博士論文

真性乱数生成器の物理攻撃に対する乱数性評価に関する研究

大須賀 彩希

2022年03月17日

奈良先端科学技術大学院大学
先端科学技術研究科

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
博士 (工学) 授与の要件として提出した博士論文である。

大須賀 彩希

審査委員：

林 優一　教授　（主指導教員）
岡田 実　教授　（副指導教員）
中島 康彦 教授　（副指導教員）
藤本 大介 助教　（副指導教員）

真性乱数生成器の物理攻撃に対する乱数性評価に関する研究*

大須賀 彩希

内容梗概

情報通信技術の発展に伴い、IoT（Internet of Things）機器やスマートカードといったローエンドの端末からスマートホン、タブレット端末やラップトップPC等のハイエンド端末まで身の回りに数多くの機器が存在する状態となっている。これらの機器に対する情報セキュリティの確保は重要な課題となっている。セキュリティの基盤技術の一つとして、秘密鍵生成等に使用される乱数を生成する真性乱数生成器（TRNG: True Random Number Generator）が存在する。TRNGはランダムな物理現象を使用して乱数を生成し、この乱数によりセキュアな秘密鍵を作ることができる。オシレータを使用して乱数を生成するTRNGは、チップ上に安価に組み込めることからローエンドの機器に使用され、広く普及している。しかし、TRNGに脆弱性が生じた場合、秘密鍵の安全性が保障されなくなり、情報セキュリティに対する現実的な脅威となる。これまで、こうしたTRNGに対して外乱を与えることで乱数性を低下させる攻撃が提案されてきた。一方、セキュリティで使用される乱数が満たすべき性質である、一様性・再現不可能性・予測不可能性に対して物理攻撃が与える影響については十分に議論されていない。

本研究では、オシレータをエントロピー源として使用したTRNGに対して、一様性・再現不可能性・予測不可能性に対する物理攻撃による乱数性への影響を評価した。なかでも、電気的外乱を使用した物理攻撃は暗号モジュールに対して非侵襲かつ強力な攻撃手法として知られていることから、電気的外乱がTRNGに与える影響について評価を行った。一様性・再現不可能性の低下は、TRNGの出

*奈良先端科学技術大学院大学 先端科学技術研究科 博士論文, 2022年03月17日.

力の偏りや外乱による出力ビットの操作によって生ずる。このことから、TRNG に対する外乱の印加手法と印加した外乱による出力ビットの評価手法について提案した。実験により、TRNG のエントロピーを抑制する周波数を探索し、外乱を与えることで TRNG の出力ビットの一様性・再現不可能性が統計的に有意に低下することを示した。続いて、TRNG から生じる電磁放射から TRNG のエントロピーと TRNG の出力ビットを推定可能であるかについて評価を行った。これにより、出力ビットに依存した回路動作の変化を反映した電磁放射から TRNG の出力ビットを予測できる可能であることを示した。

以上の結果から、本研究は TRNG に対する物理攻撃による乱数性評価手法として、電気的な外乱の印加による一様性・再現不可能性への影響の評価手法、機器内部からの出力ビットを反映した情報漏えいによる予測不可能性への影響評価を提案し、電気的な外乱が TRNG に与える乱数性への影響の評価が可能であることを示した。

キーワード

真性乱数生成器, 安全性評価, 物理攻撃, 意図的電磁妨害, サイドチャネル攻撃

A Study on Randomness Evaluation for True Random Number Generators against Physical Attacks*

Saki Osuka

Abstract

With the development of information and communication technology, a device around the low-end terminals such as IoT device and smart cards has increased, and securing information security for these devices is an important issue. As one of the basic technologies of security, there is a true random number generator (TRNG) used for secret key generation. TRNG generates random physical phenomena and generates random numbers, which is secret information, and if this TRNG has vulnerable, it will be a realistic threat to security. Among them, TRNG that uses electrical noise to generate random numbers inexpensively incorporated into chips and is widely used for low-end devices and is widely used. Until now, attacks have been proposed to reduce randomness by giving disturbances to such TRNG. On the other hand, the impact of physical attacks has not been sufficiently discussed on each element of randomness such as uniformity, reproducibility and unpredictability.

In this study, we evaluated the security of uniformity, reproducibility and unpredictability for TRNG using oscillators as an entropy source. Among them, physical attacks using electrical disturbances are known as non-invasively and powerful attack methods for cryptographic modules, resulting in evaluation of

*Doctoral Dissertation, Graduate School of Science and Technology, Nara Institute of Science and Technology, March 17, 2022.

security to electrical disturbances even for TRNG. The decline in uniformity and reproducibility is caused by the bias of TRNG and the operation of the output bit due to disturbance. From this, we proposed the disturbance application method, and further proposed the evaluation method of the output bit by disturbance. In these experiments, they have shown that I could explore frequencies to suppress TRNG entropy and introduce disturbance wave non-invasively to reduce uniformity and reproducibility. Subsequently, for unpredictability evaluation was performed on whether the output bit of TRNG and its entropy can be estimated from the outside of the device. Experiments showed that random numbers can be predicted from electromagnetic radiation reflecting changes in circuit operation dependent on output bits.

This study has proposed an evaluation of randomness and entropy source evaluation method by application of electrical disturbances, evaluation method of entropy source, and output bits from inside the device, as a security evaluation method for TRNG. And, it showed that an electrical disturbance can evaluate the impact on the randomness given to TRNG.

Keywords:

True random number generator, security evaluation, physical attack, Intentional electromagnetic interference, Side-channel attack

目 次

図 目 次

表 目 次

1. 序論

1.1 研究の背景

近年の情報通信技術の発展に伴い、我々の身の回りにある電子機器数が急激に増加している。一人一人が PC や携帯電話に代表されるハイエンド機器から、スマートカード、IoT （Internet of Things）機器といったローエンド機器まで様々な種類の複数の機器を所有している。総務省が発表した令和二年度の情報通信白書 [1] によれば、世界の IoT デバイス数は今後も増加し続けることが予想されている。自動車などの産業用途の IoT デバイスに加えて、個人の健康を管理するウェアラブル端末、医療機器、各家庭内の家電機器に搭載される IoT 機器は今後も増加していくと考えられる。これらの電子機器は個人のプライバシー情報や電子商取引に関わる様々な機密情報を扱っており、情報セキュリティの確保が重要となっている。

最も重要な情報セキュリティの基盤技術として、暗号技術が挙げられる。公開鍵暗号や共通鍵暗号を用いた暗号技術が広く用いられており、これらの暗号技術により、情報セキュリティの三要素、すなわち、情報の機密性・完全性・可用性は担保されている。ここで、機密性、完全性、可用性は以下の様に定義される。

- 機密性（Confidentiality）: 権限のない第三者から情報の内容を隠すこと
- 完全性（Integrity）: 情報が破壊、改ざんまたは消去されていない状態を確保すること
- 可用性（Availability）: 権限があるものはいつでも情報及び関連資産にアクセスできる状態を確保すること

PC や携帯電話等の大量の機密情報を保持するハイエンド機器では、この情報セキュリティの三要素を満たすことが重要であることは言うまでもない。同様に、スマートカードや IoT 機器など、扱うデータ量やデータ処理の規模が小さいローエンドのデバイスにおいて、機密情報を扱う点でセキュリティの三要素は重要である。スマートカード内の暗証番号のような秘密情報の機密性の他にも、IoT 機

器が収集したデータ内に含まれる個人情報の機密性やビッグデータに使用されるデータの完全性が暗号技術によって担保されている。ここで用いられる暗号技術は専用ハードウェアや組込みマイコン上のソフトウェアとして、スマートカードや携帯電話、IoT 機器のような様々なデバイスに組込まれている。そのため、ハードウェア上に実装された暗号モジュールの脆弱性を評価することは情報セキュリティを保証する上で重要な課題の一つである [2, 3]。

情報セキュリティの基盤技術の一つに乱数生成器（RNG: Random Number Generator）が挙げられる。RNG が生成する乱数は秘密鍵生成やノンス、ソルト、ワンタイムパッド、初期化ベクトル、量子鍵配送といった暗号プロトコル中で使用される他にも、個人情報保護のための匿名加工や情報を秘匿したままデータ解析を行う秘匿計算プロトコル、情報を分散・暗号化することで一部の情報が流出しても元の情報を推測できないようにする秘密分散技術に使用され、極めて重要な役割を担っている。暗号プロトコル中で使用される乱数には (1) 一様性、(2) 再現不可能性、(3) 予測不可能性が求められている。一様性は、出力される乱数が一様分布に従い、一様にランダムな性質である。再現不可能性は、RNG に同じ入力をした際に、過去に生成した数列と完全に無関係なビット列が出力される性質である。予測不可能性はある出力を知った際に次の出力が予測できない性質である。これらの乱数性は情報セキュリティにおいて重要であり、乱数性の低下が情報セキュリティの三要素に与える影響として、いくつかの例が報告されている [4, 5, 6]。2008 年には Debian GNU/Linux およびその派生オペレーティングシステムに含まれる OpenSSL パッケージに予測不可能性の低い乱数が生成される脆弱性が発見され、ブルートフォース攻撃によって鍵情報が推測される可能性が報告されている [4]。また、2019 年には IoT デバイスの多くに、攻撃に対する脆弱性を持った弱いデジタル認証が使用されており、これは鍵生成時の RNG のエントロピーが不十分であった可能性が指摘されている [5]。2021 年にもセキュリティ企業の Bishop Fox から、IoT デバイスが使用するハードウェア RNG の脆弱性が指摘された [6]。ここでは、RNG を備えた IoT デバイスは乱数を適切に生成できておらず、十分なセキュリティを実現できていない可能性が指摘されており、脆弱性の影響を受けるデバイスは 350 億台に上ると推定されている。このように、

使用する乱数の品質にセキュリティレベルが左右されることから、予測困難な乱数の生成は暗号による情報セキュリティの三要素を担保するうえで必須の条件である。

RNGは、アルゴリズムによって擬似的な乱数を生成する擬似乱数生成器（PRNG: Pseudo Random Number Generator）と物理現象のランダム性を使用して乱数を生成する真性乱数生成器（TRNG: True Random Number Generator）の二つに大別される。PRNGは乱数の生成にシードによる初期値設定を必要とし、アルゴリズムによって乱数を生成する。そのため、同じシードとアルゴリズムを用いることで同じ乱数列を再現する。また、使用するアルゴリズムによっては、周期性を持つことや過去の出力またはPRNGの内部状態から後の乱数を予測可能などの特徴がある。一方、TRNGは物理現象のランダム性を使用して乱数を生成することから、再現性が低く予測困難な乱数となる。セキュリティ分野では、予測困難かつ再現性の低い乱数が求められることから、TRNGによる乱数生成が広く研究されている。

これまでに、様々な物理現象をエントロピー源として乱数を生成するTRNGが研究されてきた。ユーザーのマウス操作を利用するもの [13] や原子の放射線崩壊を専用のデバイスで観測するもの [7]、量子ビットを光学装置で計測することで乱数を生成する量子乱数生成器（QRNG: Quantum Random Number Generator）[8, 9, 10] など様々なものが存在する。また、決定論的法則であっても、乱雑な時間変化を示すカオス現象によって、初期状態のわずかな誤差から乱数を生成するカオス理論に基づくTRNG[11, 12, 25, 26] や、心電図や歩行データといった身体信号をエントロピー源として利用した研究も存在する [14]。オシレータを使用して乱数を生成するTRNGは古くから研究されているTRNGの一つである [15, 16, 17, 18, 19, 20, 21, 22, 23, 24]。このTRNGはオンチップで実装可能なことから安価に組込むことができ、ローエンドのデバイスも含めた様々なデバイスで広く利用されている。そのため、オシレータを使用したTRNGに対して脆弱性が存在した場合、セキュリティに対する現実的な脅威となり得る。このことから、本論文ではオシレータをエントロピー源として利用するTRNGに対するセキュリティ評価について検討を行う。以後、TRNGと表した場合、オシレータを

表 1.1: TRNG の分類

エントロピー源	特徴
ユーザーのマウス操作等	環境ノイズを使用した乱数生成 Unix 系 OS で使用される
半導体レーザー	乱数生成用の光集積回路が必要 高スループット
量子乱数生成器	光学装置による量子ビットの観測が必要 量子力学的に予測不可能 高スループット
原子の放射線崩壊	専用の装置で原子の放射線崩壊を観測 高スループット
身体信号	身体信号のランダム性を計測 低スループット
オシレータ	オンチップで実装可能（安価に組込むことができる） 低スループット 物理攻撃への脆弱性が知られている

使用したTRNGを指すものとする。

1.2 セキュリティにおけるTRNGの重要性と物理攻撃の可能性

従来のネットワークやアプリケーションへの攻撃とは異なる、ハードウェアの脆弱性を利用したサイドチャネル攻撃が近年大きな問題となっている [28]。暗号は計算量的に安全であることを前提にセキュリティを担保している一方、正規の入出力とは異なる非正規な入出力（サイドチャネル）を利用することで、暗号解読を可能とするサイドチャネル攻撃が示されている。既に、暗号回路の動作時に副次的に生じる情報（漏えい情報）を利用して暗号鍵の解読を行う攻撃が提案されている [28, 29, 30]。漏えい情報を使用した攻撃では、暗号回路が動作する際に生じる消費電力や放射電磁波、暗号の処理時間といった非正規な出力を観測し、解析することで暗号鍵の解読を行う。また、暗号回路の動作時に外乱を注入することで計算に誤りを誘発させ、誤りパターンから鍵解読を行うフォルト攻撃が提案されている [31, 32, 33, 34]。これらのハードウェアレベルの脆弱性は、ソフトウェアレベルでの対策だけでは不十分なことが多く、既存の製品に対してハードウェア上の脆弱性を修正することは難しい。そのため、脆弱性が発見された場合、セキュリティに対する重大な脅威となり得る。

サイドチャネル攻撃によるセキュリティの低下はTRNGに対しても影響を及ぼしている。前節で述べたようにTRNGが情報セキュリティの三要素を保証するには、一様性・再現不可能性・予測不可能性を満たす必要がある。既にTRNGが実装されたデバイスを冷却する攻撃や電源電圧を低下させる攻撃、電磁波を印加することでエントロピーを抑制する攻撃など、TRNGに対して外乱を与えることで乱数性を低下させる物理攻撃が提案されてきた [35, 36, 37, 38]。これらの研究はTRNGに対する攻撃の原理に着目したものであり、乱数の一様性についてのみ統計検定を行い、TRNGに対する物理攻撃の実現可能性を評価してきた。そのため、セキュリティにおけるTRNGの満たすべき性質である、一様性・再現不可能性・予測不可能性の各要素に対して、物理攻撃が与える影響については十分に議論されていない。

1.3 本研究の目的

セキュリティに使用される TRNG には、一様性・再現不可能性・予測不可能性について質の高い乱数を生成することが求められる。これまでに、セキュリティに使用される TRNG の実装手法について様々な研究がなされ、TRNG の設計指針としてアメリカ国立標準技術研究所（NIST: National Institute of Standards and Technology）やドイツ連邦政府情報セキュリティ庁（BSI: Bundesamt für Sicherheit in der Informationstechnik）が規格を発表している [39, 40]。この規格では、乱数性をオンラインで評価する Health test や乱数性を向上させる Post-processing の実装が推奨されている。これらの実装について、NIST の特別刊行物である SP 800-90 [39] では、いくつかの例は挙げられているものの決まった規格は存在せず、暗号機器のセキュリティレベルに応じてベンダが適宜設計を行っている。また、TRNG が生成した乱数は暗号プロトコル中で、暗号鍵生成を始めとしたさまざまな用途に使用される。TRNG に対する物理攻撃における安全性への影響を評価する場合、上述の Health test や Post-processing、暗号プロトコルにおける乱数の使用方法について、それぞれ評価を行う必要がある。

本研究では、オシレータをエントロピー源として使用した TRNG に対する物理攻撃への影響評価を目的とする。具体的には、セキュリティに使用される乱数の性質として重要な、一様性・再現不可能性・予測不可能性に対する物理攻撃の影響について評価を行う。暗号回路に対する非正規な入出力を使用したサイドチャネル攻撃では、電気的な外乱と機器から生じる非意図的な情報漏えいを使用することで鍵解読を行うことを目的としている。TRNG においても電気的外乱と情報漏えいを評価することで一様性・再現不可能性・予測不可能性の低下について評価可能であると考えられる。このことから、物理攻撃による各要素への影響を以下の様に評価する。

- 一様性の低下： 外乱によって出力ビットの分布が偏りや周期性、ビット間の相関をもつ
- 再現不可能性の低下： 特定の外乱を与えることで同じ出力ビットが再現する、または再現する可能性が増加する

- 予測不可能性の低下： 機器の動作に伴って生じる副次的な情報を機器外部から計測することで出力ビットを予測可能

上述の乱数性の各要素に対する物理攻撃を評価することができれば、物理攻撃に対する TRNG への安全性を評価することが可能であると考えられる。

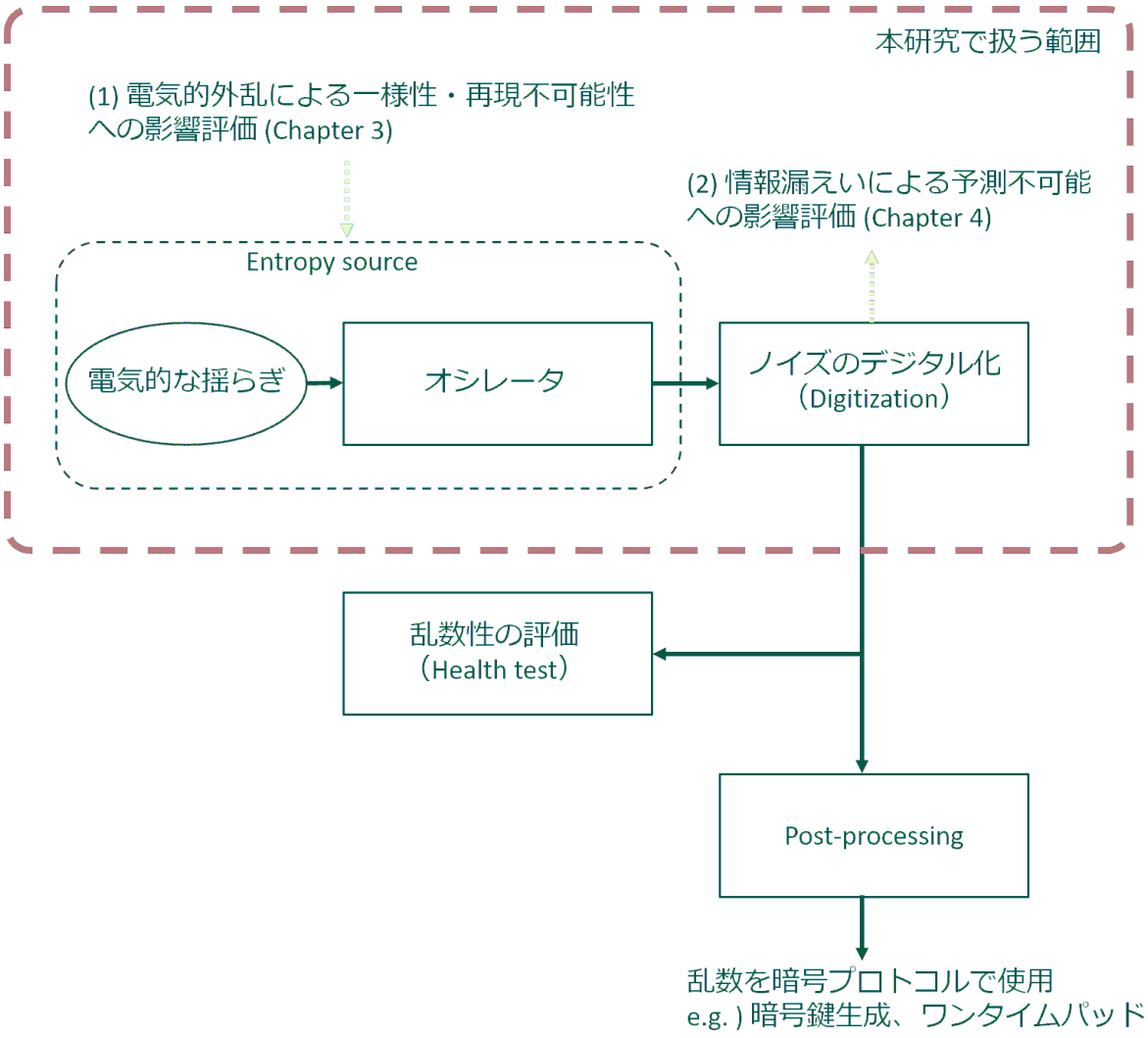


図 1.1: 本論文の構成

続いて、オシレータを使用した TRNG は図 1.1 のようにモデル化できる。乱数性を生み出す基となる電気的な揺らぎに対して、この揺らぎを抽出し、高い

エントロピーを生み出すために増幅するオシレータが必要となる。この電気的な揺らぎとノイズを増幅する回路をエントロピー源と呼ぶ。この増幅されたノイズはアナログノイズであり、乱数を生成するにはデジタル化を行う必要がある（Digitization）。このデジタル化された出力を TRNG の出力ビットとして扱う。このモデルに対して、一様性・再現不可能性・予測不可能性に対する低下が生じる箇所について述べる。まず、一様性が低下した場合、出力ビットに変化が生じ、偏りや周期性が変化する。出力ビットの乱数性は電気的揺らぎの質とその揺らぎの蓄積によって変化する。TRNG への物理攻撃として、エントロピー源に対する外乱による電気的揺らぎの質の低下やノイズの蓄積の抑制が検討されていることから、TRNG に対する外乱の印加手法と外乱による出力ビットへの影響を評価することができれば、一様性に対する物理攻撃への評価が実現可能である。続いて、再現不可能性に対しては、一様性と同様に出力ビットを操作し、同じ出力ビットを再現させる、または再現性を上げることが考えられる。このことから、一様性に対する評価と同様に、再現性に対してもエントロピー源に対する外乱への評価を行うことで物理攻撃に対する再現不可能性の評価が可能であると考えられる。最後に、予測不可能性への評価について述べる。予測不可能性では TRNG から生じる情報漏えいによって出力ビットを推定可能であるかについて評価を行う。情報漏えいが生じるモジュールとしてエントロピー源と Digitization が存在する。エントロピー源では、出力ビットの情報はアナログ信号として扱われている。アナログ信号に対して出力ビットが推定可能かを評価する場合、確率的に評価する必要があり、出力ビットの推定は難しいと考えられる。一方、Digitization では出力ビットはデジタル信号として処理されることから、アナログ信号に比べて、出力ビットとデジタル信号に明確な対応関係があり、推定は容易であると考えられる。このことから、Digitization における情報漏えいの可能性を評価し、出力ビットの推定が可能であるかを評価することができれば、物理攻撃に対する予測不可能性への影響を評価することが可能であると考えられる。

