精度に制御することで、入力タイミング違反を引き起こし、取込まれる値を観測する。図 3.1 に実験のイメージを示す。図 3.1 の左の入力信号の遷移部分に示したように High/Low の境界が遷移中の信号の中央にあると仮定した場合のパルス幅 T_P と、右の取込み結果において、50% 以上の確率で High が観測される境界を元に算出したパルス幅 T'_p を比較する。これによりタイミング違反時に取込まれる値の境界を間接的に測定し、High/Low のいずれかに偏りが生ずるか否かを明らかにする。$T_p = T'_p$ であれば、タイミング違反時にも一様性の低下が生じないことを示し、$T_p \neq T'_p$ であれば図中の赤枠のように High/Low いずれかが取り込まれる確率が高く、一様性の低下が生ずることを示す。

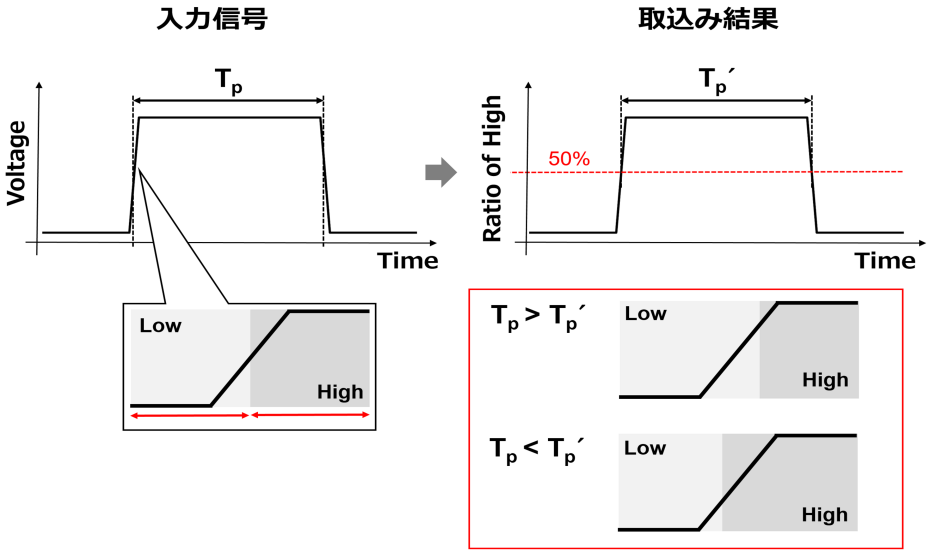


図 3.1　基礎実験のイメージ

3.1 順序回路の入力タイミング違反時の取込み値を測定するための実験環境

本節では、順序回路を FPGA 実装した単純な回路を対象とし、入力タイミング違反による取込みを行い、その取込み値を測定する基礎実験の実験環境と手順について述べる。

本実験では、実験対象として外部からの信号入力ポートおよび観測用ポートを有するサイドチャネル攻撃標準評価用基盤 SASEBO-G[31] を使用した。その外観を図 3.2 に示す。この SASEBO-G の FPGA2 にクロック信号の立上がりでデータ入力信号 D_{in} の取込みを行い、その取込み結果 D_{out} を常に出力するポジティブエッジ D-FF(Delay Flip Flop) 回路を実装した。実験系のブロック図および外観を図 3.3 に、使用した機器を表 3.1 に示す。クロック信号とデータ入力信号 D_{in} は同期した 2 台の任意信号生成器で生成し、それぞれ信号入力用の J3、J13 ポートから同期して入力した。取込み結果 D_{out} は SASEBO-G の入出力回路 (I/O) から出力し、オシロスコープで観測した。また、任意信号生成器とオシロスコープは PC により制御を行った。任意信号生成器で生成する 2 MHz の方形波であるクロック信号とパルス幅 T_p が 200 ns のパルス信号であるデータ入力信号 D_{in} を図 3.4 に示す。また本実験では、パルス信号を反転させた場合についても同様の実験を行った。これらの信号は FPGA の I/O を通して実験対象の D-FF 回路へと入力される。I/O ではアナログ・デジタル変換が行われるため、その影響により対象に所望する信号を入力できない可能性がある。そこで、I/O の影響を取り除くために図 3.5 に示すような構成で、実験対象内部の信号を観測しながら、データ入力信号 D_{in} の High の電圧値である V_{High} を変化させ、$T_p = 200$ ns となるように非反転時・反転時の信号に対してそれぞれ校正を行った。この校正の結果を表 3.2 に示す。

また本実験では、クロック信号に対するデータ入力信号 D_{in} の遅延時間を 0.01 ns 刻みで制御し、各遅延時間毎に、100 回のデータ取込みを行い、取込み結果 D_{out} を観測した。以上の実験をデータ入力信号 D_{in} の非反転時・反転時に対して同様に行った。

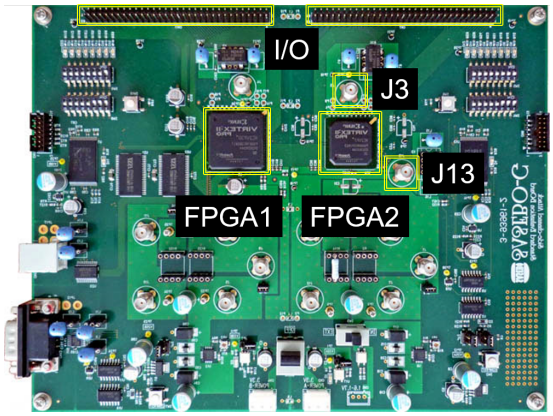
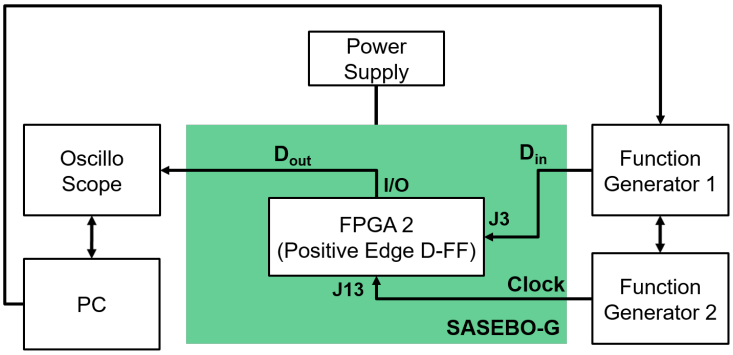
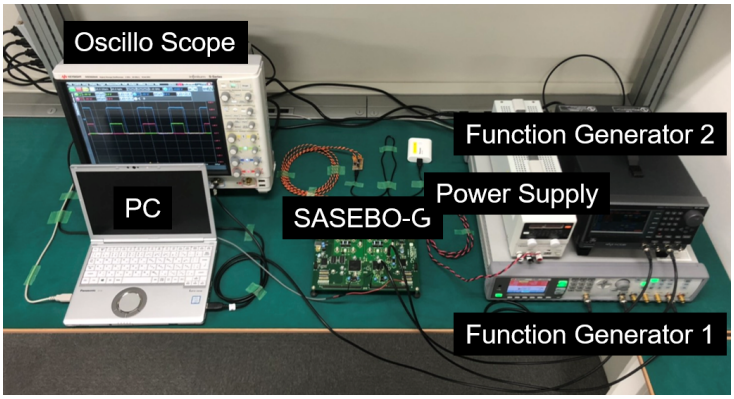


図 3.2　SASEBO-G の外観



(a) ブロック図

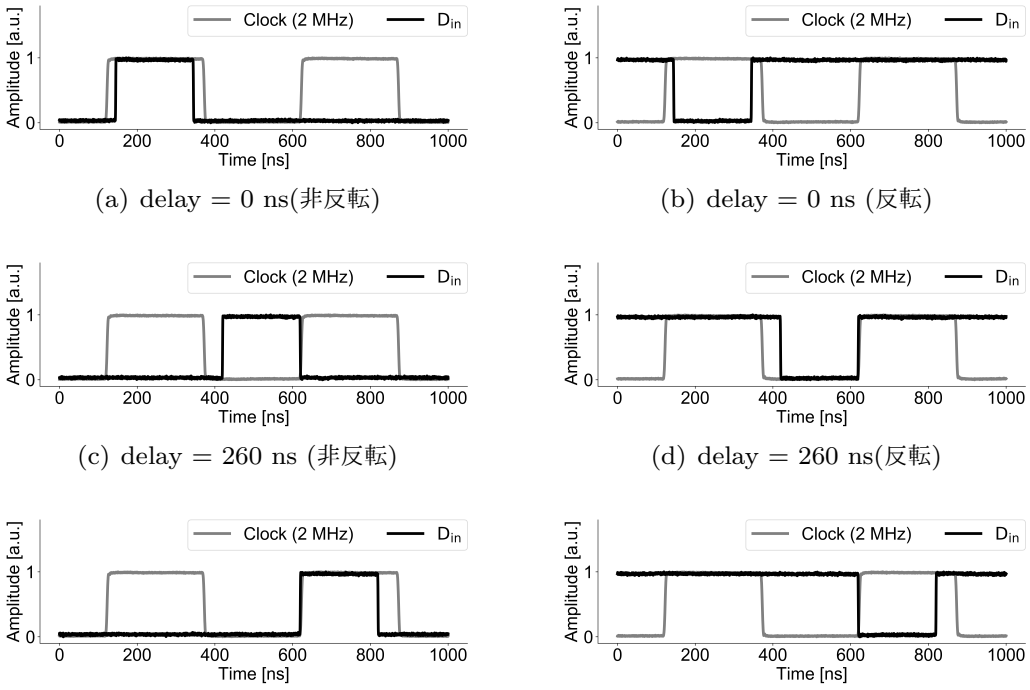


(b) 外観

図 3.3　基礎実験の実験環境

表 3.1　基礎実験に使用した機器

Power Supply	TEXIO PA18-3B
Oscillo Scope	Keysight DSOS204A
Function Generator 1	Keysight 81160A
Function Generator 2	NF WF1968
FPGA 2	Xilinx Virtex-II Pro xc2vp7-fg456-5



(a) delay = 0 ns(非反転)　(b) delay = 0 ns (反転)

(c) delay = 260 ns (非反転)　(d) delay = 260 ns(反転)

(e) delay = 460 ns (非反転)　(f) delay = 460 ns (反転)

図 3.4　基礎実験の入力信号

表 3.2　校正結果

V_{High} [V]	Reversed	Mean [ns]	Min [ns]	Max [ns]	Std Dev [ps]
1.31	False	200.076	199.805	201.138	205.705
1.28	True	199.958	199.837	200.057	34.449

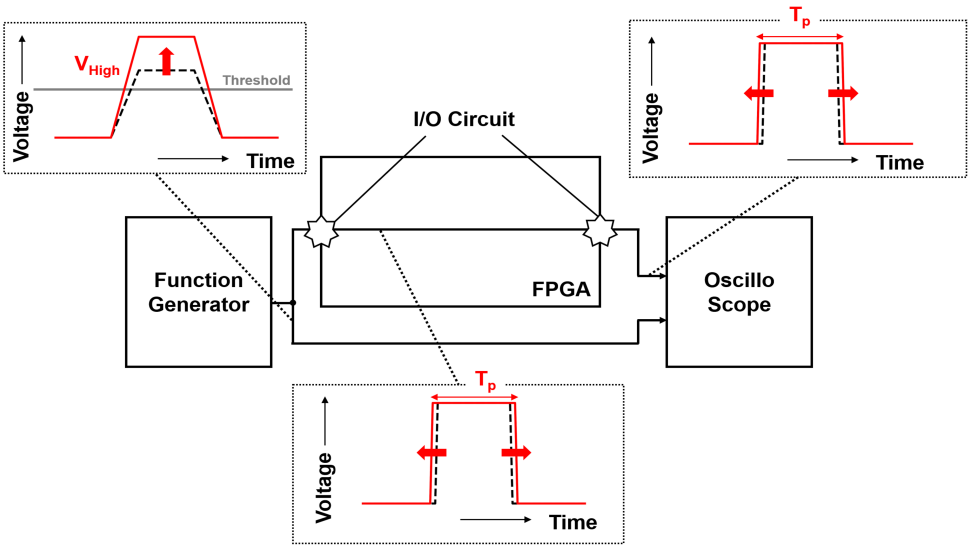
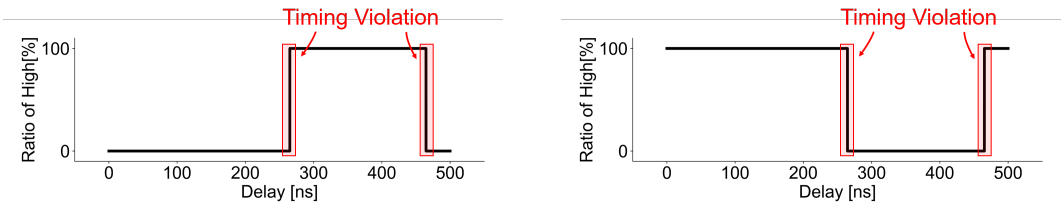