このことから、TRNG への物理攻撃に対する乱数性への影響として、 (1) 電気的外乱による一様性・再現不可能性への影響評価と (2) 漏えい情報による予測不可能性への影響評価を行うことで、TRNG の物理攻撃に対する乱数性への影響評

価を行うことが可能であると考えられる。

1.4 本論文の流れ

本論文の構成は以下のとおりである。

2 章では、TRNG の概要と暗号モジュールに対する物理攻撃について基礎的な概要を述べ、電気的外乱を使用した物理攻撃に対して TRNG のセキュリティ評価を行うことを述べる。

3 章では、実際に電気的外乱を使用した物理攻撃に対して TRNG の一様性・再現不可能性への影響評価を行う。電気的外乱による TRNG のエントロピー源への影響の評価を行うために、機器外部から非侵襲に電気的外乱を与えることが可能であることと、電気的外乱はエントロピー源に対して、時間方向に高い分解能で影響を与えることが可能であることから、一様性・再現不可能性が低下する可能性があることを実証する。

4 章では、情報漏えいによる予測不可能への影響評価を行う。エントロピー源に対する物理攻撃によるエントロピーの低下を評価する技術について検討を行う。実際に、APD 測定によって、周波数領域においてエントロピーを評価できる可能性について示す。また、機器外部から出力ビットに応じた回路動作の変化を取得することで乱数ビットが漏えいする可能性について評価を行う。

5 章では、まとめを行う。

2. TRNGに対するサイドチャネル攻撃とその原理

2.1 緒言

1章では、TRNGに対する物理攻撃の可能性と、その影響評価が不十分であることを指摘した。本章では、2.2節で暗号モジュールに対する物理攻撃を述べたのちに、暗号モジュールに対する電気的外乱を使用した物理攻撃について述べる。続いて、2.3節でTRNGに対するセキュリティ基準を述べ、オシレータを使用したTRNGについて概説する。最後に、2.4節では、TRNGに対する電磁的外乱を使用した物理攻撃について概説する。

2.2 サイドチャネル攻撃の原理

本節では、暗号技術を実装した暗号モジュールに対する物理攻撃手法について、分類及び概説を行う。

暗号モジュールはソフトウェア実装とハードウェア実装に大別される。ソフトウェア実装は汎用プロセッサ上で動作するプログラムにより暗号処理を行う。一方、ハードウェア実装は専用LSI（Application Specific Integrated Circuit: ASIC）や、Field Programmable Gate Array （FPGA）上の回路により暗号処理を行う。ソフトウェア実装はプログラムの書き換えにより機能の修正や拡張、脆弱性へのアップデートを行うことができる。しかし、汎用プロセッサの既存の命令セットを用いて暗号処理をプログラムする必要があることから、処理速度や消費電力は大きくなる。一方、ハードウェア実装では、機能修正や拡張アップデートが困難であるが暗号実装に適したアーキテクチャを使用することで、高速かつ低消費電力で暗号処理を実現可能である。

ソフトウェア実装、ハードウェア実装のいずれも、その構成要素であるTRNGはASICやFPGAといったハードウェア上に実装し、オシレータが生ずるランダムなノイズを使用することで真の乱数を生成する。このことから、どのような実装であってもハードウェアに対する物理攻撃による影響を受けることになる。以下では、ハードウェア実装された暗号モジュールに対する物理攻撃手法について

概説を行う。

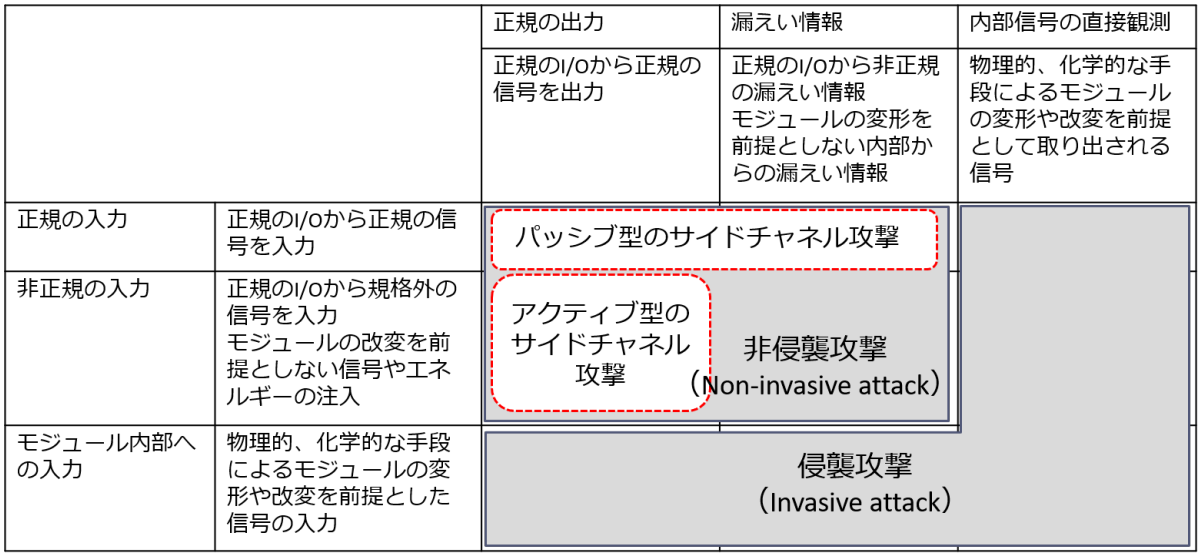


図 2.1: 物理攻撃の分類（文献 [2] の表および図 1.2 を文献 [3] を参考にして加工）

暗号モジュールに対する物理攻撃では、攻撃者が暗号モジュールに対して、非正規な入出力を行うことで、秘密情報の抽出を行う。この非正規な入出力として、チップの開封を伴う内部信号の観測や暗号処理時の消費電力や漏えい電磁波の観測があげられる。図 2.1 に、物理攻撃の分類を示す。まず、大きな分類として対象の暗号モジュールへの開封や改変を伴う侵襲攻撃（Invasive attack）とそれらを伴わない非侵襲攻撃（Non-invasive attack）に分けられる。侵襲攻撃は、暗号モジュールに対して、IC（Integrated Circuit）チップのパッケージを開封したり、回路の一部を破壊したりする攻撃である。この攻撃は暗号アルゴリズムを実装した回路に直接アクセスすることが可能なため、高い攻撃能力を持つ一方、攻撃のコストが高く、攻撃の痕跡を残すといった特徴がある。一方、非侵襲型攻撃は暗号モジュールの改変を伴うことなく、正規または非正規な入出力を使用して、秘密情報の解読を行う攻撃である。非侵襲攻撃は侵襲攻撃と比べて、検知が困難かつ安価に実現可能であるため、現実的な脅威として注目されている。非侵襲攻撃は、パッシブ型の攻撃とアクティブ型の攻撃、これらを組み合わせた攻撃に分けられる。本稿では、アクティブ型の攻撃のことをフォルト攻撃（Fault injection attack）と呼ぶ。

2.2.1 パッシブ型のサイドチャネル攻撃

パッシブ型のサイドチャネル攻撃では、暗号処理時に副次的に生じる情報を利用して秘密情報の解読を行う。サイドチャネル攻撃の代表的な研究として、Kocherらによる暗号処理時の消費電力波形を使用して秘密鍵の解読を行うSimple Power Analysis（SPA）やDifferential Power Analysis（DPA）[28, 29]が存在する。これらの攻撃は暗号モジュール内部のCMOS（complementary metal-oxide semiconductor）のスイッチングによって発生する過渡電流により消費電力が増加することを利用し、この消費電力の増加が暗号モジュール内部の処理と同期していることから、秘密鍵の解読を実現している。Kocherらの研究ののち、多くの研究者がこの問題に取り組み、現在では様々な暗号の解析手法が提案されている。代表的な例としては、タイミング解析（演算処理の時間差を利用）、電力解析（演算処理中の消費電力を利用）、電磁波解析（漏えい電磁波を利用）があげられる。なかでも、電磁波を利用したサイドチャネル攻撃では、機器遠方から非侵襲に秘密情報の解読が可能なことが示されており[30]、物理的なアクセスが困難な環境下においても攻撃が実現する可能性がある。

2.2.2 フォルト攻撃

故障注入攻撃は、暗号モジュールに対して機器の動作や計算の途中に非正規な入出力を行うことで暗号処理を誤らせることで秘密情報を入手する攻撃手法である。故障注入攻撃は、1996年に提案され、CRT（Chinese Remainder Theorem）を用いたRSA暗号に対するものが最初[44]であり、暗号アルゴリズムの出力に影響を与えることで、正しい出力値とエラー出力値を比較・解析する差分故障解析が提案された[33]。機器に対する故障の注入手法としては、クロック端子や電子端子から異常な信号を物理的に入力する手法や電磁波照射によって、意図的に計算処理を誤らせる手法が存在する。故障注入攻撃は、攻撃の検知に関してはパッシブ型のサイドチャネル攻撃と比べて容易であるが、少ない試行回数で秘密情報の解読が可能であり、強力な攻撃手法として知られている。また、近年では電源ケーブルを介して電磁波を印加する攻撃手法も提案されており[30, 34]、機器に

対する物理的なアクセスや機器についての詳細な知識がなくても攻撃が実現できる可能性が示されている。

2.3 TRNG の概要

アルゴリズムによって決定論的に乱数を生成する PRNG やランダムな物理現象を使用して乱数を生成する TRNG は、質の高い乱数を生み出すために、様々な研究や評価手法が検討されてきた。従来の RNG の評価手法は出力ビット列に対して、複数の統計検定を行うことで、乱数性を評価していた。NIST の特別刊行物である SP 800-22 [41] では、出力ビットの偏りから、周期性、連続した乱数ビットの出現ビットといった様々な項目に対して 16 の統計検定を行う統計的テストスイートを提供している。また、他にも FIPS PUS 140-2[42] や DIEHARD[43] といった複数の統計的テストツールが公開され、乱数性の評価に使用されてきた。これらの統計検定ツールは出力ビットに対して偏りや周期性といったどのような乱数性が低いのかを合格・不合格によって評価するものである。しかし、これらのテストは、テストしたビット列に対して統計的に乱数化を評価するものであり、PRNG のように決定論的に生成された乱数と真の乱数を識別することはできない。また、周期性などの乱数性低下が検出された TRNG に対して後処理を行うことで、検定を合格させることも可能であり、TRNG に対して真の乱数であるかについて適切な評価を行うことは難しい。更には、PRNG と異なり、TRNG は動作する環境や実装手法、プロセスの変化にも影響を受ける可能性がある。そのため、テスト環境で生成した乱数ビットが統計的に乱数性を示していたとしても、実際の動作環境での乱数性を保証するものではない。このことから、現在では、TRNG はセキュリティ上の重要性のため、産業で使用される過程でより厳しい評価・認証を受けている。TRNG の設計者は、統計的に優れた乱数を生成可能な回路設計を行うだけではなく、TRNG の予測不可能性を示す信頼性の高い検証可能な証拠を提供することが求められている。例えば、NIST の SP 800 90-B[39] では、TRNG の設計及び評価に関する要件が記載されており、エントロピー源の予測不可能な動作についての理論的な根拠が求められる他、生成された出力ビットの最小エントロピーの推定や、乱数性を評価するオンラインテストの実装が勧告

されている。また、BSI の規格である AIS-20/31 [40] と呼ばれる RNG のセキュリティ評価の Proporsal は、TRNG の設計・評価におけるヨーロッパのデファクトスタンダードとなっており、この文書では、提案する TRNG の予測不可能性を証明するためにエントロピー源の確率モデルを必要としている。

続いて、TRNG の基本的な構成について述べる。オシレータを使用した TRNG は、熱揺らぎ（Thermal noise）、$1/f$ ゆらぎ（Flicker noise）、ショットノイズ（Shot noise）と呼ばれる回路ノイズを使用して乱数を生成する。これらのノイズをオシレータのジッタとして扱うことで乱数を生成する。ジッタとは、オシレータの遷移タイミングの揺らぎであり、発振を繰り返すごとに図 2.2 のようにジッタが蓄積する。ジッタの蓄積によって、回路ノイズから乱数を生成するのに十分なエントロピーを抽出可能である。オシレータベースの TRNG はオシレータとサンプリングを行う回路のみで構成可能なことから、広く研究されている TRNG の一つである [15, 16, 17, 18, 19, 21, 22]。オシレータとして、複数のインバータを使用したフリーランニングのオシレータや PLL（Phase-locked loops）が一般的に用いられている。

TRNG のエントロピーはオシレータによってジッタとして表されるアナログ信号であり、このアナログ信号をデジタル信号へと処理する（Digitization）ことで、ランダムな出力ビットを生成する。この出力ビットに対して、乱数性をオンラインで評価する Health test と乱数性を向上させるための Post-processing の実装が推奨されている。エントロピー源は真のランダム性を提供する一方、出力された乱数ビットは通常、様々な理由で偏っており、一様に分布していない。そのため、Post-processing を行うことで、乱数列の相関の低減や、出力を一様に分布させる。

以下に、オシレータを使用した TRNG の代表的な実装と動作について概説する。

2.3.1 RO-based TRNG の実装と動作原理

オシレータベースの TRNG はジッタが蓄積するのに従って、エントロピーが増大するため、十分なエントロピーをもった出力ビットを生成するには時間がかかり、スループットの改善が課題の一つである。このことから、より効率よくジッ

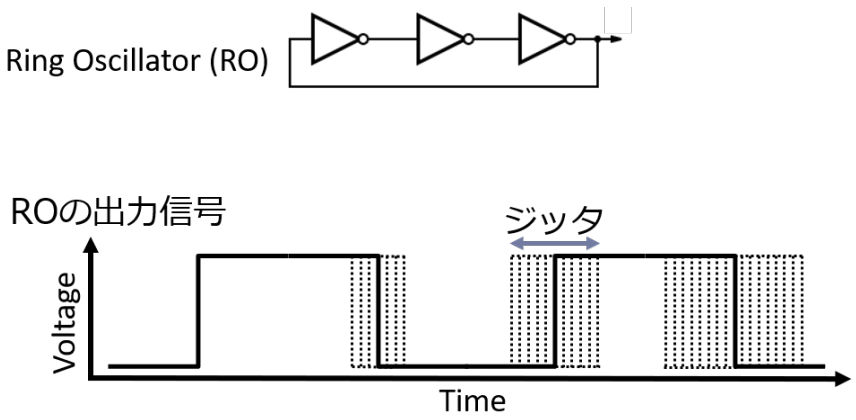


図 2.2: ジッタの蓄積のイメージ

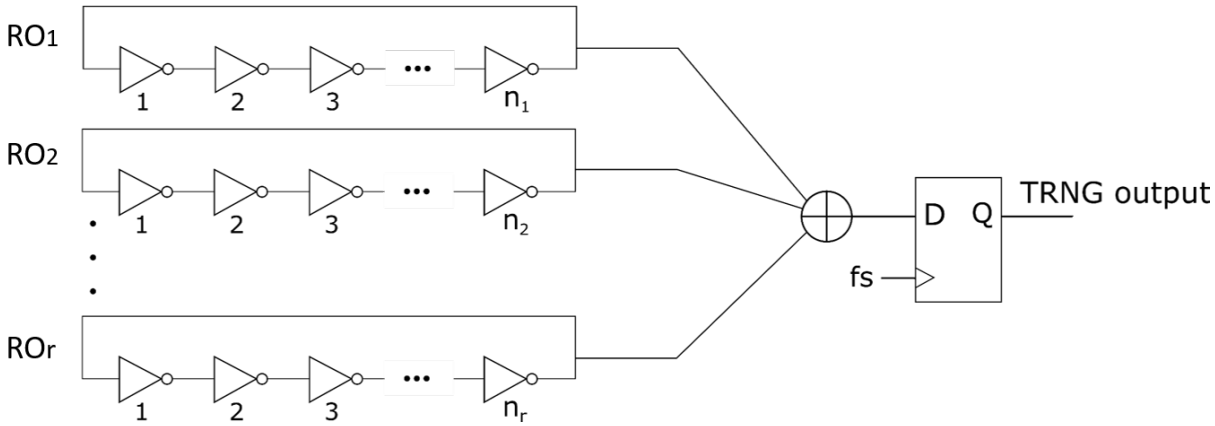
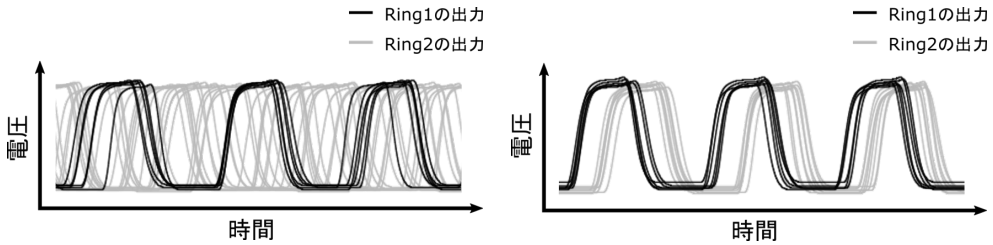


図 2.3: RO-based TRNG の基本構成



(a) 高エントロピー時　　(b) 低エントロピー時

図 2.4: エントロピーの変化による RO の出力信号の変化

タを蓄積するために複数のオシレータを使用する TRNG が Sunar らによって提案された RO-based TRNG である [15]。図 2.3 に RO-based TRNG の基本構成を示す。この RO-based TRNG は任意の r 個の RO と XOR、D flip-flop によって構成される。ここで、$k(=1, ..., r)$ 番目の RO は、n_k 個のインバータ（n_k は奇数）をリング状に接続することで構成されている。この TRNG では、各 RO の出力を XOR によって集約し、発振周波数とは異なる任意の周期 f_s でサンプリングすることで 1 ビットを生成する。

TRNG が生成するビット列の乱数性は RO のランダムノイズであるジッタによって生じる。ジッタは時間領域では RO の遷移タイミングの変動として現れ、RO を発振周波数からわずかに変化したタイミングで遷移させる。蓄積したジッタは各 RO の遷移タイミングを大きくばらつかせるため、図 2.4(a) のように出力にゆらぎが生じる。このゆらぎによって、各 RO の出力が他の RO に依存しないランダムな値をとるため、全 RO の出力の排他的論理和はランダムになる。この TRNG は複数の同じ長さのオシレータを組み合わせて、発振器の出力を XOR したのち、D flip-flop を用いてサンプリングすることで乱数を生成する。複数の RO を使用することで、それぞれの RO がジッタを蓄積することから、RO の段数が増えるほどスループットが向上する。