図 3.5　校正のイメージ

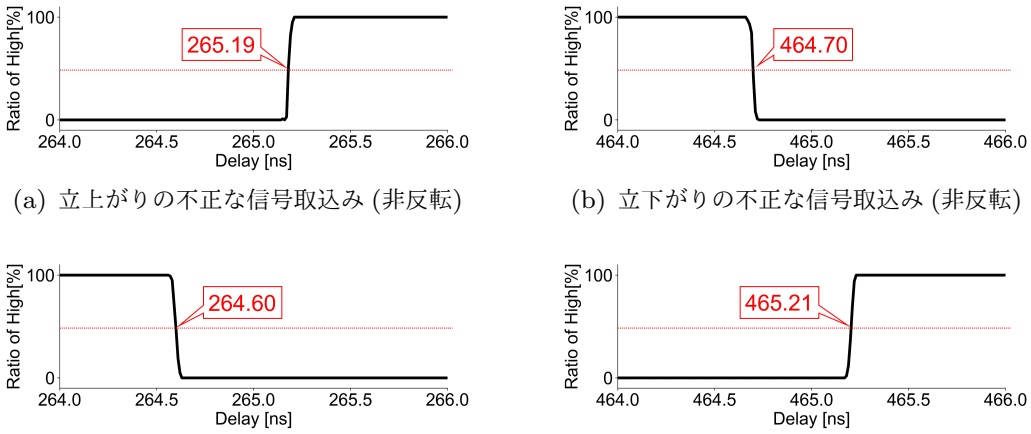
3.2　順序回路の入力タイミング違反時の取込み値の測定結果

図 3.6 に取込み値の測定結果を示す。ここで横軸はクロック信号とデータ入力信号間の遅延時間、縦軸は 100 回の取込みで High が観測された確率を表す。また、図 3.6 において赤く示した、入力タイミング違反による不正なデータ取込みが行われたと考えられる遅延時間 265 ns および 465 ns 周辺を拡大した結果を図 3.7 に示す。図 3.7 中には、50 % を横断したパラメタを赤字で示している。図 3.7 の (a) と (b) に着目すると、赤字で示したパラメタからデータ入力信号 D_{in} のパルス幅 T_p が 200 ns であったの対して取込み結果のパルス幅 T'_p は 199.51 ns(464.70-265.19) であることが確認できた。また、(c) と (d) に着目すると、同様にデータ入力信号 D_{in} のパルス幅 T_p が 200 ns であったのに対して取込み結果のパルス幅 T'_p は 200.61 ns(465.21-264.60) であることが確認できた。以上から、非反転時および反転時の両実験結果において約 0.5-0.6 ns 程度の偏りが確認でき、どちらも Low とみなされる領域が広くなっていることが確認できた。



(a) 非反転　(b) 反転

図 3.6　取込み値の測定結果



(a) 立上がりの不正な信号取込み (非反転)　(b) 立下がりの不正な信号取込み (非反転)

(c) 立下がりの不正な信号取込み (反転)　(d) 立上がりの不正な信号取込み (反転)

図 3.7　順序回路の入力タイミング違反時の取込み値の測定結果

3.3　まとめ

本章では、2.1 節で提案した故障注入の有効性を示すため、順序回路の入力タイミング違反により取込まれた値の一様性が低下することを実証する基礎実験を行った。

3.2 節で述べたように、順序回路の入力タイミング違反時の取込み値に偏りが生じ、一様性が低下することを確認した。また、本実験系においては入力タイミング違反時に取込まれる値が Low に偏ることを確認した。

第 4 章　順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析の実証と対策手法の検討

本章では、我が国における推奨暗号であり [32]、共通鍵暗号の世界的なデファクトスタンダードである AES を対象に第 2 章で述べた提案手法を適用し、秘密鍵の取得性から提案手法の実現可能性について議論する。また、対策手法についても論ずる。

4.1　順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析手法の AES への適用による有効性の実証

本節では、異なる実装方式で AES を FPGA 実装した 3 つの暗号モジュールに対して、第 2 章で述べた提案手法を適用する実験を行い、提案手法の有効性を実証する。また、本実験では AES への SFA に関する文献 [24] を参考に故障注入対象を 9 ラウンドとし、10 ラウンド入力の HW を低下させることで 1 バイト毎に部分鍵を取得する (図 4.1)。

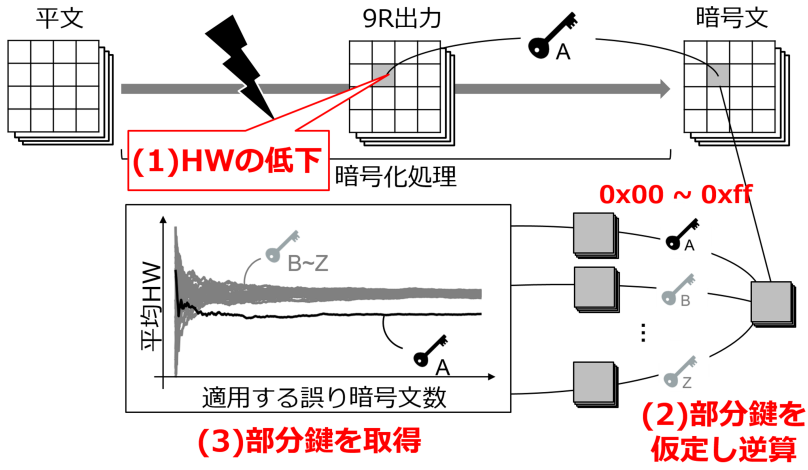


図 4.1　AES に対する SFA のイメージ

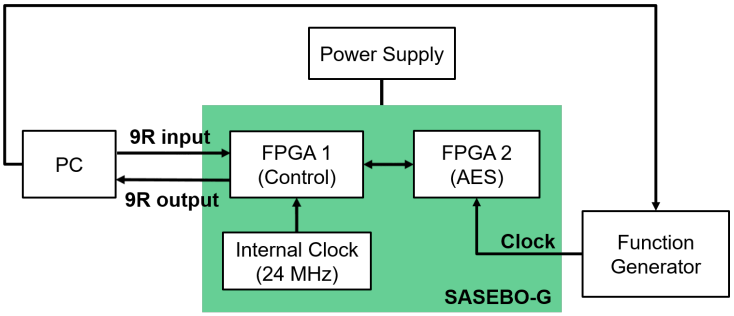
4.1.1 AES に対して順序回路の入力タイミング違反による故障を誘発する実験環境

本節では、本実験の実験環境と故障注入により出力される誤り暗号文の観測の手順について説明する。実験環境のブロック図および外観を図 4.2 に、使用した機器を表 4.2 に示す。本実験では第 3 章の実験において使用した SASEBO-G の FPGA2 に、表 4.1 に示した S-box を構成する組み合わせ回路の実装方式の異なる 3 つの 128 ビット AES 回路を実装した。また、FPGA1 には PC と通信やボードの制御を行う回路を実装した。各 FPGA は異なるクロックで動作しており、制御を行う FPGA1 に対しては通常通りに 24 MHz のクロックを供給した。暗号化を行う FPGA2 のクロックも FPGA1 と同様に通常 24 MHz で設計されているが、クロックグリッチを想定したクロック周期の短縮を行った。本実験では、再現性の向上のためにクロックを任意信号生成器で生成し、FPGA2 に実装した AES 回路のクロック入力へと接続されている J3 ポートから供給することで、クロックグリッチによるクロックの短縮を模擬した。

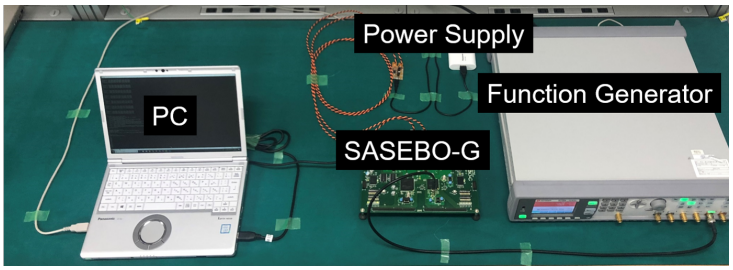
また、本実験では 9 ラウンドのみに故障注入を行うため、図 8 のフローチャートに示したように、AES の 1-10 ラウンドの処理のうち 1-8 ラウンドおよび 10 ラウンド処理を PC で、9 ラウンド処理のみを FPGA2 の AES 回路で実施しクロックグリッチを想定した故障を注入した。

本実験では、再現性を高めるために上記のセットアップを用いて実験を行ったが、実際の故障注入においても、スマートカードなど暗号モジュールに対して侵襲可能な状況を想定した場合には、攻撃者が特定のラウンドに故障を注入することが可能である。また、遠方からのクロックグリッチ挿入を想定した場合にも、暗号モジュールから生じる電磁波等のサイドチャネル情報から内部処理のトリガを得られる可能性も示されている [35] ことから現実的な攻撃を模擬した実験環境であるといえる。

グリッチ挿入タイミングを意味するクロック周期は、クリティカルパスに対して十分余裕があり、誤りが発生しない 12 ns を上限とし 0.5 ns 幅で減少させて順序回路に故障を注入した。試行回数 (N) は 5,000 とし、各クロック周期で 5,000 回の暗号化処理を行い、誤り暗号文を収集した。



(a) ブロック図



(b) 外観

図 4.2　故障注入実験の実験環境

表 4.1　故障注入実験に使用する AES の S-box の実装方式

AES-Comp[33]	合成体 (Composite field) を利用
AES-PPRM1[34]	1 ステージの AND-XOR 論理を利用
AES-PPRM3[34]	3 ステージの AND-XOR 論理を利用

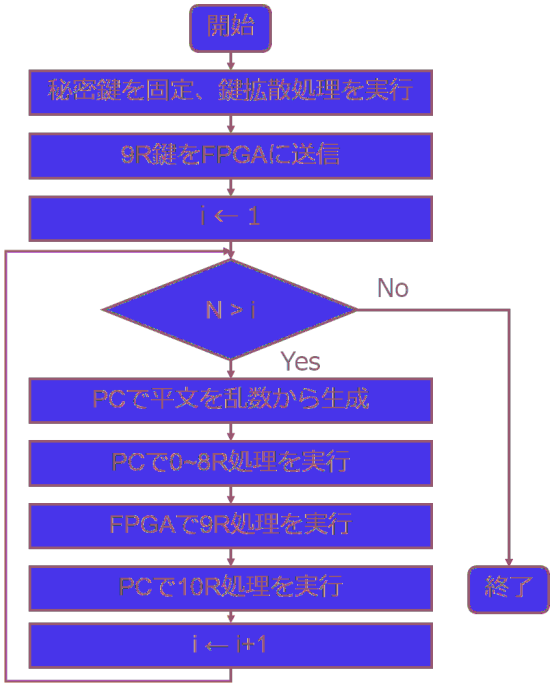


図 4.3　故障注入実験のフローチャート

表 4.2　故障注入実験に使用した機器

Function Generator	Keysight 81160A
FPGA 1	Xilinx Virtex-II Pro xc2vp30-fg676-5
FPGA 2	Xilinx Virtex-II Pro xc2vp7-fg456-5

4.1.2 秘密鍵取得結果

実験の結果、どの実装方式においても、FPGA2 の最大動作周波数を超えた動作周波数となるクロック周期 3 ns 以下では完全に FPGA2 上で暗号化処理が行われなくなった。そのためグリッチタイミングを 3.5 ns から 12 ns の間で変化させた場合の結果について示す。図 4.4 に各実装方式における、故障発生数を示す。図 4.4 の横軸はクロック周期、縦軸は 5,000 回の暗号化を行った際の故障発生数を表している。図 4.4 から、組み合わせ回路の実装方式の差異により、その伝搬遅延時間も異なり、故障が生じ始めるパラメタが違うことが確認できた。

AES-Comp の先頭バイトの部分鍵に対して解析を適用した結果を図 4.5 に示す。図 4.5 の横軸は解析に使用した誤り暗号文の数、縦軸は逆算した中間値の平均 HW を表している。図 4.5(a) は、正解鍵を仮定して使用して中間値を逆算した際に、誤った鍵を仮定した場合に比べて明らかに HW が低下した例であり、このような場合は秘密鍵が取得可能である。これに対し、図 4.5(b) は正解鍵を仮定した際の HW が誤った鍵を仮定した場合と分離できない例であり、このような場合は秘密鍵が取得できない。本実験では 5,000 個の誤り暗号文に対して解析を行い、鍵候補のうち最も HW の平均が低いものを正解鍵として推定を行った。

3 つの実装方式の AES の各グリッチタイミングでの故障注入で入手した、5,000 個の誤り出力の全 16 バイトに対して同様の解析を適用した結果を図 4.6 に示す。図 4.6 の横軸はクロック周期、縦軸は 16 バイトの秘密鍵のうち何バイトの鍵を正しく推定できたかを示している。図 4.6 から、どの実装方式に対してもクロック周期が 4 ns から 7 ns 程度のタイミングで取込みを行った際には誤り値の HW の低下が誘発され、半分以上の秘密鍵の取得に成功していることが確認できた。これは上述の 4 ns から 7 ns の区間では、多くのデータバスで値の遷移が繰り返されているため、グリッチを挿入することにより順序回路の入力タイミング違反が生じ、Low が取り込まれる確率が高くなり 10 ラウンドの入力値の HW が低下していることが原因と考えられる。

本実験の結果、故障注入による HW の低下が最も効率良く誘発可能であった 4 ns のグリッチタイミングにおいて AES-Comp では全 16 バイト、AES-PPRM1 では 15 バイト、AES-PPRM3 では 14 バイトの秘密鍵の取得に成功した。図 4.5 に示したように、HW が低下し部分鍵の推定に成功している場合には、誤った部分鍵

と有意に分離が可能である。そのため、14 バイトの秘密鍵が取得できた場合には、分離が不能であった残りの 2 バイトの鍵空間のみを探索することで全ての秘密鍵が取得できる。