2.3.2 Elementary RO-based TRNG の実装と動作原理

Baudet らによって提案された Elementary RO-based TRNG (ERO-TRNG) は、高周波のオシレータを低周波のオシレータが D flip-flop を用いてサンプリングすることで乱数を生成する TRNG である。ERO-TRNG は同じ長さの 2 つの RO から構成される TRNG であり、RO をエントロピー源とする TRNG の中で回路の構成要素が最も少なく、基本的なモデルとして考えられる。図 2.5 に ERO-TRNG の基本構成を示す。この TRNG は n 個のインバータ（n は奇数）をリング状に接続した 2 つの RO と分周器、D flip-flop によって構成される [45, 27]。RO_2 は非同期カウンタ等によって、任意の周波数に分周され、RO_1 に比べて、低周波となる。この低周波数のクロックによって、高周波の RO_1 をサンプリングすることで乱数を生成する。低周波のクロックの立ち上がりまでに、RO_1 のジッタが蓄積さ

れ、遷移タイミングがランダムに変動することがエントロピー源となる。

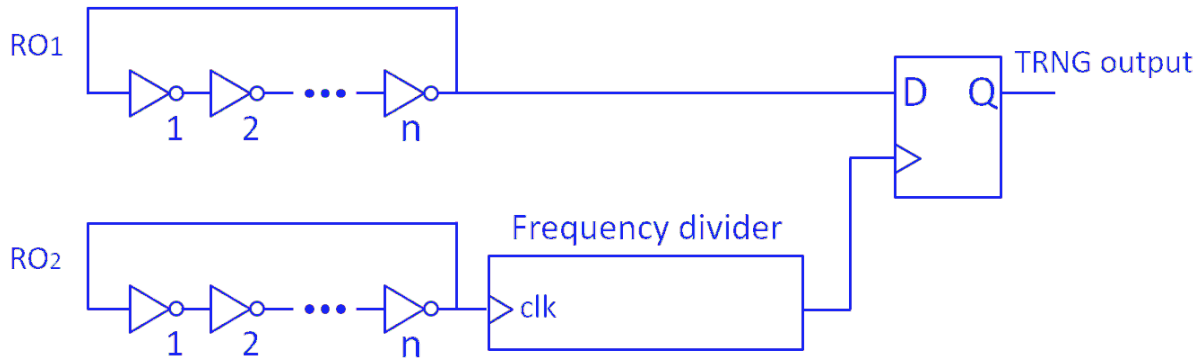


図 2.5: ERO-TRNG の基本構成

2.3.3 TERO-based TRNG の実装と動作原理

Transition Effect Ring Oscillator (TERO) based TRNG は Varchola らによって基本的な原理の提案 [19] がされた。この TRNG は、TERO と呼ばれる RS ラッチ回路のような回路構造をエントロピー源として利用し、回路の一時的な発振をカウントすることで乱数を生成する（図 2.6）。TERO は偶数個のインバータまたはバッファーと発振を制御するための二つの NAND ゲートから構成される [45]。二つの NAND ゲートに制御用の信号 V_{ctrl} が入力されることで、V_{out1} と V_{out2} は同時に発振を開始し、振動を続ける準安定状態に遷移する（図 2.7）。そして、ノイズや配線長のわずかな差によって次第に平衡状態からのずれが生じ、V_{out1} と V_{out2} のエッジが衝突することで振動を停止する。このとき、各エッジの変化はデジタル信号として変化するが、片方のエッジがもう一方のエッジに追いつくことによって、CMOS スイッチの充放電が十分に行われないため、図 2.7(a) の様にアナログ信号のような変化が観測される。この振動停止までの時間はノイズに影響されるため、発振時の振動回数はランダムとなる。この振動回数を T flip-flop でカウントし、TERO が安定状態となった後の T flip-flop の出力によって、1 ビットの乱数を生成する。TERO の振動が安定した後の T flip-flop の出力が Low であれば、出力ビットは 0 となり、High であれば出力ビットは 1 となる。TERO が生成

する出力ビットが高いエントロピーを持つには、V_{ctrl} の立下りまでに TERO が発振を終え、安定状態に遷移する必要がある。振動回数をカウントする T flip-flop は 1 ビットの乱数生成ごとにリセットする実装が一般的である [45]。この信号はクロックから生成され、TERO の発振開始から一定時間後に T flip-flop がリセットされる。

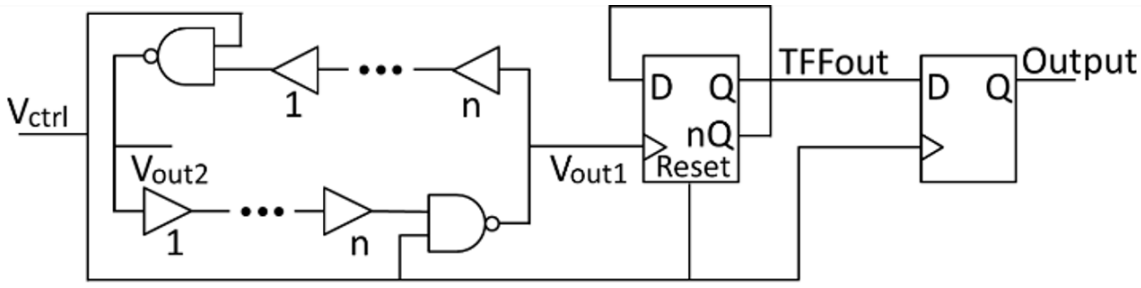
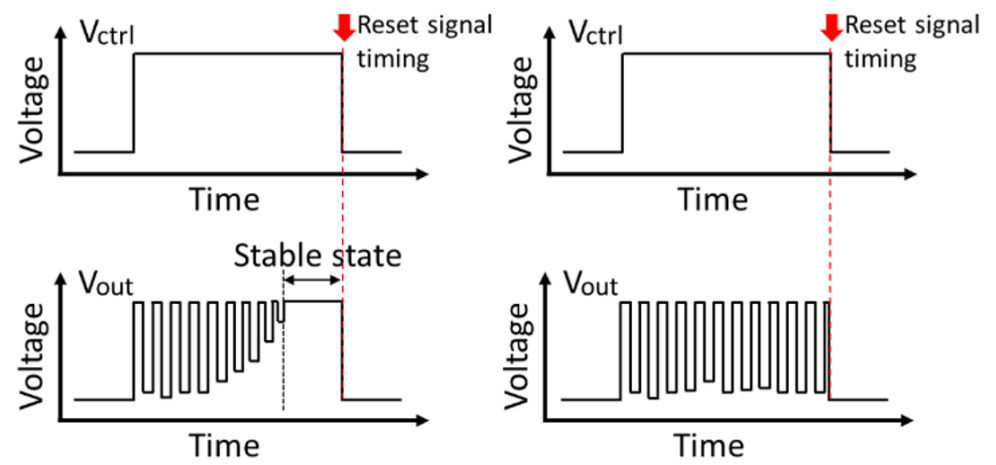


図 2.6: TERO-based TRNG の基本構成

2.4 TRNG に対する物理攻撃

本節では、TRNG に対する物理攻撃について概説する。

TRNG に対する物理攻撃として、エントロピー源に外乱を与えることでエントロピーを抑制する物理攻撃が知られている。2.3 節で述べたように、TRNG は電気的揺らぎをオシレータによって増幅してエントロピー源として扱うことでランダム性の高い乱数を生成している。しかし、この電気的揺らぎはプロセスやデバイスの設置環境や動作環境の影響を受けやすいことが知られている。TRNG の設計時にはこれらの影響を受けにくい設計や出力ビットを評価する Health test や乱数性を改善する Post-processing が実装されている。一方、TRNG に対して意図的に外乱を与えることで乱数性を低下させる物理攻撃についても検討されている。これまでに提案されてきた物理攻撃として電源電圧を操作することで電気的揺らぎを減少させる攻撃や、デバイスを直接冷却することで熱揺らぎといったエントロピーを抑制する攻撃手法が提案されてきた [35, 36, 37, 38]。特に、電気的外乱を使用した物理攻撃は電気的揺らぎを時間方向で高い分解能を持って操作できる可能性があり、Health test といったモジュールによる対策を無効化する可能



(a) 高エントロピー時　　(b) 低エントロピー時

図 2.7: TERO の出力波形の変化

性がある。また、2.2 節で述べたように、暗号モジュールに対する物理攻撃手法として電気的外乱を使用した物理攻撃は、非侵襲で実現できる可能性や攻撃が比較的安価に行うことが可能なため、セキュリティに対する現実的な脅威として注目されている。このことから、本研究では、TRNG に対する電気的外乱を使用した物理攻撃について評価を行う。

TRNG に対する電気的外乱を使用した物理攻撃の一例として、2009 年に Markettos と Moore が提案した、オシレータベースの TRNG に対する周波数注入攻撃が存在する [35]。2.3 節で述べたように、オシレータベースの TRNG は遷移タイミングの揺らぎであるジッタをエントロピー源として利用することで乱数を生成する。このオシレータは、振り子の共振現象のようにある発振器が他の発振器が生成した信号に引き込まれる現象を利用する [46, 47, 48]。TRNG に使用される RO はジッタをエントロピー源とすることから、外乱によってジッタの少ない信号の周波数や位相に引き込まれる（ロックされる）ことで乱数性が低下する。そのため、攻撃者によって印加された正弦波によって RO の発振がロックされた場合、オシレータはジッタの少ない出力波形となるため、乱数性は大きく低下する。図 2.4(b) は各 RO のジッタが注入した正弦波信号のジッタにロックされ、RO 間のジッタが同期し、エントロピーが低下したイメージを示す。ジッタの同期は各

RO の遷移タイミングのばらつきを抑制するため、RO 間のゆらぎが大きく減少する。ゆらぎの減少により各 RO の出力は他の RO と関連性の高い出力となるため、RO の出力パターンが減少し、TRNG の乱数性は低下する。[35] では、あるスマートカードに対して周波数注入攻撃を行うことで 2^{32} の乱数ビットのパターンを 2^8 まで低下可能であることを示しており、TRNG に対する周波数注入攻撃による乱数性低下はセキュリティに対して大きな脅威となり得る。

2.5 結言

本章では、暗号モジュールに対する物理攻撃に対して分類と説明を行い、電気的外乱によるセキュリティへの安全評価の重要性を述べた。次に、TRNG の実装と物理攻撃に対して基礎的な説明を行った。まず、TRNG の実装について NIST や BSI が提供する設計要件を述べたのちに、オシレータを使用した TRNG に対して基礎的な概要と実装例について説明を行った。最後に、本論文で主に取り扱う TRNG に対する物理攻撃について述べ、電気的外乱を使用した TRNG の乱数性評価の重要性について述べた。

3. オシレータベースのTRNGに対する電気的外乱を利用した物理攻撃への一様性と再現不可能性への評価

3.1 緒言

本章では、TRNG に対する電気的外乱を利用した物理攻撃に対する影響評価を行う。TRNG の乱数性評価として、物理攻撃に対する一様性・再現不可能性への影響について評価を行った。一様性・再現不可能性の低下では、出力ビットの偏りや攻撃による出力ビットの再現性が生じることから、エントロピー源に対して電気的外乱を行うことで、TRNG のエントロピーが抑制可能かについて評価を行った。まず、3.2 節で非侵襲な電気的外乱による一様性低下の実現可能性を評価した。その後、3.3 節で電気的外乱による出力ビットの評価を行い、再現不可能性と一様性の低下を実証した。

3.2 非侵襲な電磁波印加手法の評価

本節では、オシレータベースの TRNG に対する物理攻撃手法の一つである周波数注入攻撃によって、非侵襲に TRNG に電気的外乱を与えることで一様性の低下が実現可能かについて評価を行った。

Markettos と Moore が提案した周波数注入攻撃 [35] は RO-based TRNG に接続された電源線に直接、正弦波電流を印加することで乱数性のソースとなるジッタを抑制し、TRNG の乱数性を低下させる。その後、文献 [36, 37] において、回路近傍からの電磁波注入によっても TRNG の乱数性を低下させる攻撃が可能であることが示されている。これらの手法は、モジュールのごく近傍での操作やモジュールが実装されている機器への改変・侵襲を必要としており、対象となる機器への物理的な接近や改変が前提となっている。これに対して、暗号機器にはモジュールが筐体で覆われたものや、改変を検知する機構が備わっているものといったモジュールへの物理的な接近や改変を困難にする耐タンパー性を備えているものも少なくない。更には、物理的なアクセスが困難な場所に機器が設置されている場合もあり、このような状況においては既存の攻撃手法を適用することは難しい。

これに対し、本節では TRNG 近傍へのアクセスが困難な状況においても乱数性を低下させる攻撃の可能性について検討を行う。具体的には、TRNG が実装された機器に接続された電源ケーブルやコミュニケーションケーブルなどの接続線路を通じて機器の遠方から電磁波の周波数を変化させながら印加する。それと同時に TRNG の動作時に生ずるサイドチャネル情報を遠方で計測し、乱数性のソースとなるジッタの変動パターンを観測することで、遠方から TRNG の乱数性が低下したか否かを判定する。

また、提案手法が成立した場合、物理的な接近が困難であり、かつ、実装などを自由に操作・改変する事ができない乱数生成器も周波数注入攻撃の対象となることから、これまで攻撃対象外とされてきた機器においても対策を講ずる必要があると考えられる。

3.2.1 遠方からの周波数注入攻撃手法

周波数注入攻撃により TRNG の乱数性を低下させるためには、乱数性のソースとなるジッタを抑制可能な周波数 (ここでは f_{inj1} とする) を選択して注入する必要がある [35]。この周波数は解析的に求めることが困難なため、従来は RO の動作や TRNG の生成するビット列を直に観測して f_{inj1} を探索した。しかし、遠方から非侵襲に攻撃を行う場合、RO の動作や TRNG の出力を観測することは困難なため、f_{inj1} を求めることは容易ではない。また、実デバイスへの攻撃を考えた際、RO の動作は個々のインバータの製造ばらつきによって決定されるため、f_{inj1} は個体依存になる可能性が高い。そのため、対象となるデバイスを事前に入手し、f_{inj1} をプロファイリングして攻撃に適用することも難しいと考えられる。このことから、遠隔で攻撃を行うには遠方で得られる情報から TRNG の乱数性を推定する手法が必要となる。TRNG の乱数性が低下する際には RO の動作に何らかの変化が生ずると考えられるため、その変化が機器外部から取得できれば、乱数性を低下させる周波数を推定できる可能性がある。

そこで本節では、図 3.1 に示す様に、乱数生成器の動作時に生ずるサイドチャネル情報を遠方で計測することで機器内部の RO の動作の変化を計測しつつ、機器に接続された電源ケーブルやコミュニケーションケーブルなどの接続線路を通

じて特定の周波数で電磁波を印加することで、乱数性の低下が実現可能であるかについて評価を行う。

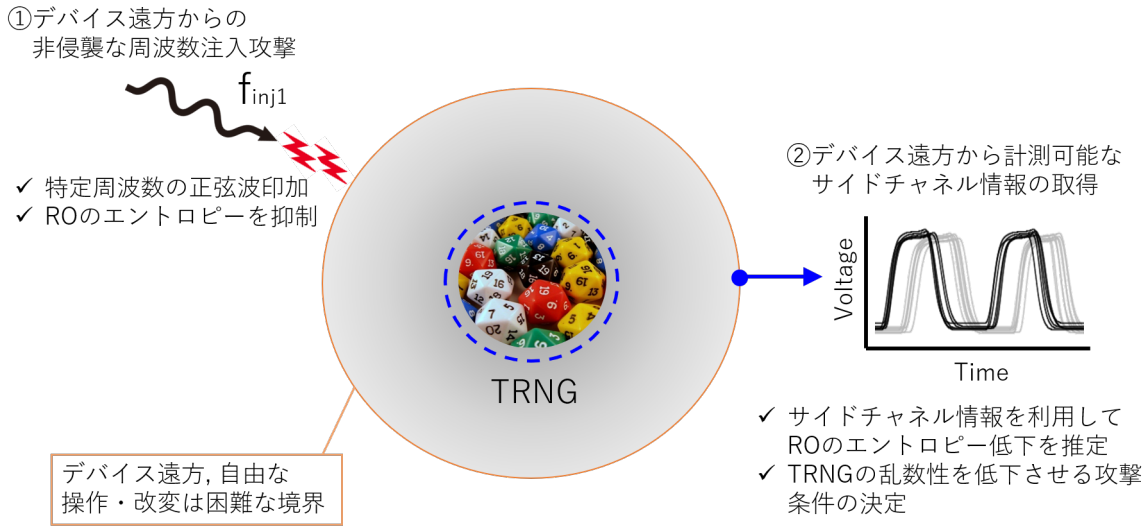


図 3.1: 非侵襲な周波数注入攻撃のイメージ

3.2.2 RO の内部状態に依存したコモンモード電流の観測

攻撃対象の RO の内部状態を非侵襲に観測可能なサイドチャネル情報について概説し、TRNG の乱数性を推定する手法について検討を行う。以下では、RO の内部状態の情報を含んだコモンモード電流を機器外部で観測できる原理を概説し、乱数性の低下した TRNG の推定手法の概要について述べる。

環境電磁工学（Electro Magnetic Compatibility）の分野において、非意図的な情報漏えいが機器の内部処理を反映したコモンモード電流によって起きることが知られている [49, 50, 51, 52]。機器の内部状態の変化によって生じた過渡電流は回路内部に存在するインダクタンスによって交流電圧源へと変換される。この電圧変動は共通のグランドを介してコモンモード電流として電源ケーブルといった周辺回路に伝導・放射する。文献 [30] では、電源ケーブル上から電磁波解析攻撃にも使用可能なほど暗号モジュールの内部処理と関連性の高いコモンモード電流が観測されることが報告されている。そのため、RO の内部状態も同様の原理

によってコモンモード電流を生じることが予想されるため、電源ケーブル上からROの内部状態と関連性がある情報を取得できる可能性が高い。

図3.2に本節で提案する手法の概要を示す。まず、TRNGを含むデバイスに対して、電源ケーブルにクランプしたインジェクションプローブから周波数f_{inj1}の連続的な正弦波を印加する。続いて、同じく電源ケーブルにクランプしたカレントプローブを用いてコモンモード電流を計測する。この時、ROのロックによる内部状態の変化（図2.4）に関連する情報をコモンモード電流から取得できれば、乱数性の低下を推定することが可能となる。

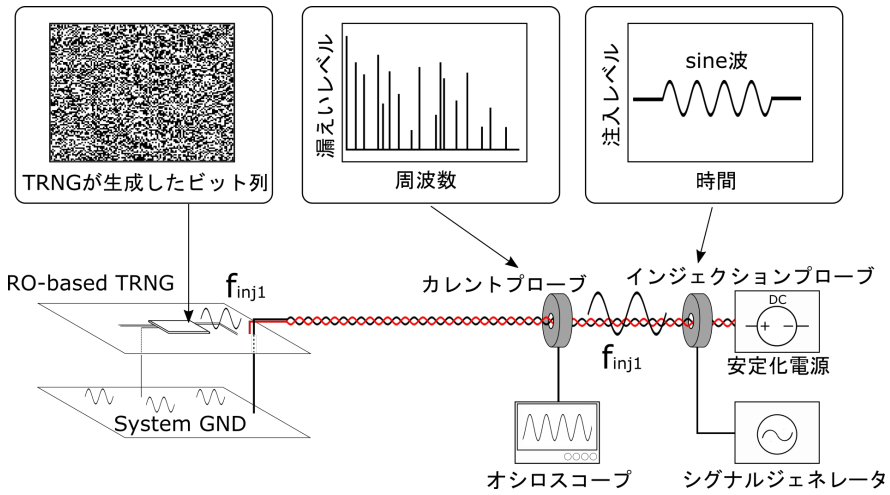


図 3.2: 遠方からのRO-based TRNGに対する周波数注入攻撃のイメージ

3.2.3 実験

電気的外乱の印加に用いるインジェクションプローブは、電子機器の外来電磁波に対する耐性試験（イミュニティ試験）において電子機器が妨害波の影響を受けやすい状況を模擬する試験として一般に用いられるものである。具体的な使用方法としては、機器に接続された線路をインジェクションプローブによってクランプし、プローブと線路間の電磁結合を用いて妨害波を線路に対して印加する。本実験では、サイドチャネル情報取得のため、オシロスコープに接続するカレントプローブを別途クランプする。また、ROの内部処理の変化を確認するために、電

源線に漏えいするコモンモード電流をカレントプローブで計測し、オシロスコープを用いて取得する。更に、FPGA による RO 波形の排他的論理和とロジックアナライザによる任意の周波数でのサンプリングによって乱数を生成し、TRNG の乱数性を確認する。