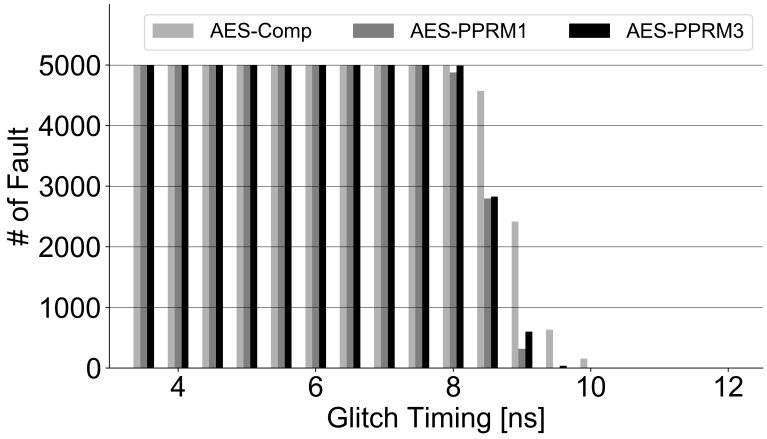
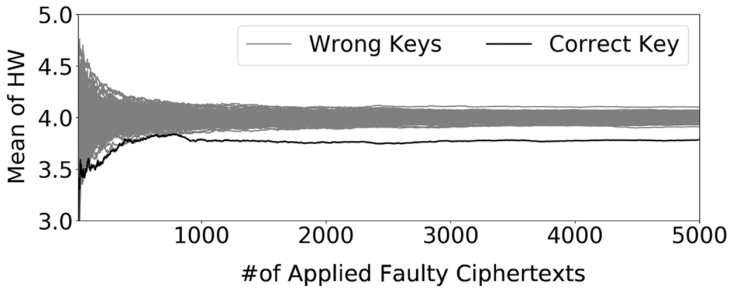
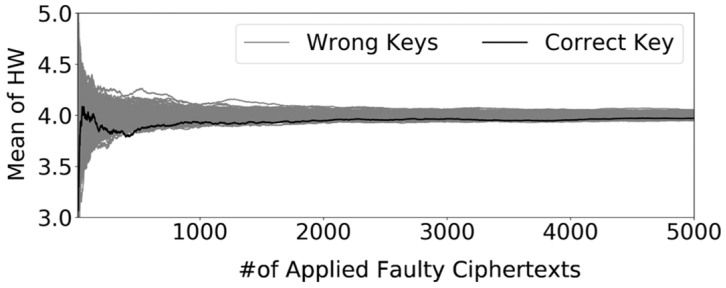


図 4.4　故障発生数



(a) 部分鍵が取得可能な波形 (Glitch Timing=4.0 ns)



(b) 部分鍵が取得不能な波形 (Glitch Timing=3.5 ns)

図 4.5　AES-Comp の先頭バイトの部分鍵取得結果

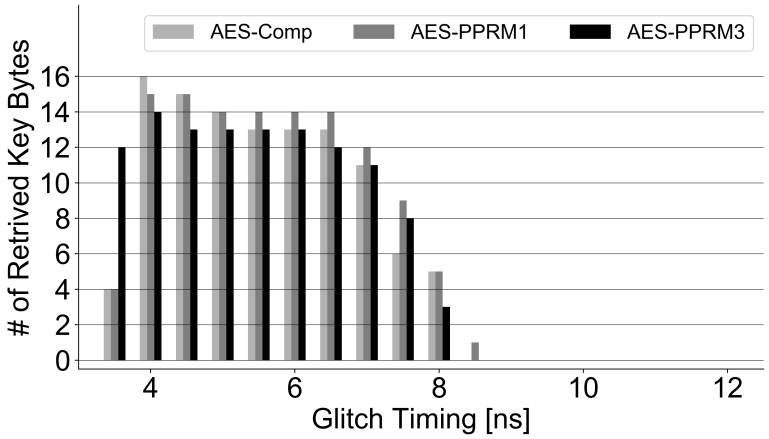


図 4.6　秘密鍵取得数

4.1.3　順序回路に着目した故障利用解析による脅威範囲の拡大に関する考察

4.1.2 節に示した実験結果より、本提案手法であるクロックグリッチを用いた順序回路の入力タイミング違反により生ずる誤り出力に基づく故障利用解析により秘密鍵が取得可能であることが確認された。

本節では、グリッチ挿入タイミングと秘密鍵の取得性の観点から、本提案手法と従来の組み合わせ回路のセットアップタイム違反を対象とした故障利用解析手法との比較を行う。従来 AES に対するクロックグリッチを用いた故障利用解析では秘密鍵の取得性の高さから差分故障解析 [22] が頻繁に適用されてきた。本実験結果における、差分故障解析に適用可能な 1 バイト誤りの発生数を図 4.7 に示す。図 4.6 と図 4.7 を比較することで、従来手法は組み合わせ回路の伝搬遅延時間の差異に着目しているため詳細なタイミング制御が必要であるのに対して、本提案手法では信号が遷移している適当なタイミングでグリッチを挿入することで秘密鍵解析に適用可能な誤りが誘発可能であり、より広い区間で秘密鍵が取得可能であることが確認できる。図 4.6 の 3.5 ns では秘密鍵の取得性が悪いがこれはグリッチ挿入タイミングが早く、信号の遷移が始まっていないためである。また、本提案手法は複数の誤り出力の統計的な性質を利用する手法である。そのため本実験では行っていないが、グリッチ挿入タイミングの制御が困難でありランダムなタイミングでグリッチ

挿入が行われる場合にも同様に秘密鍵が取得可能であると考えられる。

以上より本提案手法の有効性が示された。これにより従来グリッチ挿入タイミング制御が困難であり脅威対象外とされていた暗号モジュールもクロックグリッチを用いた故障利用解析の脅威対象となる可能性があり対策が必要である。

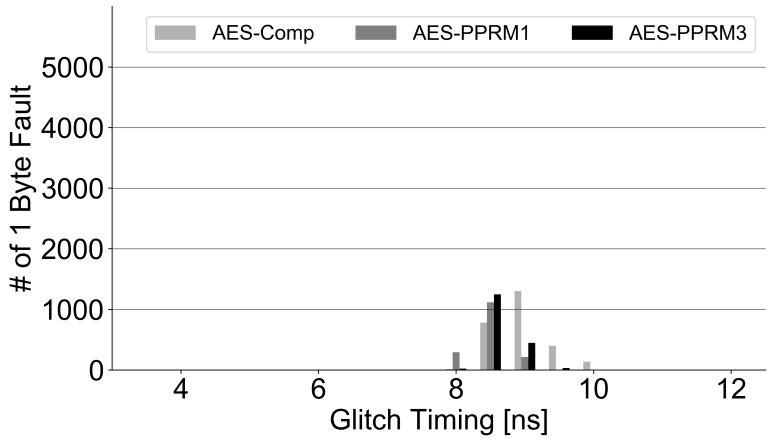


図 4.7　従来手法が適用可能な誤りの発生数

4.2　順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析に対する対策手法の検討

本節では、4.1 節で実証した新たな故障利用解析の脅威に対する対策手法について論ずる。

本論文で検討した故障利用解析で用いた故障注入は、従来の組み合わせ回路のセットアップタイム違反を対象としたクロックグリッチによる故障注入と同様の手順で引き起こされるため、対策手法についても同様の手法が適用可能であると考えられる。以下では、従来行われてきた故障利用解析に対する対策手法に関する議論を元に対策手法について論ずる。