11 段の RO と 9 段の RO から構成される RO-based TRNG（図 3.3）を攻撃対象の TRNG として使用する。RO には 74HCU04AP インバータを使用し、電源電圧は 4.0 V を供給した。11 段と 9 段の RO の発振周波数はそれぞれ約 16.27 MHz と約 18.67 MHz である。この TRNG に対してサイドチャネル情報を用いた乱数性の推定と遠方からの電磁波注入による攻撃を行う。図 3.4 に実験セットアップを表 3.1 に実験に使用した機器を示す。TRNG の乱数性を失わせる電気的外乱の印加は、電源ケーブルを通した TRNG への電磁波の印加を用いる。シグナルジェネレータが生成した連続した正弦波をインジェクションプローブから、電源ケーブルに印加する。TRNG の乱数性の推定には、RO の内部処理に応じて電源ケーブル上に生ずるコモンモード電流を用いる。コモンモード電流は電源ケーブルにクランプしたカレントプローブから取得し、波形をオシロスコープで観測する。RO のロックと TRNG の乱数性の評価のために、オシロスコープによる RO 波形の観測と TRNG が生成するビット列の取得を行なう。ビット列は、RO の出力を FPGA によって排他的論理和をとり、ロジックアナライザによって 1 kHz のサンプリング周波数で取得する。また、本実験では、カレントプローブを対象の TRNG モジュールから約 35 cm 離れた位置に、インジェクションプローブを約 40 cm 離れた位置に設置する。

3.2.4 周波数注入時のコモンモード電流のスペクトル変化

遠方から攻撃を行うための基礎検討として、RO をロックする攻撃信号を機器外部から注入可能であることと RO の内部状態の変化がコモンモード電流の変化として現れ、それが機器外部で計測できることを実証する。

実験では、オシロスコープを用いて RO の出力波形を観察しながら、インジェクションプローブから電源ケーブルに正弦波を印加すると共に、RO を搭載した機器から漏えいするコモンモード電流波形をカレントプローブで取得した。ここ

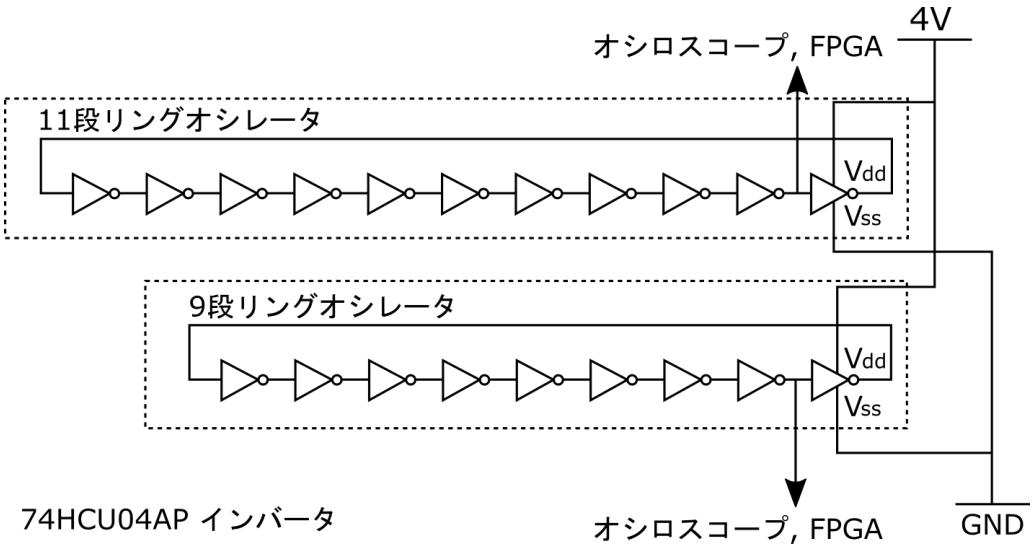


図 3.3: 実験に使用したオシレータの構成

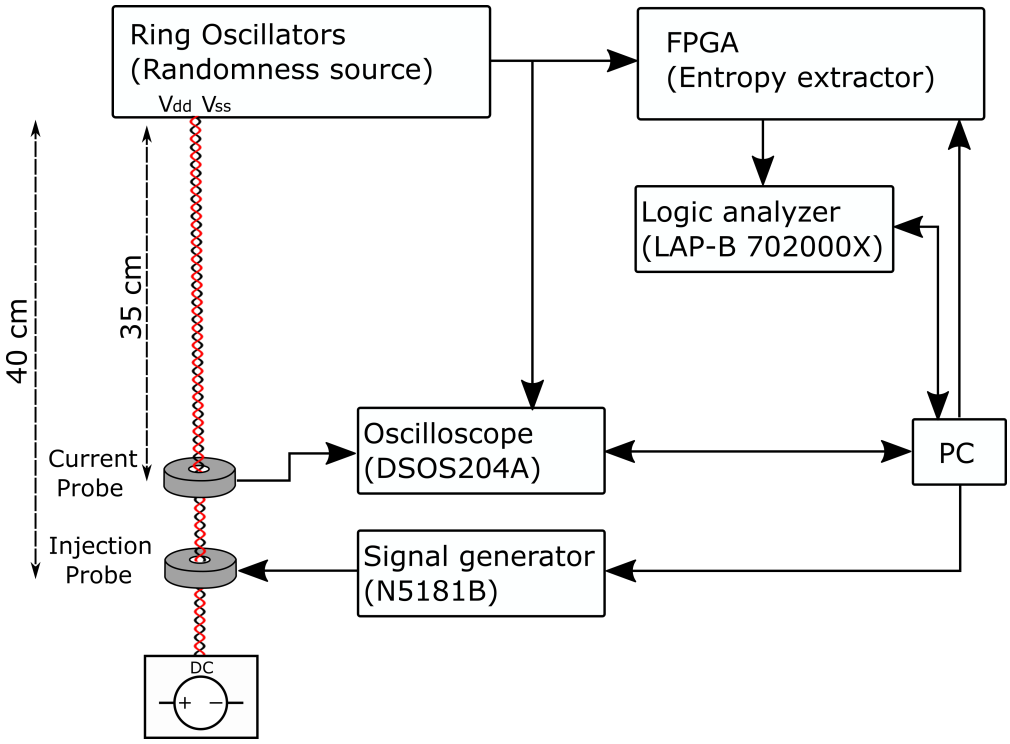


図 3.4: 実験セットアップ

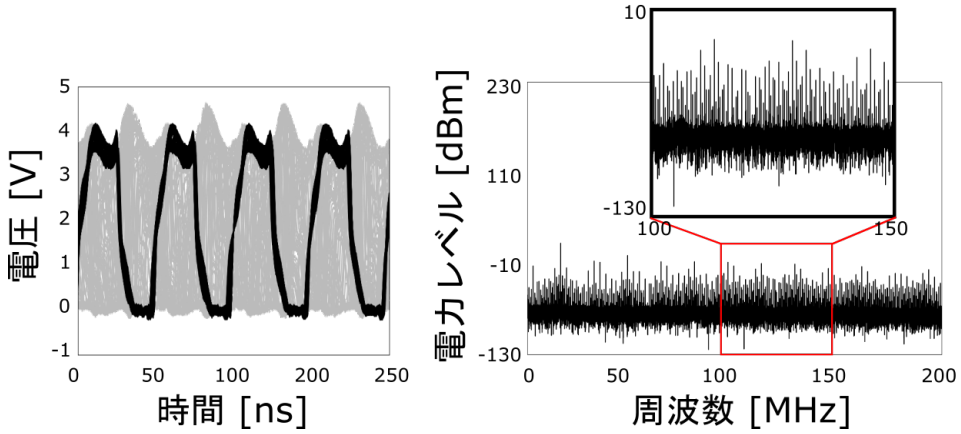
表 3.1: 実験に使用した機器

CMOS インバータ	74HCU04AP
インジェクションプローブ	FCC F-140 (100 kHz to 1.3 GHz)
カレントプローブ	FCC F-2000 (10 MHz to 3 GHz)
オシロスコープ	Keysight DSOS204A
シグナルジェネレータ	Keysight N5181B
ロジックアナライザ	Zeroplus LAP-B 702000X

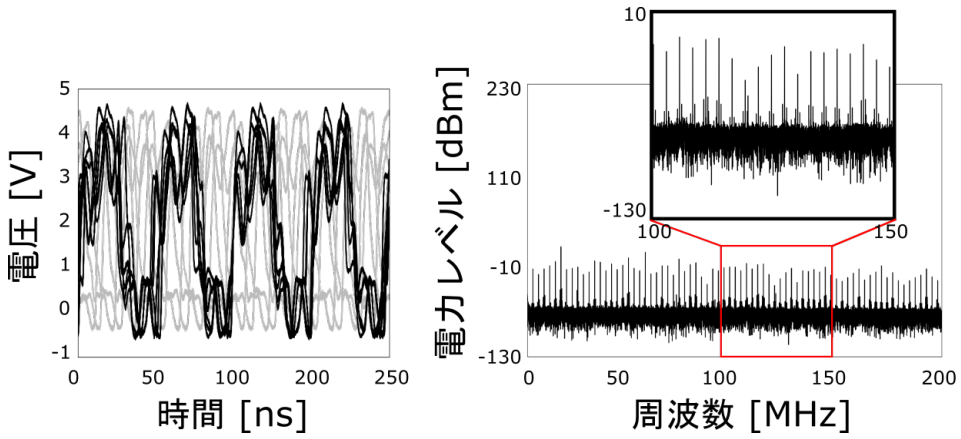
で、注入した電磁波の電力は 25.2 dBm で、注入する周波数は後述するコモンモード電流波形に大きな違いが観測された 32.3 MHz 及び 57.0 MHz とした。

図 3.5 はオシロスコープによって計測した RO 波形を示している。時間領域では 11 段 RO（黒線）にトリガをかけ、取得したデータを 100 波形重ねている。後方のグレー線は 9 段 RO 波形を示している。図 3.5(a) は 32.3 MHz を注入した結果を示している。この結果では 11 段 RO に対して、9 段 RO 波形が多数のパターンをとり、波形のゆらぎが大きいことが確認できる。これは、図 2.4(a) に示したように 11 段 RO に対して 9 段 RO の遷移タイミングがばらついていることを示す。このことから、32.3 MHz で正弦波を注入した場合、RO はロックされないことが確認できる。一方、57.0 MHz を注入した際の観測を示す図 3.5(b) では時間領域において、9 段 RO が少数のパターンをとり、波形のゆらぎが小さいことが確認できる。これは、RO のロックによって遷移タイミングのばらつきが減少していることを示す。以上より、遠隔から（モジュールからの距離 40 cm 程度）電磁波によって RO をロックする攻撃信号が注入可能であることを確認した。

続いて、コモンモード電流からロックによる RO の変化を観測する手法について検討を行う。図 3.6 の時間領域波形は、図 3.5 上に赤線でコモンモード電流を描画したものである。各コモンモード電流は注入周波数と同一の周波数で発振していることが確認された。これは、時間領域では注入する電磁波による影響が大きく反映されていると考えられる。そのため、注入する周波数の影響を抑制し、

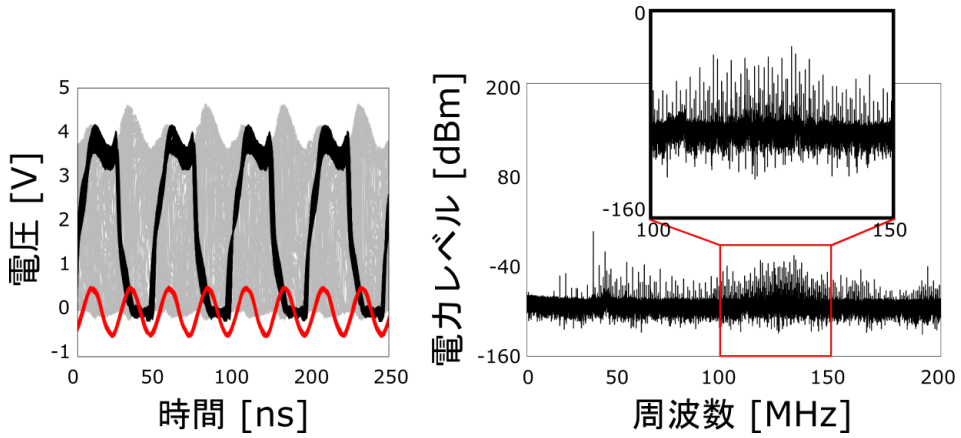


(a) 32.3 MHz injection

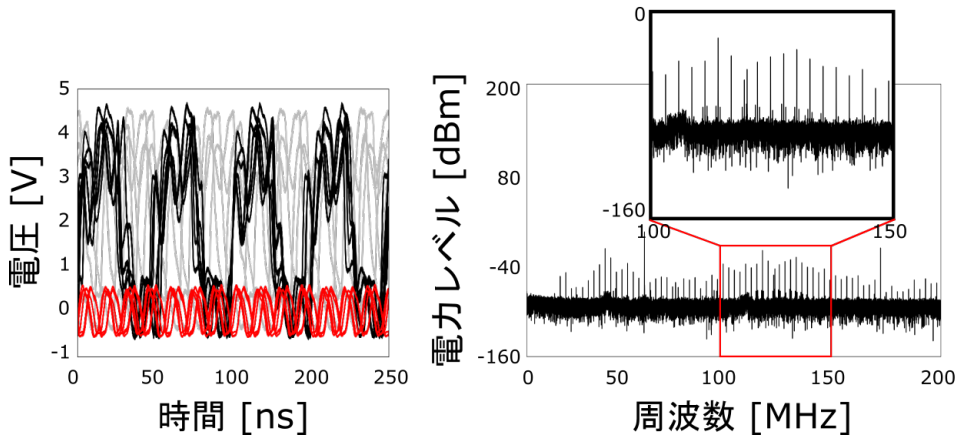


(b) 57.0 MHz injection

図 3.5: 電磁波印加時の RO の出力信号



(a) 32.3 MHz injection



(b) 57.0 MHz injection

図 3.6: 電磁波印加時のコモンモード電流波形

TRNG の動作をより明確に観察するためには、周波数領域において、注入周波数とそれ以外の周波数帯を分離して観測することが有効な手法であると考えられる。

続いて、周波数領域における RO ロック時のスペクトルの変化について考察する。図 3.5(a), (b) の右図に左図の周波数スペクトルを示す。図 3.5(a), (b) それぞれの右図は左図と同様に明確に区別することができる。これは RO がロックされていない図 3.5(a) では、ジッタ及び RO の相互作用によって生じたノイズにより、多数のピークが観察されるのに対し、図 3.5(b) では RO がロックされたことで、そのノイズが減少し、ピークの数が減少することに起因する。また、これらの波形はコモンモード電流においても同様に計測可能であることが図 8 から確認でき、特に 100-150 MHz の範囲で非ロック時（図 3.6(a)）/ロック時（図 3.5(b)）の差が明確に観測された。

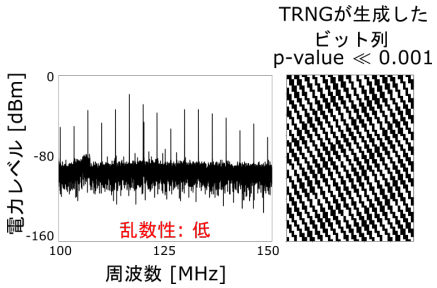
以上より、RO の動作の変化がコモンモード電流からも観測可能であることが確認されことから、これらを識別子として用いることで、TRNG の乱数性が低下した状態を推定できると考えられる。

3.2.5 コモンモード電流の観測に基づく TRNG の乱数性の推定

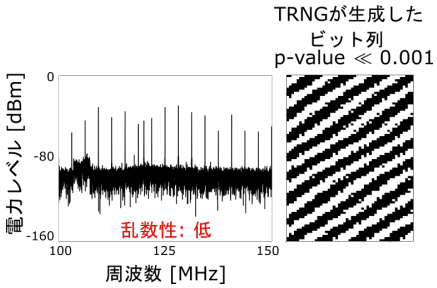
前節で得られた結果に基づきコモンモード電流をサイドチャネル情報として用いることで TRNG の乱数性低下が推定できることを示す。

本実験では、ロック周波数が分からないという前提で、10-100 MHz の範囲において変化させた正弦波を電源線から TRNG に印加する。この時、コモンモード電流をカレントプローブから観測し、周波数領域波形を取得する。取得した周波数領域波形が図 3.6(b) に示す波形に類似する場合は TRNG の乱数性が低下していると判断する。実際に乱数性の低下を評価するために、TRNG が生成するビット列の観察を行った。

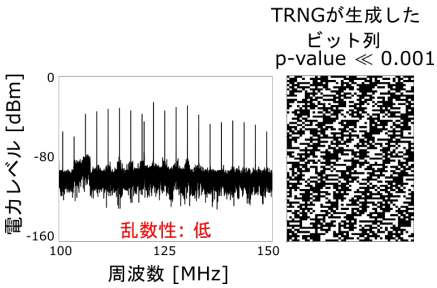
図 3.7 にコモンモード電流の周波数領域波形、乱数性の推定結果、TRNG が生成したビット列を示す。TRNG が生成したビット列は 1 を黒、0 を白として、左から右、下から上の順に表している。また、乱数性の評価には、NIST の DFT 検定を用いた [41]。乱数性の検定は各条件下で得られた 6.5×10^4 ビットを使用し、有意水準は 0.1 %とした。P 値が 0.001 より低い時、ビット列の乱数性は棄却さ



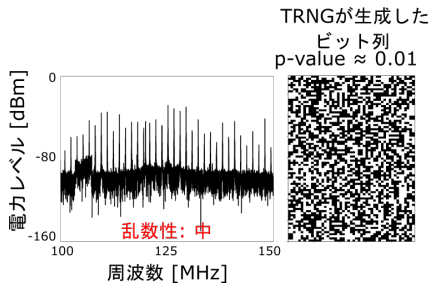
(a) 58.3 MHz injection



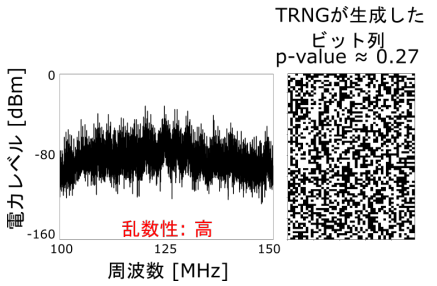
(b) 78.1 MHz injection



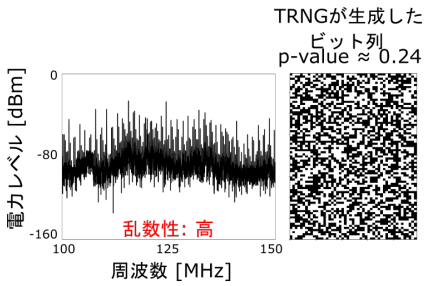
(c) 90.3 MHz injection



(d) 18.5 MHz injection



(e) 27.2 MHz injection



(f) 91.4 MHz injection

図 3.7: サイドチャネル情報を使用した乱数性推定と攻撃結果

れる。

図 3.7 上段は乱数性が低下したと推定した結果である。これらの条件下では、TRNG が生成するビット列に周期性が観測されている。DFT 検定の結果も、コモンモード電流を用いて判定した結果と同様に、図 3.7 上段の条件ではいずれのビット列も乱数とは認められなかった。

次に、図 3.7(d) は上段に比べピークが多く観測されていることから、乱数性は中程度であると推定した条件である。この条件下では、TRNG が生成するビット列の P 値は 0.001 を上回るため、乱数性は棄却されなかった。最後に、乱数性は低下していないと推定した図 3.7(e), (f) でも、TRNG のビット列は P 値が 0.001 を大きく上回り、乱数性は棄却されないことが確認された。以上より、コモンモード電流から、乱数性が大きく低下する条件を推定可能であることが確認された。また、図に示した注入周波数以外にも、図 3.7(b) のような傾向を示すコモンモード電流が発見されたが、いずれの場合も RO がロックされていることが確認された。

本実験では、コモンモード電流をサイドチャネル情報として用いることにより、TRNG の乱数性を推定し、デバイス遠方からの電磁波注入によって非侵襲に TRNG の乱数性を低下させることが可能であることを実証した。

3.3 電気的外乱による出力ビット操作に対する一様性・再現不可能性への影響評価

本節では、電気的外乱による一様性･再現不可能性への影響の評価を行う。TRNG に対して電気的外乱を与え、一時的に出力ビットを操作することで、一様性・再現不可能性を低下可能なことを示す。

TRNG が生成する乱数は暗号プロトコル中で、セッション鍵の生成やノンス、サイドチャネル攻撃対策のマスキングなど様々な用途に使用されている。暗号プロトコル中では、これらの秘密情報が一様かつ予測不可能であることによってセキュリティが保証されている。既に、TRNG には乱数性を評価する Health test や出力ビット列をより乱数性の高いビット列に変換する Post-processing の実装が推奨されている [39, 40]。TRNG の乱数性を保証することは、セキュリティを担保するう

えで極めて重要である。FPGA プラットフォームでは、TRNG 実装の制約として、デジタル回路のみで構成可能であることが求められる。そのため、RO のジッタをエントロピー源とした TRNG が数多く提案されている [15, 16, 17, 18, 19, 21]。なかでも、[19] で提案された TERO-based TRNG は、RO をエントロピー源とする TRNG のなかで、高いエントロピーを持つ乱数を高速に生成可能であることから、広く利用されている TRNG の一つである。この TRNG に対する物理攻撃手法として、Markettos と Moore が提案した周波数注入攻撃 [35] や電源電圧の操作による乱数性の低下 [38] が知られている。周波数注入攻撃では、エントロピー源となるオシレータの発振周波数の基本波や高調波を機器に印加することで、オシレータのジッタを抑制し、乱数性を低下させる。攻撃者は印加する電磁波を操作することで、TRNG が生成するビットの乱数性を操作可能である。また、[38] で示されている供給電圧の変化は、TRNG の出力ビットを大きく偏らせる可能性を示している。これらの攻撃は機器に対して電気的な外乱を与えることで乱数性の低下を引き起こす。しかし、TRNG には前述したとおり、乱数性を評価する Health test や出力される乱数の質を高める Post-processing が実装されている。そのため、従来のような攻撃手法では、TRNG に対して影響を与えることは難しい。

これに対して、本節では電気的な外乱による出力ビットへの影響の評価を行う。なかでも、乱数性を保証する機構が実装されている TRNG に対しても乱数性低下が実現可能であるかについて評価を行う。具体的には、TERO-based TRNG に対して出力ビットを決定論的に変化させるような妨害を一時的に注入する。これにより、出力ビットの一部が大きく偏ることから、乱数列の一部が予測できる可能性があり、生成される乱数のエントロピーを低下できる可能性がある。この決定論的な乱数性低下が実現した場合、TRNG に対する一様性や再現不可能性の低下が生じることから、これらの乱数性に対する物理攻撃への影響を評価可能である。

3.3.1 出力ビットを操作する電気的外乱の印加手法

周波数注入攻撃では、振り子の共振現象のように、ある発振周波数を持った発振器が特定の周波数によってロックされる現象を利用する。TERO-based TRNG

に対する周波数注入攻撃では、TERO の発振周波数の基本波またはその高調波に近い信号を印加することでジッタを抑制し、V_{out1} と V_{out2} のエッジの衝突を抑制する。[53] では、TERO に摂動を与えることで、ジッタが抑制されて TERO の Duty 比が一定の値に収束し、振動が続くことが示されている。文献 [54] では、TERO の発振周波数の二次高調波を印加することで、図 2.7(b) のように V_{ctrl} の立下りまで発振を続け、カウンタ数に偏りが生じることが示されている。一方、RO は発振時のスイッチングイベントによって自己発熱を生じるため、TERO では 1 ビット生成時においても発振周波数の変化が生じる。この発振周波数の変化はインジェクションによるロック効率に影響を及ぼす可能性がある。[53] では、周波数注入攻撃による TERO の発振周波数のロックは全てのビットで生じるわけではないことが示されている。このことから、周波数注入攻撃によって TERO-based TRNG の出力ビットを決定論的に操作することは難しいと考えられる。

TERO-based TRNG の乱数性を決定論的に低下させるには、攻撃によって確実に、図 2.7(b) のように TERO の振動を変化させる手法が必要である。そのため、周波数注入攻撃による決定論的な出力ビットの操作は難しい。それに対して、[54] では V_{out1} と V_{out2} のエッジが互いにロックする Self-locking によって発振が安定する可能性を示している。TERO の発振開始時間において、Self-locking が引きおこりやすい V_{out1} と V_{out2} の発振周波数や初期ノイズ条件を外部からの妨害によって与えることができれば、TRNG の乱数性を決定論的に操作できる可能性がある。

一方、意図的な電磁妨害による電磁波の印加は機器に対して高周波の電磁界を印加することで、機器の V_{dd}/GND 間の電位を変化させる。一般的に、正弦波の印加による電位の変化は交流として生じる。一方、機器に交流成分を直流成分に変換するような回路構造が存在した場合、妨害波の印加によって機器の電源電圧を変化させられる可能性がある。TRNG に対する電源電圧の操作はエントロピー源となる TERO の発振周波数を変化させる。そのため、機器に対して妨害波を印加し、電源電圧を操作することができれば、TERO の発振周波数を操作し、Self-locking による乱数性低下を引き起こすことができる可能性がある。

このことから、本節では印加する妨害波を操作することで、TRNG の出力ビッ

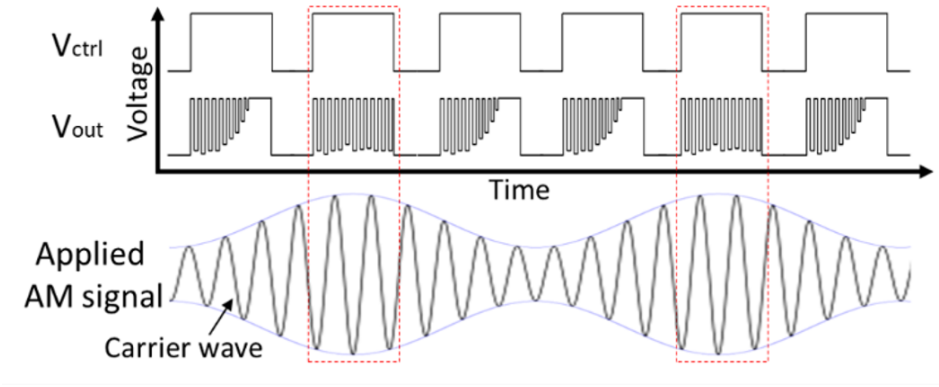


図 3.8: 振幅変調波印加時の TRNG の動作の変化

トを決定論的に操作する手法を提案する。具体的には、振幅変調した妨害波を印加することで、機器の V_{dd}/GND 間の電位を変化させる。そして、機器の電圧値に応じて特定のビットに対しては出力を偏らせ、その他のビットに対しては乱数性を保った出力を生じさせる。振幅変調をした妨害波印加時の TRNG の変化について図 3.8 に示す。まず、TRNG の出力を決定論的に低下させる注入周波数 f_1 を搬送波として異なる周波数 f_2 で振幅変調を行う。図 3.8 のように印加強度が一定の値を超えたときに出力ビットが固定の値をとり、出力の予測が可能となる。このとき、変調を行う周波数 f_2 を TRNG の乱数生成速度の $1/n$ (n は任意の整数) とすることで、攻撃によって出力が固定化したビットを周期的に発生させることができる。

3.3.2 実験セットアップ

攻撃対象の TRNG として、FPGA 上に実装された TERO-based TRNG を使用した。TERO を制御する信号は 11 段の RO と非同期カウンタによって生成されるクロックである。クロックの立ち上がりに応じて TERO の発振が開始し、クロックの立下りまでに安定状態に遷移する。また、クロックの立下り時に、T flip-flop にリセット信号が入力される。TERO は二つの NAND ゲートと 20 個のインバータから構成される。この TERO の発振回数を T flip-flop でカウントし、1 ビットの乱数を生成する。また、FPGA 上の TERO の実装については、二つの TERO-

branch を同トポロジーとなるように SLICE を指定し、TERO-branch が隣接するように実装を行った。

図 3.9 に実験セットアップを示す。本章では、電源電圧の操作による乱数性低下と妨害波印加による乱数性低下を評価するために二つの実験が可能な実験セットアップを構成した。TERO-based TRNG を実装した FPGA を攻撃対象のデバイスとする。本稿では、妨害波印加による電源電圧の変化の可能性を示すため、電気的外乱の印加が容易なデバイスを仮定し、ボード上の改変を行った Spartan6 LX9 Microboard を使用した。改変内容は、IC 周辺のデカップリングコンデンサの除去と、IC 近傍に妨害波印加のための SMA ポートを実装した。FPGA は PC から 5 V の電源が供給されており、ボード上のレギュレータによって IC に 1.2 V が供給されている。妨害波の印加による電源電圧の操作のために、シグナルジェネレータ（Keysight, N5181B）から生成された正弦波は 10 W アンプを介し、SMA ポートに印加した。また、電源電圧の変化による乱数性低下を示すために、FPGA に付加した SMA ポートを T コネクタで分岐させ、Low-pass filter (DC-5 MHz) を介して、安定化電源に接続した。安定化電源と Low-pass filter の間の配線をプロービングし、オシロスコープ (Keysight, DSOS204A) で測定することで IC に供給されている電源電圧の評価を行った。また、電源電圧の変化による TERO-based TRNG の変化を評価するために、I/O ピンから出力した TFF 波形と TERO-based TRNG が出力した rawbit 波形を取得した。

3.3.3 電源電圧操作による乱数性の低下

FPGA の IC に供給される電源電圧を直接操作することで、TERO-based TRNG に生じる変化について検討を行う。その後、電磁波印加によって、Vdd/GND 間の電位が変化することと、それによって乱数性低下が生じることを示す。

まず、電源電圧の操作による乱数性低下の検討を行う。実験では、安定化電源から FPGA 上に付加された SMA ポートを介して、IC に供給される電源電圧を操作した。攻撃対象の TRNG は発振周波数 109.4 MHz の TERO を利用し、乱数を生成する。TERO を制御する信号は、RO（発振周波数：145 MHz）を 9 段の非同期カウンタから分周した 286.8 kHz のクロック信号である。また、オシロスコー

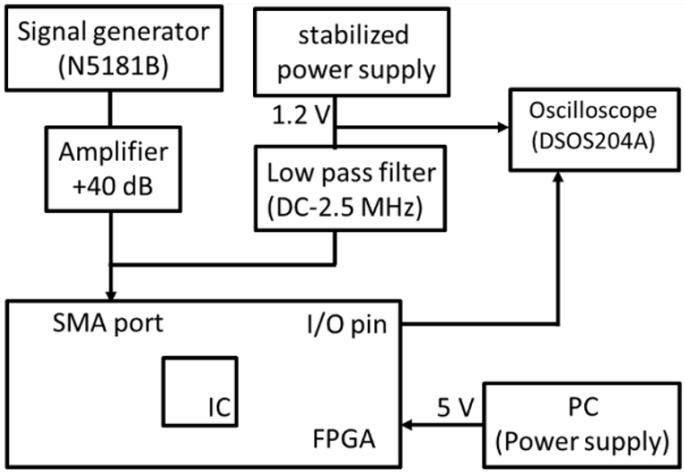
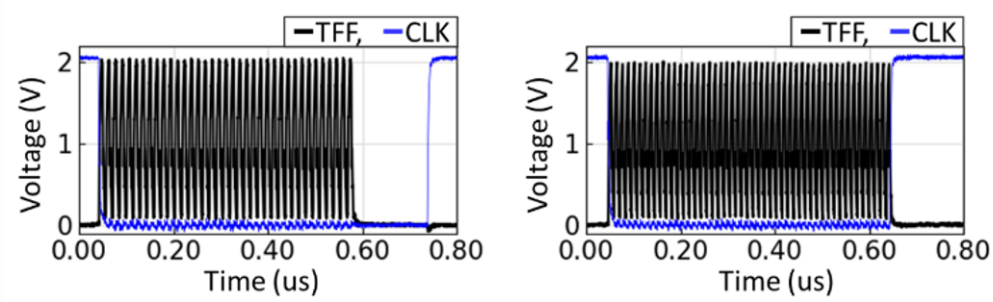


図 3.9: 実験セットアップ



(a) 供給電圧 1.20 V　　(b) 供給電圧 1.43 V

図 3.10: 供給する電圧を変化させたときの TFF 波形とクロック波形の変化

プによって、TFF 波形の観測とクロック波形の観測、電源電圧の評価を行った。

図 3.10 は既定の電圧値である 1.20 V の電圧を供給した結果と電源電圧を掃引し、乱数性が大きく低下した 1.43 V の電圧供給を行った結果を示している。既定の電圧値を供給した場合は、3.3.1 節で示した TERO の設計に従い、リセット信号の印加までに TERO の振動が停止していることを示す。このとき、出力したビット列は乱数性を示していた。また、オシロスコープで測定した V_{dd}/GND 間の電位は 1.10 V であった。一方、図 3.10 (b) に示すように、1.43 V の電圧を印加した時の TFF 出力波形はクロック信号の立下りと同時に TFF 出力波形の発振が停止していることが確認できる。TERO の振動回数が大きく偏ったことから、出力

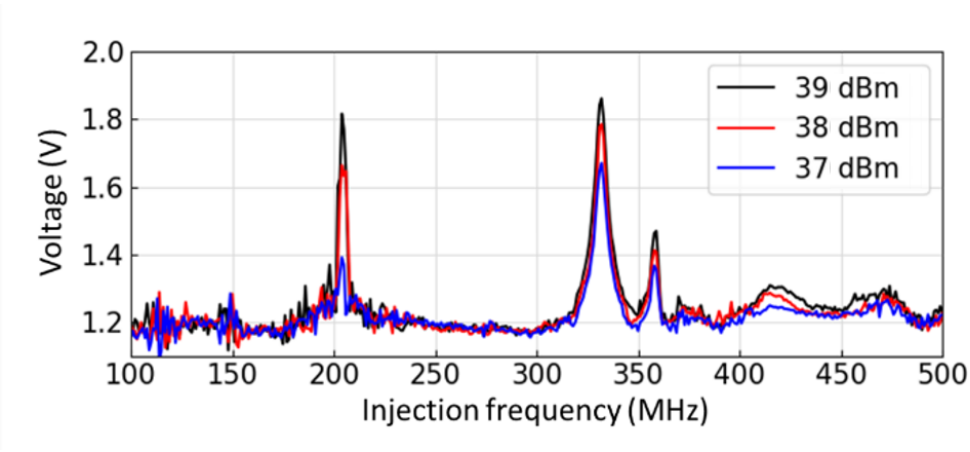


図 3.11: 電気的外乱印加による V_{dd}/GND 間の電圧変化

ビットはすべて 1 の値をとった。このとき、オシロスコープで計測した V_{dd}/GND 間の電位は 1.33 V であった。

続いて、電気的外乱の印加によって生じる V_{dd}/GND 間の電位の変化と乱数性の低下について示す。実験では、印加する外乱の周波数と電力を掃引しながら、V_{dd}/GND 間の電位と TFF 出力波形の取得を行った。図 3.11 に注入した周波数と電力に対する V_{dd}/GND 間の電位の変化を示す。横軸は注入周波数を示し、縦軸は電位を示している。205 MHz と 332 MHz、358 MHz において大きなピークが存在し、電位が大きく変化していることが確認できる。また、注入する電力を大きくするほど、電位の変化が大きくなっていることが確認できる。このとき、図 3.10 (b) の V_{dd}/GND 間の電位である 1.33 V と一致する攻撃条件下（注入周波数 332 MHz）における TFF 出力波形と乱数列は図 3.10（b）と同様の結果を示した。以上より、TRNG に対する電気的外乱の印加によって V_{dd}/GND 間の電位を変化させることで、出力ビットを固定できる可能性を示した。

3.3.4 振幅変調波の印加による出力ビットの操作

振幅変調した妨害波を印加することで、出力ビットの一部を操作可能なことを示す。

実験では、FPGA のレギュレータをバイパスすることで、評価が容易な実験系

を作成し、検討を行った。FPGA には発振周波数 115.6 MHz の TERO と TERO を制御するクロック信号（発振周波数：602 kHz）を実装した。注入周波数を掃引して、効率よく乱数性低下を引き起こす正弦波（周波数 237 MHz、電力 38.5 dBm）を搬送波として選択した。変調波として、クロック信号の 1/5 倍の周波数である 120.4 kHz のサイン波を利用した。また、変調度は 100 %とした。

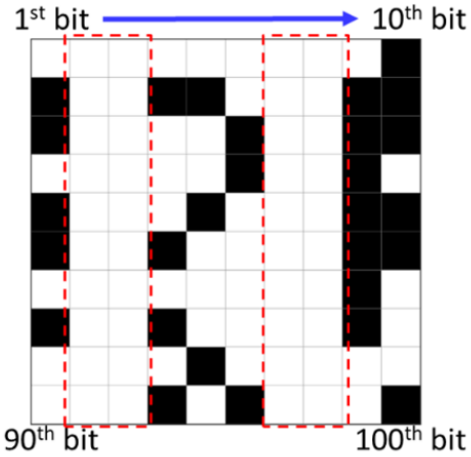


図 3.12: 振幅変調波印加時の TRNG の出力ビット列

図 3.12 に振幅変調した妨害波の印加を行った結果を示す。印加した妨害波の振幅が高いときの TFF 出力波形は図 3.10 (b) のように、クロックの立下りまで TERO が振動していることが確認できる。また、このような波形は図に示したように 5 ビット周期で確認できる。これらの出力は全て 0 を示している。このとき、他のビットについては乱数性を失っていない。

以上より、振幅変調波を妨害波として TRNG に印加することで、TRNG の出力ビットの一部を偏らせる可能性について示した。出力が偏ったビットは周期的に表れることから、乱数列の一部を推定可能であると考えられる。また、変調波を変化させることで、出力が偏ったビットの周期を変化させることができる。

最後に、電気的外乱の印加によって IC に供給される電源電圧が変化する理由について考察を行う。本稿で用いたデバイスにおいては、妨害波の印加により電源電圧の直流値が上昇する現象を観測した。IC の電源には ESD (Electro-Static Discharge) 保護のための回路が搭載されていることが多い [55]。一般的には ESD

保護にはダイオード構造が用いられ、ブレイクダウン電圧を超える電位差が電源・グラウンド間に発生するとダイオードに電流が流れる。この現象が正弦波による電位変動に歪みを発生させ、電源電圧の直流値が変化した可能性がある。

3.4 結言

本章では、TRNG に対する物理攻撃による、一様性・再現不可能性について影響評価を行った。3.2 節では、非侵襲な電気的外乱の印加手法について検討を行った。機器遠方から電源ケーブルを通じて非侵襲に電気的外乱を印加が可能であることと、機器外部から得られる情報を利用することで攻撃条件が推定可能であることを示した。そして、実際に遠方から非侵襲に電気的外乱を与えることで、TRNG の周期性を統計的に有意に低下させることを示した。3.3 節では印加する妨害波を操作することで、出力ビットの乱数性を一時的に大きく低下させ、一様性と再現不可能性の低下を引き起こすことが可能であることを示した。電気的外乱によるエントロピー源の操作は時間方向に対して分解能が高いことから、振幅変調波を妨害波として印加することで TRNG の乱数性を一時的に大きく減少させた。実際に、攻撃によって、特定の周期でビット列を操作することが可能であり、一様性とともに再現不可能性についても低下させることを実証した。

4. オシレータベースの TRNG から生じる漏えい情報による予測不可能性への影響評価

4.1 緒言

前章では、TRNG に対する電気的外乱を使用した物理攻撃に対する一様性・再現不可能性への影響評価を行った。本章では、TRNG から生じる漏えい情報の解析による、予測不可能性への影響評価を行う。4.2 節では、オシレータから生じる漏えい情報により、TRNG のエントロピーを評価する手法について検討を行う。続いて、4.3 節では予測不可能性の低下を評価するために、出力ビットの推定が可能であるか評価を行う。具体的には、出力ビットが機器外部から得られる情報によって推定可能であるか評価を行うために、出力ビットに依存した回路動作の変化を反映した電磁放射から乱数を予測できる可能性を示す。

4.2 オシレータベースの TRNG に対する APD を使用したエントロピー評価手法

本節では、オシレータから生じる漏えい情報によって、TRNG のエントロピーを推定可能であるかについて検討を行う。TRNG のエントロピーを機器外部から推定することは予測不可能性の評価を行うと共に、電気的外乱に対する TRNG の攻撃耐性評価手法として適用できる可能性がある。

これまで、TRNG のエントロピー源である RO のジッタを評価する手法として、時間領域におけるジッタの測定が用いられてきた。この測定では、エントロピー源として使用する全ての RO に対して観測ポートを用意して、各 RO の出力波形を観測する必要がある。一方、3.2 節で示したように、オシレータから生じる電磁放射を利用することで、オシレータが持つエントロピーを評価できる可能性がある。特に、周波数領域において RO のエントロピーを評価することができれば、観測ポートを設けることなく、TRNG の攻撃耐性評価を実現できる可能性がある。