4.2.1　故障利用解析に対する対策手法の分類

故障利用解析の脅威に対する対策手法は、今回対象とする脅威への対策に限らず一般的に、図 4.8 に示したように以下の 2 つに大きく分けられる。

(a) 故障注入を防ぐ対策
(b) 誤り暗号文の出力を防ぐ対策

ここで、(a) の故障注入を防ぐ対策を実施する場合には、図 4.8 に示したように攻撃者がアクセスできる範囲で実施されうる様々な故障注入法に応じて個別の対策が必要である。それに対して、(b) の誤り暗号分の出力を防ぐ対策は故障注入法に関わらず同一の対策が可能である。クロックグリッチは様々な手法により引き起こされることが報告されており、それら全てに対して物理的な対策を実施するのはコストの面から現実的ではない。そこで、以下では、低コストに一般的な対策が可能となる (b) の誤り暗号文の出力を防ぐ対策について述べる。

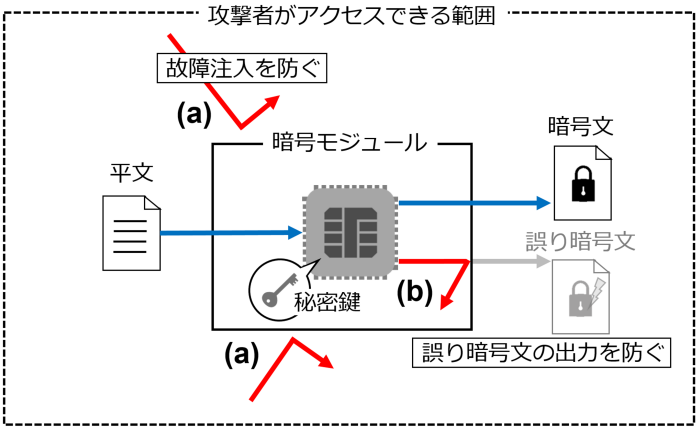


図 4.8　故障利用解析に対する対策手法のイメージ

4.2.2　順序回路の入力タイミング違反を検知する手法

誤り暗号文の出力を防ぐためには、故障による誤りを検知する必要がある。故障検知手法として、空間的または時間的に冗長性を持たせ、同一の演算を複数回行い

検算することで故障を検知する手法 (Doubling/Verification)[36][37] が代表的である。図 4.9 に A および B で同一の演算を行い (Doubling)、両演算の結果を比較することで (Verification)、故障を検出するイメージを示す。この手法は誤り値が生じたか否かに着目するため、故障注入法に依存せず実施することが可能である。しかし、SFA では、攻撃者が冗長性を持たせた複数の演算のうち、特定の演算のみに故障を注入できる場合、暗号モジュールは誤りのない出力のみを出力するにも関わらず、攻撃者が一様性の低下した偏りのある出力を入手可能であることが知られている [27][28]。そのため、検算に基づく検知手法は本論文で議論した新たな脅威に対する対策として不十分である。そこで検算を用いず、単一の演算のみで故障を検出し、出力を停止する手法が求められる。以下では、追加回路を実装することでクロックグリッチ等により生じるクロック周期の短縮 (オーバークロック) を検知する対策手法を紹介する。

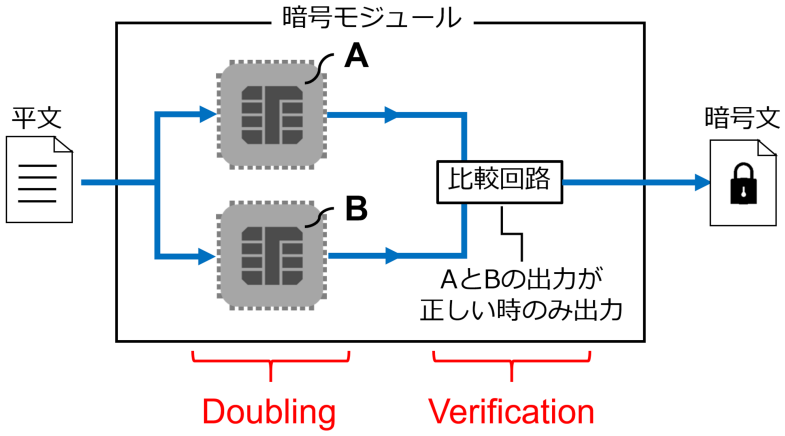


図 4.9　検算による故障検知のイメージ

遅延素子を用いた検知手法

文献 [38] における対策回路では、暗号化処理を実行する組み合わせ回路と並列に図 4.10 に示した遅延要素を配置する。遅延要素における遅延時間よりもクロック周期が十分長ければ組み合わせ回路の出力が回路全体の出力とする。対して、遅延時間に比べてクロック周期が短い場合には、オーバークロックが生じたと判断し、

組み合わせ回路による出力ではなく、別の無効な値を出力する。この手法ではオーバークロックによる違反を検出し、その場合には暗号回路の出力とは無関係な値が出力されるため、計算誤りが生じた場合であっても秘密鍵解析が困難となる。

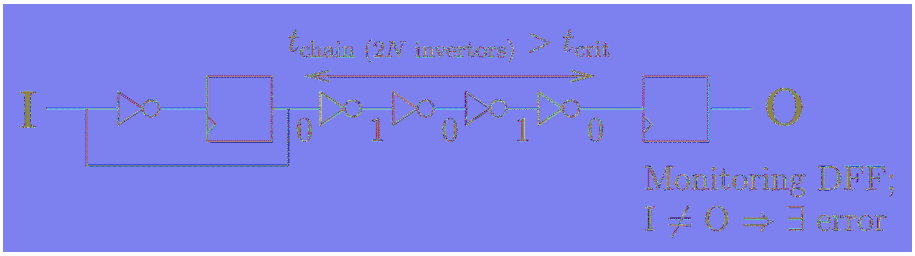


図 4.10　対策のため追加する遅延要素 ([38] の Figure.14 より引用)

桁上げ加算回路を用いた検知手法

文献 [39] は、図 4.11 に示す、非常に長い遅延時間を持つ加算回路を利用し、クロック周期を計測する評価手法を提案している。この評価回路では、0xFFFFFFFF（16 進数表記、2 進数表記では 1 が 128 個並ぶ）に 1 を足す計算を行う。評価回路では、下位ビットから次々と桁上げの伝搬が発生し、下位ビットの加算器から順に出力が 1 から 0 へ変化していく。ここで、桁上げの伝搬の途中で次のクロックの立上がりが到来した場合には、桁上げが伝搬したビットの出力は 0 となり、それよりも上位のビットは 1 のままとなる。クロック周期が短いほど 0 の個数が少なくなることから、0 の個数が極端に少なくなった場合にはオーバークロックが発生したと判断することができる。この回路を暗号処理回路と組み合わせて実装することができれば、違反の検出に利用可能であると考えられる。

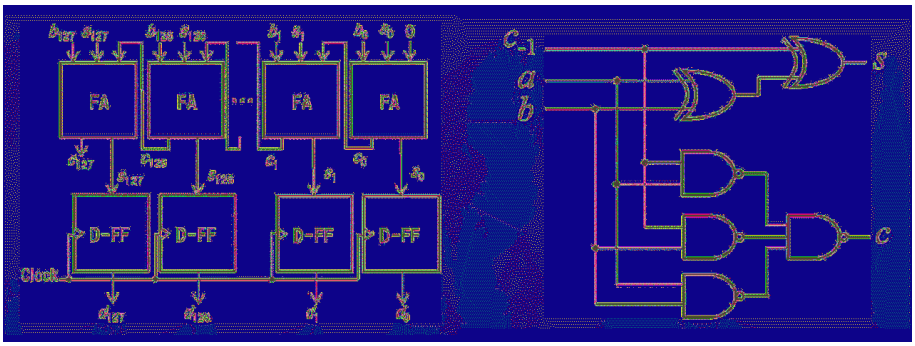


図 4.11　対策のため追加する桁上げ加算回路 ([39] の Figure.1 より引用)

第 5 章　結論

従来のクロックグリッチを用いた組み合わせ回路のセットアップタイム違反による故障注入では、解析に適用可能な誤り出力を得るために、組み合わせ回路の伝搬遅延時間の僅かな差異を狙いグリッチを挿入する必要があった。そのため、半導体集積技術の進歩に伴うプロセスの微細化・高速化による伝搬遅延時間の縮小に伴い、その脅威範囲は縮小すると考えられてきた。

一方、クロックグリッチによりデータ取込みを担う順序回路の値取込みに対して故障注入が可能であり、その誤り出力に対して故障利用解析が適用できる場合には、組み合わせ回路の伝搬遅延時間の差異を狙ったグリッチの挿入が不要となる。そのため、脅威範囲が再び拡大する可能性があり、安全な暗号モジュールを設計するためには、順序回路の故障に着目した故障利用解析について検討を行うことでセキュリティ境界を明らかにし、対策手法を適用していく必要があった。

そこで、本論文では、順序回路の入力タイミング違反に着目した故障利用解析の実現可能性の検討と対策手法についての議論を行った。

第 2 章では、順序回路の入力タイミング違反により生ずる誤りに基づく故障利用解析手法を提案した。提案手法は故障注入と秘密鍵解析で構成され、故障注入では暗号文の持つ頻度分布の一様性の低下を誘発する手法について述べ、秘密鍵解析では、その一様性の低下を利用した鍵解析について述べた。

第 3 章では、第 2 章で提案した故障注入の有効性を示すため、順序回路の入力タイミング違反により取込まれた値の一様性が低下することを基礎実験により実証した。

第 4 章では、共通鍵暗号 AES を FPGA 実装した暗号モジュールに対して第 2 章で述べた提案手法を適用しその有効性を実証した。また、秘密鍵取得のためのグリッチ挿入タイミングの制御について従来手法と比較し、本提案手法では組み合わせ回路の伝搬遅延の際に着目すること無く秘密鍵が取得可能であることを示した。更に、追加回路により故障を検知する対策手法を提案した。

以上より、順序回路の入力タイミング違反による誤りに基づく故障利用解析の実現可能性を示した。この故障利用解析は組み合わせ回路の伝搬遅延時間の差異を狙ったタイミング制御が不要であり比較的容易に実行可能であるため、従来、脅威

対象とされていなかった暗号モジュールにも脅威が及ぶ可能性がある。そのため、暗号モジュールのセキュリティ確保のため、本論文で論じた故障利用解析の脅威についても考慮したセキュリティ評価を行い、必要に応じて対策技術の検討が求められると考えられる。

謝辞

未筆ながら、本研究を行うにあたり、ご支援下さった皆様に深く感謝の意を表します。

本学の林優一教授には、日頃の研究活動において、丁寧かつ熱心な御指導、御鞭撻を賜りました。心より感謝申し上げます。

本学の岡田実教授及び藤川和利教授には、研究を進めるにあたり有益な御助言、御討論を頂きました。心より御礼申し上げます。

本学の藤本大介助教には、研究方針の策定や研究活動においての多くの御支援、御助言を賜り、学会参加に置いても御支援、御助言を頂きました。厚く御礼申し上げます。

本学の Youngwoo Kim 助教には、英文執筆をはじめとして研究活動においての多くの御支援、御助言頂きました。厚く御礼申し上げます。

仙台高等専門学校の衣川昌宏助教には、日頃の研究活動において、実験等に関わる様々な御支援、御助言を頂きました。厚く御礼申し上げます。

本研究室秘書の石谷由美様には諸手続きをはじめとして様々な場目でお世話になりました。厚く御礼申し上げます。

最後に、日頃の研究室生活において、様々な面でご協力いただきました、林研究室の皆様にこの場を借りて、深く感謝申し上げます。

参考文献

[1] 総務省, "令和元年版情報通信白書," https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/pdf/01honpen.pdf, 2019.

[2] RL. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM 21.2 pp.120-126, 1978.

[3] B. Kaliski and J. Staddon, "PKCS# 1: RSA cryptography specifications version 2.0," RFC 2437, October, 1998.

[4] I. Blake, G. Seroussi and N. Smart, "Elliptic curves in cryptography," Vol. 265, Cambridge university press, 1999.

[5] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima and T. Tokita, "Camellia: A 128-bit block cipher suitable for multiple platforms—design andanalysis," International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2000.

[6] NIST-FIPS, "Announcing the advanced encryption standard (AES)," Federal Information Processing Standards Publication 197.1-51, pp.3-3, 2001.

[7] S. Kiyomoto, T. Tanaka, and K. Sakurai, "K2: A Stream Cipher Algorithm using Dynamic Feedback Control," SECRYPT, pp.204-213, 2007.

[8] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1996.

[9] S. Mangard, E. Oswald and T. Popp, "Power analysis attacks: Revealing the secrets of smart cards," Vol. 31. Springer Science & Business Media, 2008.

[10] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1999.

[11] B. Brier, C. Clavier and F. Olivier, "Correlation power analysis with a leakage model," International Workshop on Cryptographic Hardware and

Embedded Systems. Springer, Berlin, Heidelberg, 2004.