これに対して、本節では妨害電磁波の評価に使用される振幅確率分布（APD: Amplitude Probability Distribution）測定 [56, 57, 58] を利用することで、周波数領域における RO のエントロピー評価を行う。APD は動的な特性を持つ信号やノイズなどの非定常な信号を有効に調べる手法であり、APD 測定によって RO のエントロピーのような確率的な事象についても評価できる可能性がある。

4.2.1 APD 測定を利用した RO のエントロピー評価手法

現在、広く利用されているオシレータをエントロピー源とする TRNG は、RO の遷移タイミングの揺らぎであるジッタを利用することで乱数を生成する。ジッタはランダムな物理現象であり、ジッタの蓄積によって RO の遷移タイミングのばらつきが大きくなる。一般的に、エントロピー源には複数の RO が使用され、個々の RO がもつエントロピーを合わせることで質の良い乱数が生成される。これに対して、2 章で述べたように、周波数注入攻撃は振り子の共振現象のようにある発振周波数を持った発振器が特定の周波数を持った注入信号によってロックされる引き込み現象を利用する。RO が複数存在する場合には、全ての RO のエントロピーが低下することで、TRNG の乱数性が低下する。そのため、周波数注入攻撃に対する TRNG の耐性を評価するには、TRNG に使用される全ての RO のエントロピーを評価する必要がある。RO のエントロピー評価には、時間領域におけるジッタの測定が用いられてきた。ジッタを測定するには、個々の RO に対して観測ポートを設けて、RO の出力信号を観測する必要がある。これに対して、3.2 節では機器の内部状態を反映した電磁波の取得により、RO の内部情報を周波数領域で観測可能であることを実証した。周波数領域において各 RO のエントロピーを評価することができれば、特別な観測ポートを設けることなく、TRNG の乱数性低下を評価できる可能性がある。

周波数領域における評価手法として、電磁妨害波の評価に使用されている APD 測定が存在する [58]。APD 測定は電磁雑音の特性評価などに使用されており、測定で得られた情報には電磁界の強度だけでなく，時間的な継続性の情報も含まれている。このことから、RO のエントロピーといった確率的な事象についても統計的に評価できる可能性がある。APD は、被測定信号 $W(t)$ がある振幅値 X_k を

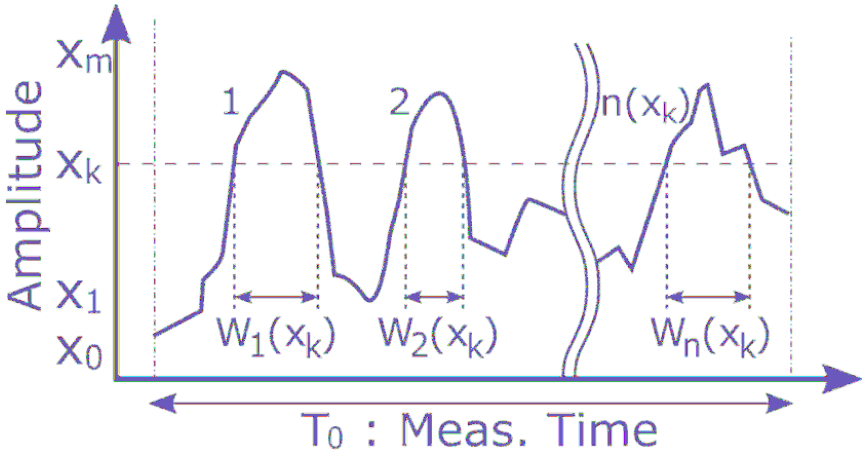
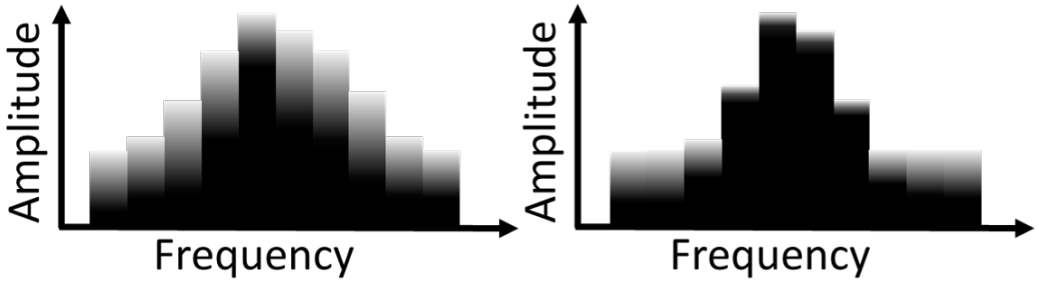


図 4.1: APD の概念

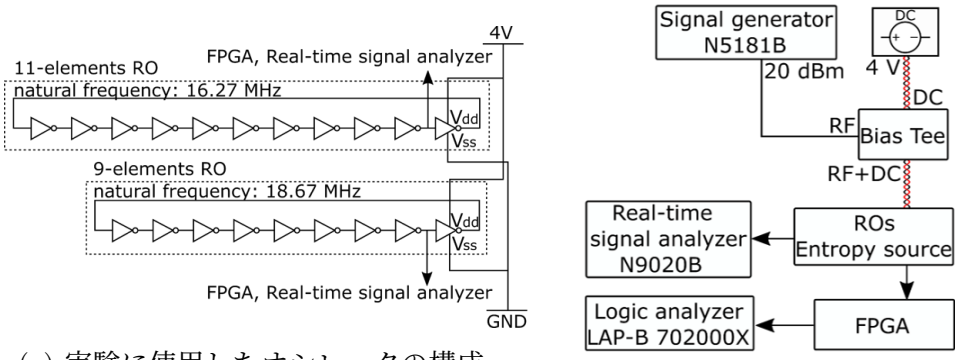


(a) 高エントロピー時　　(b) 低エントロピー時

図 4.2: APD 測定における RO のエントロピー

超える時間確率によって表される（図 4.1）。

続いて、RO のエントロピーが APD にどのように反映されるかについて述べる。RO のエントロピーは、周波数領域では位相雑音として現れ、発振周波数を中心としたスペクトルの広がりとして表現される。一方、RO のエントロピーが低下した場合は、発振周波数近傍の位相雑音が低減する。このエントロピーの変化を Multi-channel APD で表す。図 4.2 (a), (b) は、横軸は周波数を縦軸は振幅を表し、ある周波数に対する APD をグレースケールで表している。RO が高エントロピーの時、位相雑音により発振周波数近傍での振幅変動が増大するため、



(a) 実験に使用したオシレータの構成

(b) 実験セットアップ

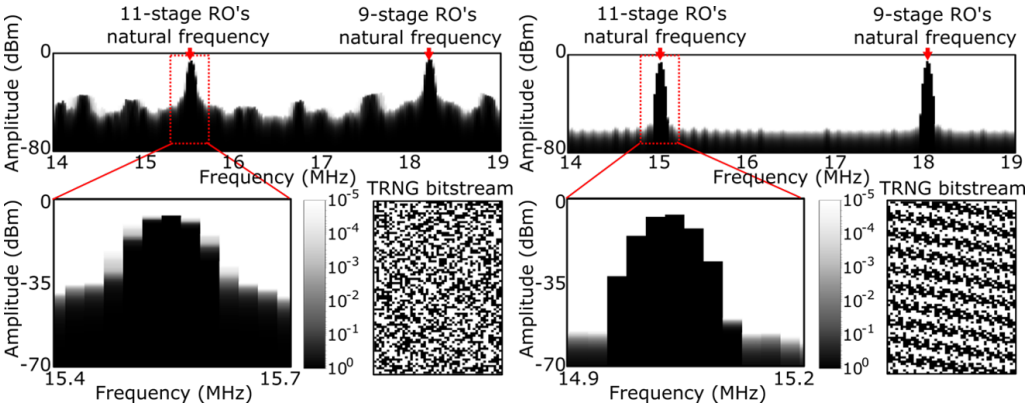
図 4.3: CMOS インバータを使用した RO-based TRNG に対する APD 測定の評価セットアップ

振幅方向に分布の裾が広がる。一方、RO のエントロピーが低下すると位相雑音が低減するため、振幅方向に分布が急峻に変化する。以上の変化を利用することで、RO のエントロピー低下を推定し、攻撃による TRNG の乱数性低下を評価できる可能性が高い。

4.2.2 APD 測定によるエントロピー評価の基礎検討

本節では、APD 測定によるエントロピーの評価が実現可能であるかの基礎検討を行うために、CMOS インバータを使用した RO-based TRNG に対する電気的外乱を行った際の乱数性と Multi-channel APD 波形の評価を行った。図 4.3 に実験セットアップを示す。TRNG の乱数性を低下させるため、シグナルジェネレータで生成した正弦波を Bias-Tee を用いて、直流電圧に合成し、RO に印加した。続いて、リアルタイムシグナルアナライザによって、RO 基板の V_{dd}/GND 間のスペクトルを測定し、APD を取得した。また、TRNG が生成するビット列を取得するために、二つの RO の出力信号を FPGA によって排他的論理和をとり、ロジックアナライザによって 1 kHz のサンプリング周波数で取得した。

実験では、発振周波数を掃引して乱数性を低下させる攻撃条件（周波数 90.0 MHz、電力 20.0 dBm）を探索し、計測を行った。また、乱数性が低下しない攻撃条件のうち代表的な例である、周波数 97.0 MHz、電力 20.0 dBm の正弦波を印



(a) 97.0 MHz の正弦波印加時　　(b) 90.0 MHz の正弦波印加時

図 4.4: 正弦波印加による Multi-channel APD 波形とビット列の変化

加したときの Multi-channel APD 波形と出力ビット列を取得した。

図 4.4 に正弦波印加時の Multi-channel APD 波形と TRNG が生成したビット列を示す。ビット列は 1 を黒、0 を白として、左から右、下から上の順に表している。図 4.4 (a) では、RO の発振周波数近傍の振幅確率が次第に変化していることから、高いエントロピーを持つと考えられる。このとき TRNG は乱数性を持つことが確認できる。一方、図 4.4 (b) では、振幅確率が急峻に変化していることから、エントロピーが低下していると考えられる。このとき、TRNG の乱数性が大きく低下していることが確認できる。以上から、RO の発振周波数近傍の APD の変化から、TRNG の乱数性を評価可能であると考えられる。

4.2.3 FPGA 実装した ERO-TRNG に対する RO のエントロピー評価

本節では、実デバイス環境を想定して、FPGA 上に実装した TRNG に対して、APD 測定を行うことで、RO のエントロピーを評価可能であることを示す。具体的には、FPGA 上に実装した ERO-TRNG に対して周波数注入攻撃を行い、攻撃による乱数性低下が、RO の APD 波形から推定可能であることを示す。

評価対象として使用する 2 つの RO のエントロピーを低下させるために、各 RO の発振周波数の高調波を 2 台のシグナルジェネレータを用いて生成し、FPGA に印加した。また、妨害波印加時、非印加時に生成される乱数の出力ビット列と RO

の APD 波形の観測を行った。

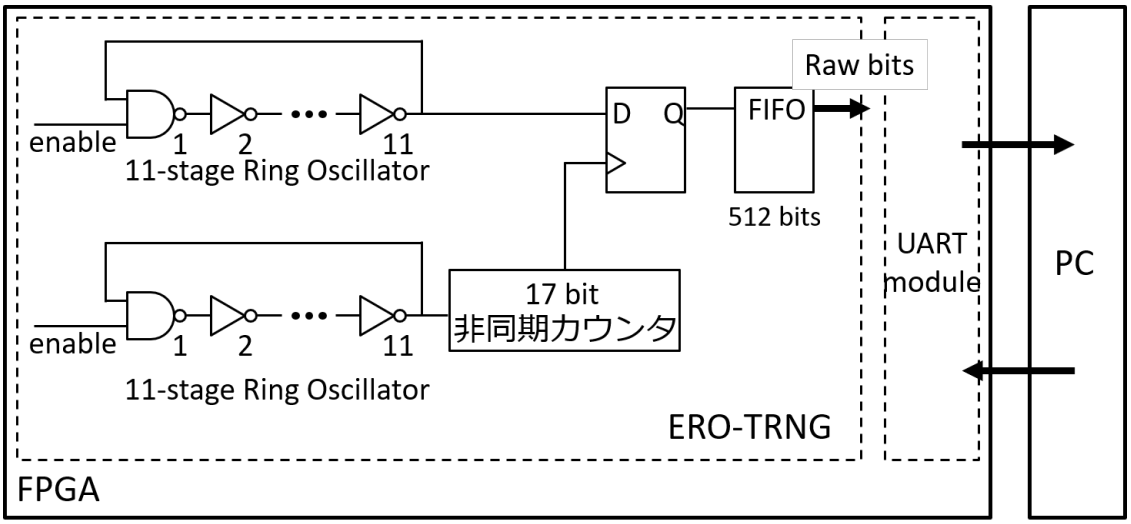


図 4.5: ERO-TRNG の実装

本提案手法の有効性を示すために、FPGA 上に ERO-TRNG を実装し、攻撃の実現可能性について評価を行った（図 4.5）。RO は共に 11 個の Look-up tables (LUTs) を使用し、発振周波数はそれぞれ約 109.58 MHz と 115.35 MHz である。115.35 MHz の RO は 17 ビットの非同期カウンタによって 880 Hz のサンプリングクロックを生成し、もう一方の RO を D フリップフロップによってサンプリングすることで乱数を生成する。ここでは、サンプリングされる RO を RO_1、サンプリングクロックを生成する RO を RO_2 と呼ぶ。TRNG は PC からコマンドを受信することで、RO を発振させ、乱数生成を開始する。そして、512 ビットの連続した乱数を生成した後、RO の動作を停止し、生成したビット列を PC に送信する。実験では、APD 測定によるエントロピー評価が実現可能であることを示すために、電気的外乱の印加が容易なデバイスを仮定し、改変した FPGA（Spartan6 LX9 Microboard）を評価用ボードとして使用した。FPGA には、デカップリングコンデンサの除去と IC 近傍に SMA ポートを付加することで、レギュレータをバイパスして妨害波を印加可能な改変を行った。図 4.6 に実験セットアップを示す。各 RO のエントロピーを抑制する正弦波は 2 台のシグナルジェネレータを用いてそれぞれ生成し、付加した SMA ポートを介して FPGA に印加する。また、

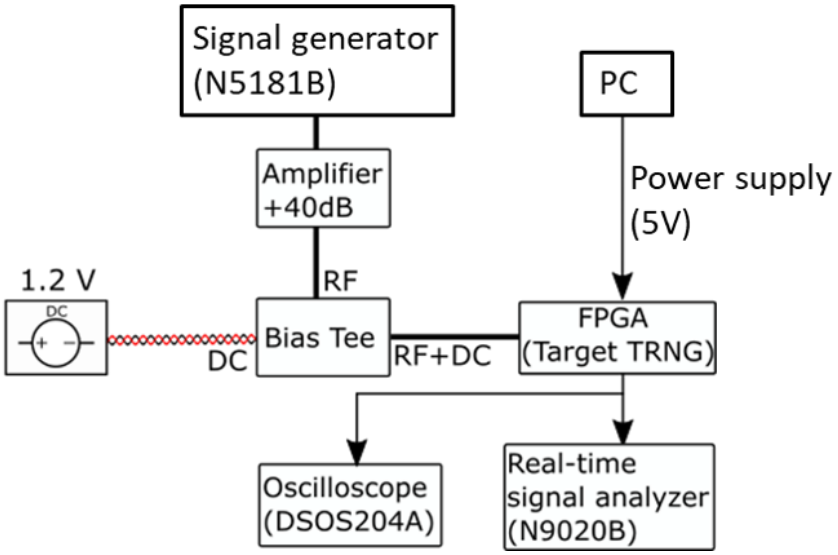
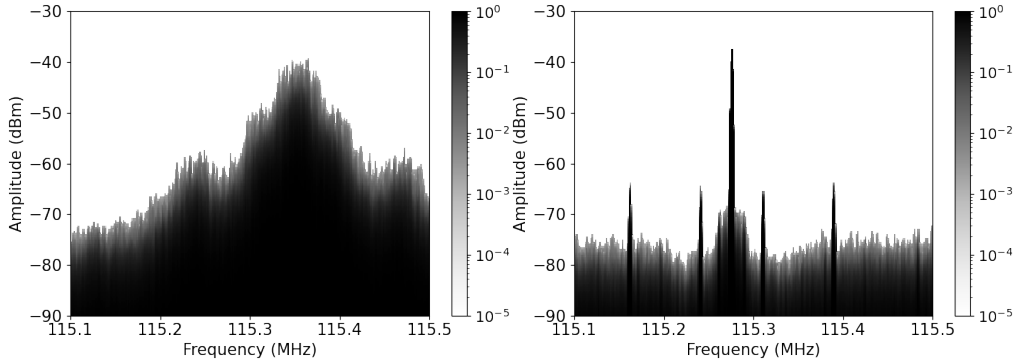


図 4.6: 実験セットアップ

FPGA は PC から USB ケーブルを通じて給電される。RO のエントロピーを評価するために、FPGA の I/O ピンから V_{dd}/GND 間の電圧スペクトルをリアルタイムシグナルアナライザによって取得し、APD を測定した。APD は各 RO の発振周波数を含む 1 MHz の範囲で測定を行い、Resolution bandwidth を 2.4 kHz とし、30 ms の測定時間中に含まれる振幅確率を取得した。

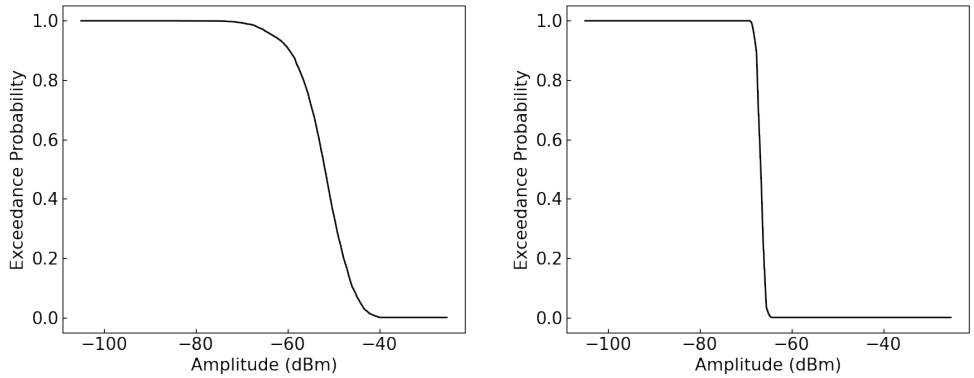
実験では、各 RO の発振周波数に対して、高調波近傍の周波数と電力を掃引することで、出力ビット列の乱数性を低下させる攻撃条件を探索した。妨害波非印加時、印加時についてそれぞれ、リアルタイムシグナルアナライザを用いて、V_{dd}/GND 間の電圧スペクトルを観測することで RO の APD 波形を取得した。RO_1 に対する攻撃条件は周波数 219.0700 MHz、電力 30.5 dBm の正弦波で、RO_2 に対しては周波数 230.5512 MHz、電力 28.6 dBm の正弦波である。

図 4.7 に妨害波非印加時と印加時の RO_2 の APD と TRNG が生成したビット列をそれぞれ示す。図 4.7 (a), (b) は RO_2 の発振周波数近傍の Multi-channel APD を示しており、図 4.7 (c), (d) は RO_2 の発振周波数の APD を示したものである。このとき、妨害波印加時の発振周波数は印加した正弦波の影響を受けて、妨害波非印加時に比べて変化している。図 4.7 (e), (f) は TRNG の出力ビット列であり、左上を 1 ビット目、右下を 512 ビット目として、縦軸方向に連続した 16 ビットを