[12] JM. Schmidt and C. Herbst, "A practical fault attack on square and multiply," Proc. 5th Workshop on Fault Diagnosis and Tolerance in Cryptography, pp.53–58, Oct. 2008.

[13] N. Selmane, S. Guilley and JL Danger, "Practical setup time violation attacks on AES," 2008 Seventh European Dependable Computing Conference, IEEE, 2008.

[14] SP. Skorobogatov and RJ. Anderson, "Optical fault induction attacks," International workshop on cryptographic hardware and embedded systems. Springer, Berlin, Heidelberg, 2002.

[15] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall and C. Whelan, "The sorcerer's apprentice guide to fault attacks," Proceedings of the IEEE 94.2 pp.370-382, 2006.

[16] P. Maurine, "Techniques for em fault injection: equipments and experimental results," 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography. IEEE, 2012.

[17] T. Fukunaga and J. Takahashi, "Practical fault attack on a cryptographic lsi with iso/iec 18033-3 block ciphers," Proc. 6th Workshop on Fault Diagnosis and Tolerance in Cryptography , pp. 84–92, Sept. 2009.

[18] Y. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki and H. Sone, "Non-invasive EMI-based fault injection attack against cryptographic modules," 2011 IEEE International Symposium on Electromagnetic Compatibility. IEEE, 2011.

[19] D. Boneh, RA. Demillo and RJ. Lipton, "On the importance of checking cryptographic protocols for faults," International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 1997.

[20] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," Advances in Cryptology (Crypto ' 97), Lecture Notes in Computer Science Volume 1294, pp.513-525, Aug. 1997.

[21] J. Blomer and JP. Seifert, “Fault Based Crypt- analysis of the Advanced Encryption Standard (AES),” Financial Cryptography: 7th International Conf., (FC 2003), LNCS 2742, pp.162-181, Jan. 2003.

[22] G. Piret and JJ. Quisquater, “A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad,” Workshop on Crypto-graphic Hardware and Embedded Systems (CHES 2003), LNCS 2779, pp.77-88, Sep. 2003.

[23] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi and K. Ohta, "Fault sensitivity analysis," International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2010.

[24] T. Fuhr, E. Jaulmes, V. Lomne and A. Thillard, "Fault attacks on AES with faulty ciphertexts only," 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography. IEEE, 2013.

[25] Y Li, Y. Hayashi, A. Matsubara, N. Homma, T. Aoki, K. Ohta and K. Sakiyama, "Yet another fault-based leakage in non-uniform faulty ciphertexts," International Symposium on Foundations and Practice of Security. Springer, Cham, 2013.

[26] C. Dobraunig, M. Eichlseder, T. Korak, V. Lomne and F. Mendel, "Statistical fault attacks on nonce-based authenticated encryption schemes," International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2016.

[27] C. Dobraunig, M. Eichlseder, H. Gross, S. Mangard, F. Mendel and R. Primas, "Statistical ineffective fault attacks on masked aes with fault countermeasures," International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2018.

[28] C. Dobraunig, M. Eichlseder, T. Korak, S. Mangard, F. Mendel and R. Primas, "SIFA: exploiting ineffective fault inductions on symmetric cryptography," IACR Transactions on Cryptographic Hardware and Embedded Systems pp.547-572, 2018.

[29] LR. Marino, "General theory of metastable operation," IEEE Transactions on Computers 100.2 pp.107-115, 1981.

[30] L. Zussa, JM. Dutertre, J. Clediere, B. Robisson and A. Tria, "Investigation of timing constraints violation as a fault injection means," 27th Conference on Design of Circuits and Integrated Systems (DCIS), Avignon, France, 2012.

[31] 産業技術総合研究所, "サイドチャネル攻撃用標準評価基板 SASEBO-G 仕様書," http://satoh.cs.uec.ac.jp/SASEBO/pdf/SASEBO-G_Spec_Ver1.0_Japanese.pdf, 2008.

[32] 総務省, 経済産業省, "電子政府における調達のために参照すべき暗号のリスト (CRYPTREC 暗号リスト)," https://www.cryptrec.go.jp/list/cryptrec_ciphers_list_2016.pdf, 2013.

[33] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, “A Compact Rijndael Hardware Architecture with S-Box Optimization,” ASIACRYPT, pp.239–254, 2001.

[34] S. Morioka and A. Satoh, "An optimized S-Box circuit architecture for low power AES design," International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2002.

[35] Y. Hayashi, "Remote Fault-injection Method with Timing Control Based on Leaked Information," International Workshop on Security, IWSEC2013, Okinawa, 2013.

[36] TG. Malkin, FX. Standaert and M. Yung, "A comparative cost/security analysis of fault attack countermeasures," International Workshop on Fault Diagnosis and Tolerance in Cryptography. Springer, Berlin, Heidelberg, 2006.

[37] M. Doulcier-Verdier, JM. Dutertre, J. Fournier, JB. Rigud, B. Robisson and A. Tria, "A side-channel and fault-attack resistant AES circuit working on duplicated complemented values," 2011 IEEE International Solid-State Circuits Conference. IEEE, 2011.

[38] N. Selmane, S. Bhasin, S. Guilley, T. Graba and JL. Danger, "WDDL is

protected against setup time violation attacks," 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). IEEE, 2009.

[39] A. Nagao, Y. Okugawa, K. Takaya, Y. Hayashi, N. Homma and T. Aoki, “Detection method for overclocking by intentional electromagnetic interference,” IEEE International Symposium on Electromagnetic Compatibility (EMC), pp.241-245, 2015.

著者発表論文

1. 岡本拓実, 藤本大介, 林優一, 本間尚文, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, “ガウス雑音を用いた暗号機器への意図的な電磁妨害に対する耐性評価手法,”ハードウェアセキュリティ研究会，HWS2018-17，2018.7.25.
2. 岡本拓実, 藤本大介, 林優一, “電磁的非侵襲攻撃により生ずる誤り暗号文の統計的な性質に着目した秘密鍵解読法に関する研究,”ハードウェアセキュリティサマーセミナー, 2019.9.26.
3. 西山 輝, 岡本 拓実, 藤本 大介, 林 優一, "意図的な電磁妨害が IC 通信に与える影響に関する基礎検討," 環境電磁工学研究会 (EMCJ), EMCJ2019-23, pp. 29-33, 2019.7.18.
4. Hikaru Nishiyama, Takumi Okamoto, Youngwoo Kim, Daisuke Fujimoto, Yuichi Hayashi, "Fundamental Study on Influence of Intentional Electromagnetic Interference on IC Communication," 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits(EMC COMPO 2019), 1570580764, 2019.10.23.
5. 岡本拓実, 藤本大介, 崎山一男, 李 陽, 林優一, “順序回路への故障注入に起因した不均一な頻度分布を持つ誤り出力を用いた故障利用解析,”ハードウェアセキュリティ研究会，VLD2019-128 HWS2019-101，2020.3.6.