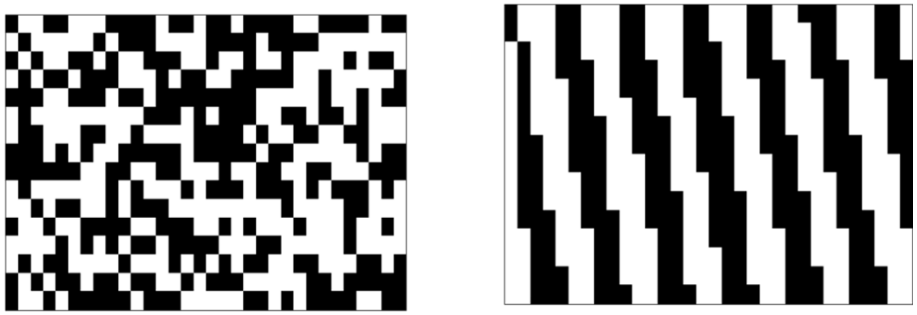
(a) 電気的外乱非印加時の Multi-channel APD 波形

(b) 電気的外乱印加時の Multi-channel APD 波形



(c) 電気的外乱非印加時の APD 波形

(d) 電気的外乱印加時の APD 波形



(e) 電気的外乱非印加時の出力ビット

(f) 電気的外乱印加時の出力ビット

図 4.7: 電気的外乱による RO の APD 波形の変化と出力ビットの変化

32 列並べ、1 を黒、0 を白としたヒートマップで表している。また、RO_1 の振幅確率の分布は RO_2 のものと同様の概形であったため、ここでは省略した。妨害波非印加時は位相雑音により発振周波数近傍の振幅が大きく変動し、どの周波数に対しても振幅の分布が広がっていることが確認できる（図 4.7 (a)）。このとき、発振周波数における APD の変化（図 4.7 (c)）は、振幅値が増えるにしたがって緩やかなカーブを描いて、閾値を超える時間確率（Exceedance Probability）が低下していることが確認できる。また、生成されたビット列に明確な乱数性低下は確認されなかった（4.7 (e)）。続いて、妨害波を印加したときは、位相雑音の低下によって振幅確率の分布の広がりが抑制され、特に発振周波数近傍において、振幅確率がほぼ一点に収束していることが確認できる (図 4.7 (b))。この変化は発振周波数における APD の変化でも確認でき、振幅値に対して、その閾値を超える時間確率が急峻に変化していることが確認できる（図 4.7 (d)）。このとき、TRNG が生成したビット列は、周期性を持つことが確認できる（図 4.7 (f)）。

本実験では、ERO-TRNG に対して複数の信号源を用いて電気的外乱を印加することで TRNG の乱数性を低下させる周波数注入攻撃を行うと共に、攻撃による RO のエントロピー低下が RO の APD として観測可能であることを実証した。TRNG を構成する RO に対して APD 測定を行うことで、TRNG の乱数性を評価できる可能性があり、TRNG に対する攻撃耐性評価手法として適用できる可能性がある。

4.3 放射電磁波による情報漏えいが引き起こす TRNG の予測不可能性への影響評価

本節では、機器外部からの放射電磁波の観測により、TRNG の出力ビットを推定可能であるかについて評価を行う。

乱数の予測不可能性の低下は、秘密情報の推定が容易になることから、暗号デバイスにおけるセキュリティを大きく低下させる可能性がある。実際に、予測不可能性の低い RNG を使用したことによって暗号システムに脆弱性が生じ、機密性が低下したことが報告されている [4, 5, 6]。ハードウェア上に実装された RNG

の予測不可能性に対する攻撃として、Markus による理論研究が存在する [59]。この研究では、以下の二つの要因によって、ある RNG の出力が予測可能であることを示した。

1. RNG のエントロピーが低い
2. RNG のエントロピーを低下させる情報が取得可能である

これらの要因によって、RNG のエントロピーは、設計時に想定されたエントロピーを大きく下回る可能性が示され、予測不可能性に対する攻撃が成立し得ることが報告された。これに対して、現在では TRNG のエントロピーを評価することが強く要求されている。既に、TRNG の設計に対する米国のセキュリティ基準である NIST SP800-90B [39] では、エントロピー源が予測不可能であることの証明が要求されている。また、ドイツ情報セキュリティ庁（BSI）が定めたヨーロッパのデファクトスタンダードである AIS-20/31 [40] では、TRNG に対してエントロピー源の確率モデルを定式化するように要求している。既に、論理ゲートのみで構成可能であることから、広く開発・利用されている RO をエントロピー源とする TRNG では、エントロピー源の確率モデルが定式化された設計が複数報告されている。なかでも、TERO-based TRNG は、RO をエントロピー源とする TRNG のなかで、高いエントロピーを持つ乱数を高速に生成可能であることから、広く利用されている TRNG の一つである。この TERO-based TRNG に対してもエントロピー源である物理過程を反映した確率モデルがたてられていることから、出力に十分なエントロピーを持つことが数学的に保証されている。そのため、TERO-based TRNG は高い予測不可能性を持つと考えられている。

しかし、これらの設計指針や確率モデルに対する評価は上述の一つ目の要因に対するものであり、二つ目の要因については十分に評価されていない。後者の要因を評価するには、TRNG のエントロピーを低下させる情報が漏えいするモデルの構築や出力ビットを推定する解析手法が必要である。そのため、前者に比べて評価が難しく、これまで RO をエントロピー源とする TRNG に対して、TRNG のエントロピーを低下させる情報の取得を行った研究は少ない [35, 36, 37]。また、[36] の研究は TRNG に対する電磁波印加によって乱数の一様性を低下させることを目的としており、予測不可能性については評価されていない。

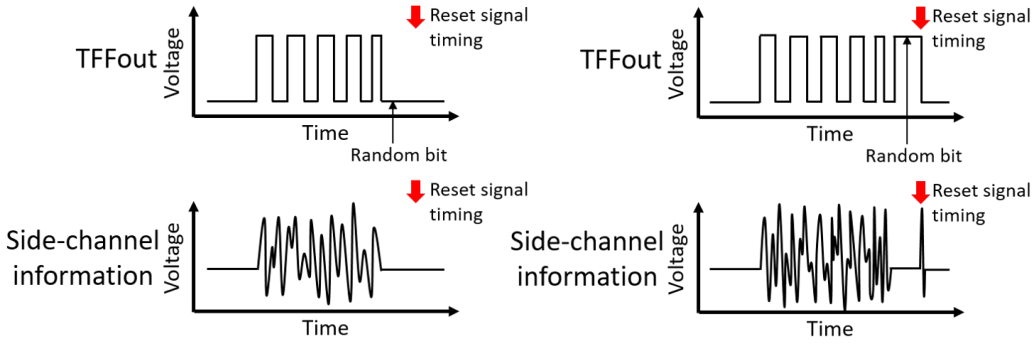
一方、ハードウェア上に実装された暗号アルゴリズムに対して、機器の動作時に副次的に発生するサイドチャネルリーケージを利用することで、秘密鍵の情報を取得するサイドチャネル攻撃が知られている [28, 29, 30, 61, 62]。暗号処理時には、消費電力や放射電磁波は計算内容によって変化することから、これを情報漏えい元としてモデルをたてることで、秘密鍵の解析を行う。この消費電力や放射電磁波の変化によるサイドチャネルリーケージは TRNG に対しても生じる可能性があり、仮にサイドチャネル攻撃によって TRNG の出力が推定できた場合、暗号システム全体のセキュリティが大きく低下する可能性がある。

本節では、暗号ハードウェアで広く利用されている TERO-based TRNG に対する非侵襲なサイドチャネル攻撃によって、TRNG の予測不可能性を低下させ、出力ビットを推定する手法について検討を行う。具体的には、TRNG の出力ビットを示すサイドチャネル情報の漏えいモデルを構築し、磁界プローブによって非侵襲にサイドチャネル情報を計測する手法を示す。そして、サイドチャネル情報から出力ビットを推定する手法を提案する。また、本提案手法による予測不可能性に対する攻撃は、TERO-based TRNG を実装した暗号ハードウェアのセキュリティを大きく低下させる可能性があることから、本攻撃に対する回路レベルの対策手法についても検討を行う。

4.3.1 関連研究

RO をエントロピー源とする TRNG に対するサイドチャネル攻撃として、[37] が存在する。この攻撃は周波数注入攻撃のための攻撃パラメタを取得することを目的として、localized EM analysis によってチップ上の RO の位置とその発振周波数の取得を実現した。そのため、この攻撃では乱数の一様性の低下を目的としており、予測不可能性に対する検討は行われていなかった。

一方、PUF（Physically Unclonable Function）に対する攻撃の一つに、TERO を利用した PUF の PUF bits をサイドチャネル攻撃によって推定する攻撃手法が提案されている [60]。この攻撃では、TERO の EM 放射から TERO の振動回数の推定を行うことで、PUF のエントロピーを低下させている。しかし、この推定手法はノイズの大きい振動回数の最下位ビットに適用することは困難である。その



(a) 出力ビット: 0　　(b) 出力ビット: 1

図 4.8: TFF 出力波形とサイドチャネル情報

ため、振動回数の最下位ビットを利用する TERO-based TRNG に対して [60] の手法によって、乱数列を推定することは難しい。

4.3.2 TRNG の出力ビットを反映した漏えいモデル

TERO-based TRNG の出力ビットを含んだサイドチャネル情報の漏えい原理について概説した後、漏えいしたサイドチャネル情報を非侵襲に計測する手法を提案する。

暗号ハードウェアに対するサイドチャネル攻撃では、計算内容に応じた CMOS ゲートにおける消費電力の変化をサイドチャネル情報として計測することで鍵解読が可能である [28]。このことから、TRNG における出力ビットの変化が、CMOS ゲートにおける消費電力の変化として反映される漏えいモデルをたてることができれば、サイドチャネル情報によって出力ビットを推定できる可能性が高い。

図 4.8 に示すように、T flip-flop へのリセット信号の入力は、出力ビットに応じて回路の動作が変化する。図 4.8 (a) のように、リセット信号入力前の T flip-flop の出力が Low、つまり出力ビットが 0 であった場合、リセット信号入力時に、T flip-flop の出力は変化しない。これは CMOS ゲートにスイッチングが生じないため、消費電力が小さいことを示す。一方、リセット信号入力前の T flip-flop の出力が High、つまり出力ビットが 1 であった場合、リセット信号入力時に、T flip-flop の出力が変化する。これは、リセット信号の入力によって CMOS ゲートに High

からLowへのスイッチングが生じ、放電が生じていると考えられる。このことから、リセット信号入力時のT flip-flopの消費電力は出力ビットを示すサイドチャネル情報の漏えい元になると考えられる。このような急峻な消費電力の変化は電磁界によって機器外部から観測できる可能性がある。消費電力の変化は電磁界で観測した場合、微分信号として観測される。そのため、T flip-flopの出力信号の電圧値に関わらず、スイッチングによる急峻な変化が電磁界においてピークとして観測される。そのため、出力ビットが0の時は（図4.8 (a)）、CMOSゲートのスイッチングが生じないため、電磁界ではピークが観測されない。一方、出力ビットが1の時は（図4.8 (b)）、CMOSゲートのスイッチングによる急峻な変化によって、電磁界でピークが観測される。電磁界におけるこのようなピークの振幅値の強度は、元の信号の立ち上がりの鋭さに依存して決定される。そのため、ノイズが大きい環境においても電磁波を計測することで、TRNGの出力ビットに対応したサイドチャネル情報が取得できる可能性がある。

4.3.3 サイドチャネル情報の解析による出力ビット推定

TRNGの出力ビットを反映するサイドチャネル情報は、T flip-flopにリセット信号が入力された時の振幅値の変化として反映される。そのため、計測したサイドチャネル情報からリセット信号が入力されるタイミングを推定することができれば、TRNGの出力ビットを推定可能であると考えられる。以下では、サイドチャネル情報の解析によって、リセット信号が入力されるタイミングを推定し、振幅値を利用することで出力ビットを推定する手法を提案する。電磁界計測によるサイドチャネル情報には、前節で示した出力ビットに対応するデータと共に、TERO発振時のカウンタのスイッチングも観測可能である。[60]では、TEROの発振をサイドチャネル情報の変化から解析することで振動回数の推定を行っている。図4.8に示すようにTEROが発振し、T flip-flopの出力信号が変動している場合は、充放電が繰り返されることから、サイドチャネル情報においても大きな振幅の変化が観測される。そして、TEROが安定状態に遷移し、T flip-flopの出力信号の振動が停止することで、このサイドチャネル情報の変化は小さくなる。このサイドチャネル情報の変化は一時的なピークではなく、図4.8に示すように

連続した振幅値の増大として表れることから、TERO の発振開始を推定することは容易であると考えられる。続いて、リセット信号の入力タイミングについて述べる。リセット信号は前節で示したように、クロックによって生成され、TERO の発振開始から一定時間後に T flip-flop がリセットされる。そのため、事前に攻撃対象のデバイスをプロファイリングし、TERO の発振開始からリセット信号入力までの時間を取得することで、TRNG の出力信号を反映する振幅値の変化を推定可能であると考えられる。このとき、出力ビットに応じて振幅値の大きさが変化することから、サイドチャネル情報の振幅に対して閾値を設けることで出力ビットの識別を行う。リセット信号入力時におけるサイドチャネル情報の振幅が閾値を超えた場合は出力ビットを 1、閾値を超えなかった場合は出力ビットを 0 と推定する。

4.3.4 実験セットアップ

実験に使用した FPGA の実装を説明する（図 4.9）。FPGA は UART モジュールを介して PC からコマンドを受信することで、TRNG が動作を開始し、512 ビットの連続した乱数を生成した後、出力ビット列を UART モジュールから PC に送信する。TERO を制御する信号は 11 段の RO と 8 段の非同期カウンタによって生成されるクロックである。クロックの立ち上がりに応じて TERO の発振が開始し、クロックの立下りまでに安定状態に遷移する。また、クロックの立下り時に、T flip-flop にリセット信号が入力される。TERO は二つの NAND ゲートと 20 個のインバータから構成される。この TERO の発振回数を T flip-flop でカウントし、1 ビットの乱数を生成する。また、FPGA からは 512 ビットの乱数の生成開始を示すトリガ信号を I/O ピンから出力する。

図 4.10 に実験セットアップを示す。TERO-based TRNG を実装した FPGA を攻撃対象のデバイスとする。攻撃対象の FPGA には、Spartan6 LX9 Microboard を使用した。サイドチャネル情報は、チップ直上に設置した磁界プローブ（Langer EMV, RF-U 5-2）によって計測を行う、ローノイズアンプ（COSMOWAVE, LNA270WS）によって増幅した後、オシロスコープで観測した。また、FPGA は PC から USB ケーブルを通じて給電を行った。

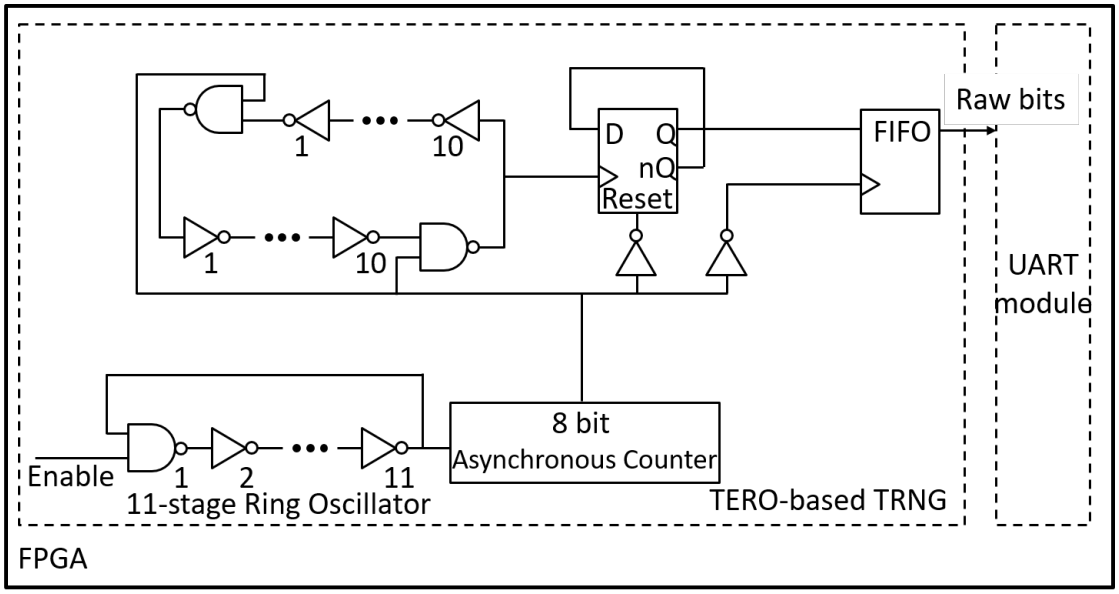


図 4.9: TERO-based TRNG の実装

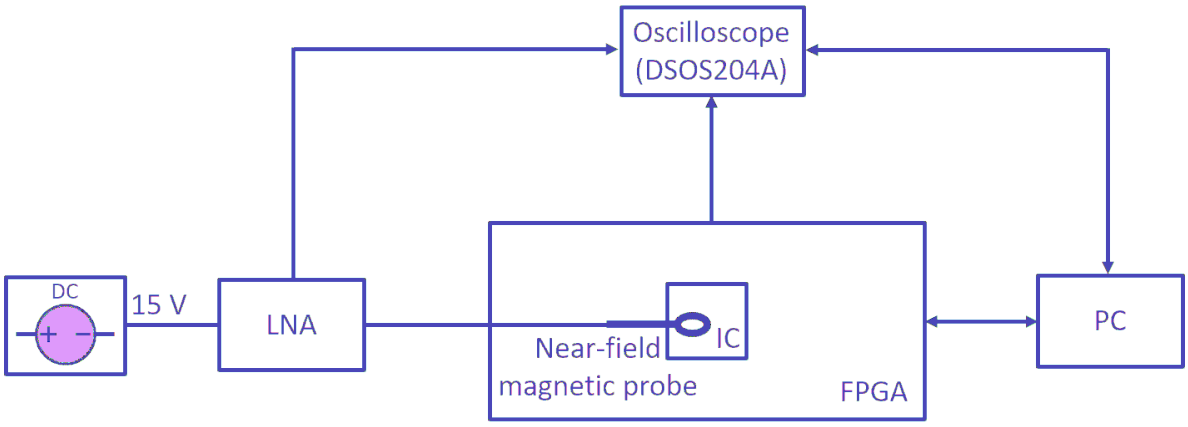


図 4.10: 実験セットアップ

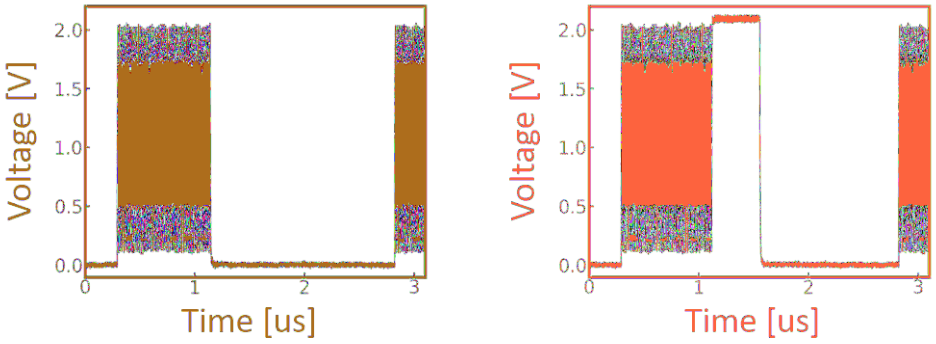
4.3.5 漏えいモデルの評価

続いて、リセット信号入力時における回路の動作の変化に対応したサイドチャネル情報の計測について述べる。TRNG の出力ビットに対応して、リセット信号入力時の T flip-flop の出力信号の動作が変化することを示し、この変化がサイドチャネル情報においても観測可能であることを示す。実験で使用した TERO-based TRNG は、127.56 MHz の発振周波数の TERO と 434.30 kHz のクロックを使用して、乱数を生成する。実験時には T flip-flop の出力信号を I/O ピンから出力した。

図 4.11, 4.12 に出力ビットが 0 の時と 1 の時にそれぞれ対応した T flip-flop の出力信号とサイドチャネル情報を示す。どちらの場合でも、TERO が振動し、T flip-flop の出力信号が変化しているときはサイドチャネル情報の振幅が大きく変化し、T flip-flop の出力信号が安定することでサイドチャネル情報の変動も減少することが確認される。図 4.11 (a) のように、出力ビットが 0 の時は TERO の発振が収束した後、T flip-flop の出力信号は Low となっている。このとき、リセット信号の入力よる T flip-flop の出力信号の変化は生じない。そのため、サイドチャネル情報においても振幅の変化は観測されない。一方、出力ビットが 1 の時は TERO の発振が収束した後、T flip-flop の出力信号は High となる（図 4.11 (b)）。このとき、リセット信号の入力によって T flip-flop の出力信号は Low に立下り、放電が生じる。また、サイドチャネル情報では T flip-flop の出力信号の変化を反映した振幅値の変化が生じ、ピークが観測される (図 4.12 (b))。以上より、TRNG の出力ビットに応じたサイドチャネル情報の振幅値の変化を観測可能であることを示した。

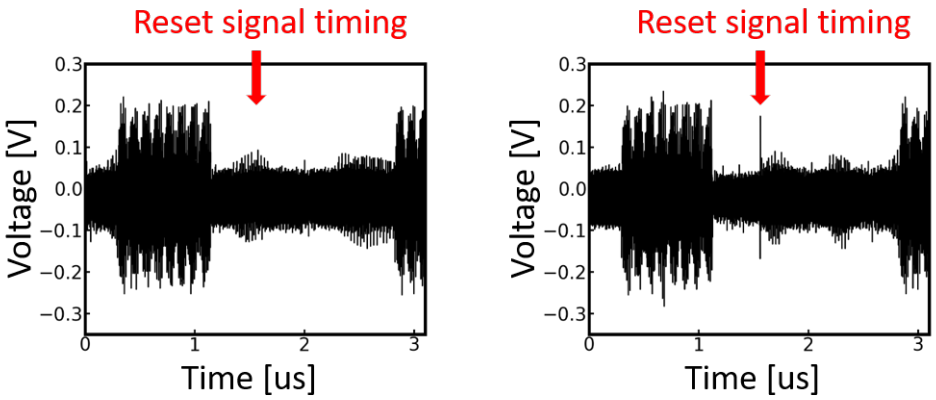
4.3.6 サイドチャネル情報を利用した出力ビット推定

本節では、実際のデバイスを模した環境下においても出力ビットに対応したサイドチャネル情報の変化が観測可能であることを示した後、サイドチャネル情報を利用した出力ビット推定を行う。具体的には、リセット信号入力時のサイドチャネル情報の振幅値の分布が TRNG の出力ビットに対応して変化することを示した後、連続した 512 ビットの乱数列に対して、出力ビットの推定を行う。



(a) 出力ビット: 0　　(b) 出力ビット: 1

図 4.11: 出力ビットに対応する TFF 波形



(a) 出力ビット: 0　　(b) 出力ビット: 1

図 4.12: 出力ビットに対応するサイドチャネル波形

攻撃に使用した TRNG は、実際のデバイスを模擬するために TRNG の出力に関わる信号を外部に出力しないような実装を行った。具体的には、TERO の出力信号や T flip-flop の出力信号、クロック信号は I/O ピンへと出力せず、512 ビットの乱数生成の開始を示すトリガ信号のみ I/O ピンから出力を行った。そのため本実験での構成では、I/O によるサイドチャネル情報の漏えいは生じていないと考えられる。また、生成した 512 ビットの乱数を PC へと送信する UART モジュールは TRNG が乱数の生成を終了した後に動作を開始するため、UART 通信による出力ビットの漏えいは、本実験環境下では存在しないと考えられる。

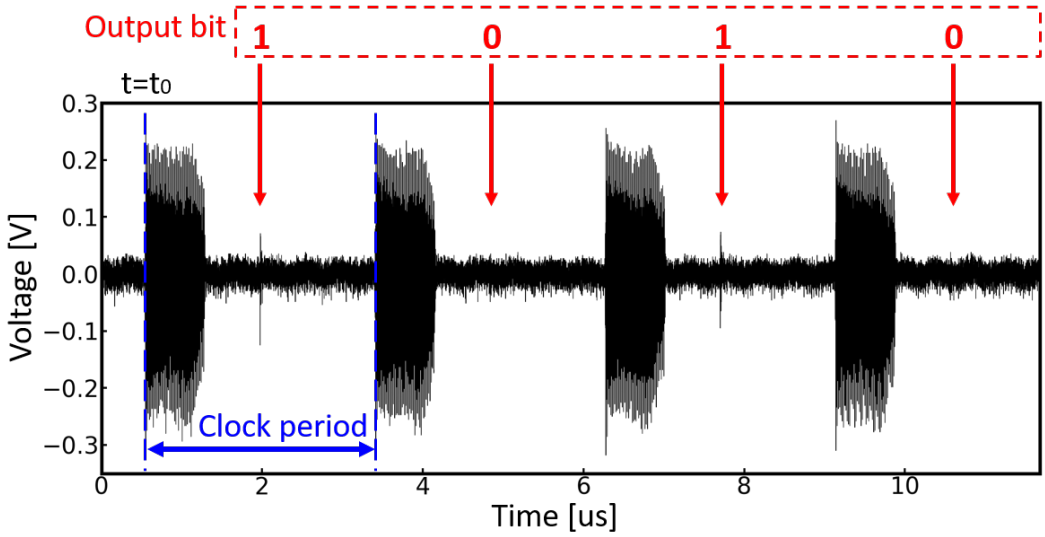
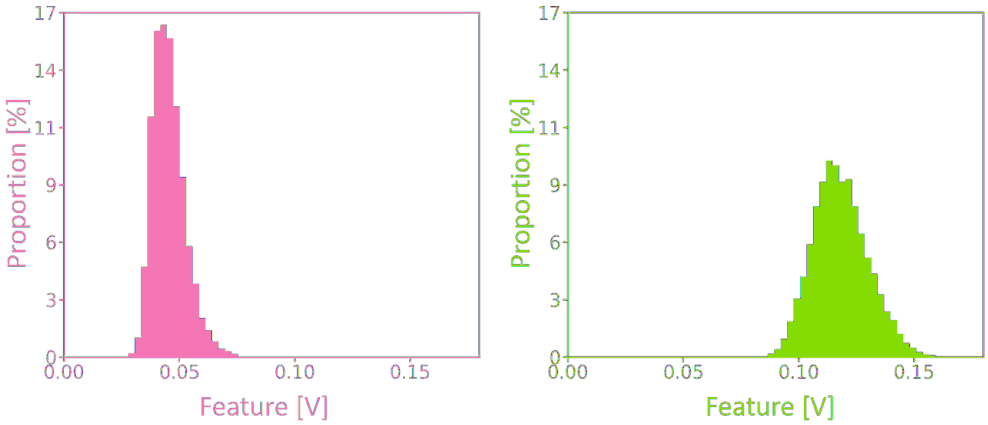


図 4.13: 出力ビットとサイドチャネル情報

図 4.13 に TERO-based TRNG の乱数生成時のサイドチャネル情報と UART モジュールから取得した出力ビットを示す。図 4.12 に示したサイドチャネル情報と同様に、TERO の振動や T flip-flop の出力信号の振動を示したサイドチャネル情報の変化が観測された。このことから、図 4.13 に示した矢印の区間が TERO を制御するクロックの 1 周期であると予測され、この区間において TRNG は 1 ビットの乱数生成を行っていると考えられる。また、本実験で使用した TRNG の構成では、クロックの立下りによってリセット信号が入力されるため、赤矢印で示した時間においてリセット信号が入力され、出力ビットに対応したサイドチャネ



(a) 出力ビット: 0　　(b) 出力ビット: 1

図 4.14: 出力ビットに応じた特徴量の分布

ル情報の変化が生じていると考えられる。図 4.13 に示した例では、リセット信号が入力された時にピークが立っているものについては、UART モジュールから取得した出力ビットが 1 となり、ピークが存在しないものについては出力ビットが 0 となっていることが確認できる。これは前節で観測した出力ビットに応じた T flip-flop の変化をサイドチャネル情報が反映し、サイドチャネル情報から出力ビットが推定可能であることを示す。

続いて、出力ビットに対応した振幅値の分布について評価を行った。連続した 512 ビットの乱数生成を 100 回繰り返し、オシロスコープによるサイドチャネル情報の計測と UART モジュールから 51,200 ビットの乱数の取得を行った。出力ビットが 1 の時にサイドチャネル情報に生じたピークは、波形の平均値に対してプラス方向とマイナス方向どちらにも存在していることから、取得したサイドチャネル情報に対して、波形の平均値を減算し、絶対値を取ることで補正を行った。続いて、TERO の発振開始（$t = t_0$）を検出し、これに対してリセット信号が入力されると予想される区間 $[t_0{+}1.42\ \text{ns}, t_0{+}1.46\ \text{ns}]$ における補正したサイドチャネル情報の振幅値の最大値を特徴量として 51,200 データ取得した。そして、UART モジュールで取得した出力ビットに対応する特徴量の分布を図 4.14 に示した。図は横軸に特徴量、縦軸に割合を示したヒストグラムである。出力ビットが 0 の時

は特徴量 0.082 V 以下に分布しているのに対して、出力ビットが 1 の時は特徴量が 0.082 V 以上に分布していることが確認される。このことから、出力ビットに対応してサイドチャネル情報の振幅値が大きく変化し、この特徴量を用いることで出力ビット推定が可能であると考えられる。

最後に、サイドチャネル情報を利用することで TRNG の出力ビットが推定可能であることを示すため、連続した 512 ビットの乱数列に対して、出力ビットの推定を行った。実験では、512 ビットの乱数生成を 100 回繰り返し、サイドチャネル情報と UART モジュールからの乱数列取得を行った。そして、サイドチャネル情報に対して先ほどと同様の補正と特徴量の取得を行った。この特徴量に対して閾値を 0.08 と設定し、閾値以上の場合は出力ビットを 1 とし、閾値未満であれば出力ビットを 0 と推定した。推定を行った全てのデータに対して 512 ビットの乱数を完全に推定することに成功した。

以上より、実際のデバイスを模した環境において、サイドチャネル情報を利用しすることで、TERO-based TRNG の出力ビットを推定可能であることを実証した。

4.3.7 本攻撃に対する対策手法の提案

提案した TERO-based TRNG に対する出力ビット推定攻撃に対する対策手法について検討を行う。まず、一般的な TRNG の構成における本提案手法の実現可能性を検討した後、回路レベルでの対策技術を提案し、攻撃に対する耐性評価を行う。

2 章で説明したように、TRNG に対して乱数性を検証する Health test や TRNG が出力した Raw bit の乱数性を向上させる Post-processing の実装が推奨されている。Health test にはエントロピー源を評価するテスト [63, 64] や TRNG の出力ビットを評価する Health test[65, 66] など、様々な Health test が提案されてきた。しかし、今回提案したサイドチャネル情報を利用した予測不可能性に対する攻撃では、デバイスに対して非侵襲にサイドチャネル情報を取得するため、エントロピー源や出力ビット列に影響を及ぼさないことから、Health test による攻撃の検知は困難であると考えられる。そのため、Health test を実装した機器に対し

ても本提案手法は有効であると考えられる。

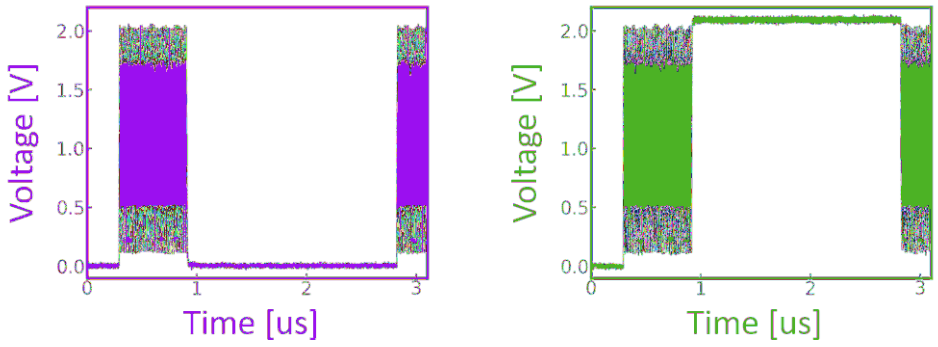
また、Post-processing が存在した場合についても、前章で示したように連続した 512 ビットの乱数列全てを推定可能であることから、Post-processing の実装が判明している場合、Post-processing 後の乱数列に対しても推定ができる可能性がある。このことから、一般的な TRNG の構成に対しても本提案手法による出力ビット推定は実現する可能性があり、従来の Health test による対策とは異なる対策を実装する必要があると考えられる。

本提案手法は電気的な情報漏えいを電磁界で観測することによってサイドチャネル攻撃を実行していることから、アルゴリズムやゲートレベルでの対策によって、出力ビットを反映するサイドチャネル情報の漏えいを抑制することが考えられる。本節では、その一例として、TERO-based TRNG のサイドチャネル情報の漏えい元を抑制するような回路実装を提案する。本節で提案した攻撃手法では、出力ビットに対する T flip-flop にリセット信号が入力された時の回路の動作の違いを利用して出力ビット推定を行っている。そのため、出力ビットに応じて T flip-flop の動作が変化しないような回路構成にすることが考えられる。具体的には、リセット信号による T flip-flop のリセット自体を除くことで、CMOS からの放電が生じず、出力ビットを反映したサイドチャネル情報が観測されなくなると考えられる。このとき、出力される乱数列は振動回数の偶奇によって、1 ビット前の出力に対して反転するかどうかが決まる。カウンタのリセット信号の有無により、TERO の確率モデルは変化しないと考えられることから、リセット信号を除いたことによる乱数性の低下は生じないと考えられる。

4.3.8 対策技術を実装した TERO-based TRNG に対するサイドチャネル情報の観測

前節で提案した対策技術を実装した TERO-based TRNG に対して、T flip-flop の出力信号の観測とサイドチャネル情報の観測を行い、出力ビットに対応した回路動作の変化がサイドチャネル情報として観測困難であることを示す。

本節で評価に使用した TERO-based TRNG は 4.3.5 節で評価に用いたものと同様の実装であり、FPGA 上に存在する物理スイッチと AND ゲートによってリセッ



(a) 出力ビット: 0　　(b) 出力ビット: 1

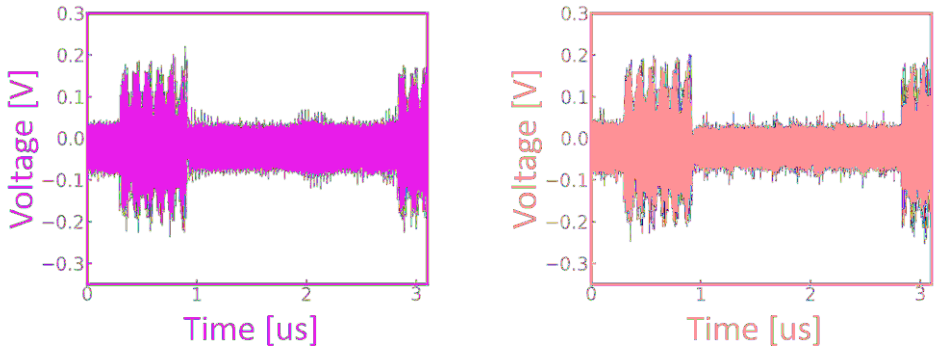
図 4.15: 対策実装時の出力ビットに対応する TFF 波形

ト信号の動作を制御したものである。実験で使用した TERO-based TRNG は、127.56 MHz の発振周波数の TERO と 434.30 kHz のクロックを使用して、乱数を生成する。実験では、512 ビットの乱数生成の開始を示すトリガ信号と T flip-flop の出力信号を I/O ピンから出力しオシロスコープで観測を行った。サイドチャネル情報は、チップ直上に設置した磁界プローブによって取得した。

図 4.15, 4.16 に出力ビットが 0 の時と 1 の時にそれぞれ対応した T flip-flop の出力信号とサイドチャネル情報、出力ビットを示す。出力ビットは TERO が安定状態に遷移した後の T flip-flop の出力が High であれば 1 となり、Low であれば 0 となる。T flip-flop の出力はリセット信号が存在しないため、TERO の安定状態への遷移から次の TERO の発振開始まで同じ値を保持し続けていることが観測される。このとき、サイドチャネル情報は TERO やカウンタの発振を反映した振幅値変化の増大は観測されるが、前章で見られたようなリセット信号による振幅値の変化は観測されない。これにより、出力ビットに対応したサイドチャネル情報の取得が困難化していることが確認された。

4.3.9 対策技術を実装した TRNG に対する攻撃の実現可能性の評価

続いて、提案した対策技術の実装により、本論文で提案した出力ビット推定攻撃が無効化されることを示す。具体的には、4.3.6 節同様の手法を用いてサイド



(a) 出力ビット: 0　　(b) 出力ビット: 1

図 4.16: 対策実装時の出力ビットに対応するサイドチャネル波形

チャネル情報を観測し、特徴量を抽出することで出力ビットを推定可能であるかについて評価を行う。

本節で評価に使用した TERO-based TRNG は 4.3.6 節で攻撃に用いたものと同様の実装であり、FPGA 上に存在する物理スイッチと AND ゲートによってリセット信号の動作を制御したものである。実験では、512 ビットの乱数生成の開始を示すトリガ信号を I/O ピンから出力し、チップ直上に設置した磁界プローブによってサイドチャネル情報を取得した。

図 4.17 に TERO-based TRNG の乱数生成時のサイドチャネル情報と UART モジュールから取得した出力ビットを示す。図 4.16 に示したサイドチャネル情報と同様に、TERO の振動や D-filpflop の出力信号の振動を示したサイドチャネル情報の変化が観測された一方、リセット信号の入力時（図 4.16 赤矢印）におけるサイドチャネル情報の振幅値の変化は観測されていないことが確認できる。

続いて、出力ビットに対応した振幅値の分布について評価を行った。連続した 512 ビットの乱数生成を 100 回繰り返し、オシロスコープによるサイドチャネル情報の計測と UART モジュールから 51,200 ビットの乱数の取得を行った。特徴量として使用した振幅値の評価手法は 4.3.6 節と同様である。図 4.18 に UART モジュールで取得した出力ビットに対応する特徴量の分布を示す。出力ビットが 1 のときの特徴量の分布と出力ビットが 0 の時の出力ビットの分布が同様の概形を

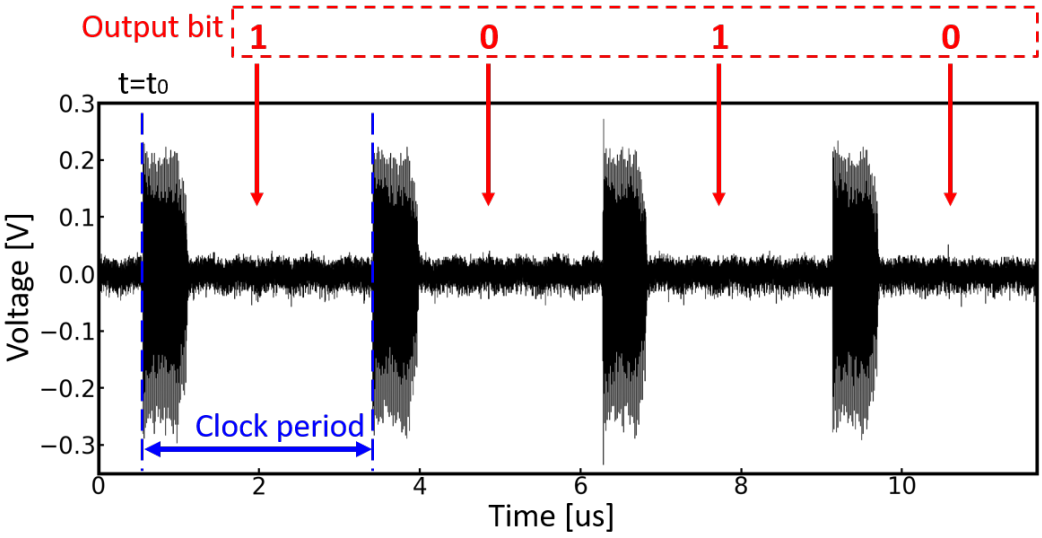
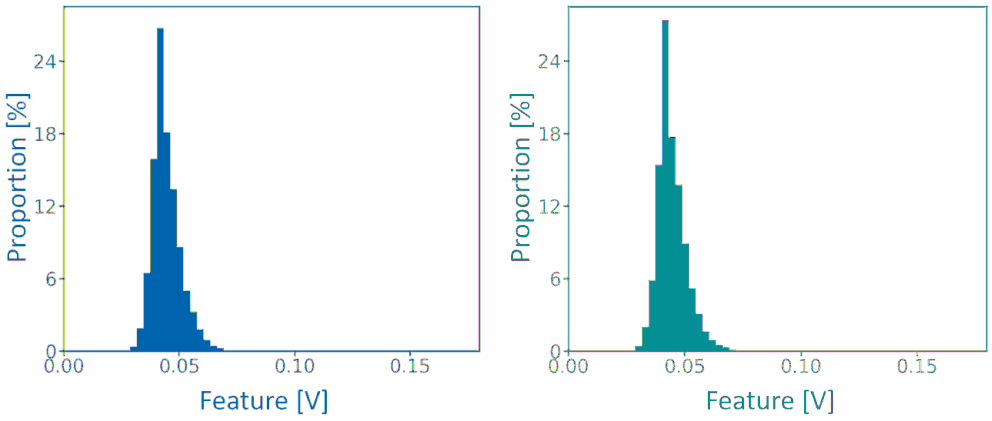


図 4.17: 対策実装時の出力ビットとサイドチャネル情報



(a) 出力ビット: 0　　(b) 出力ビット: 1

図 4.18: 対策実装時の出力ビットに応じた特徴量の分布

取ることが確認できる。これにより、任意の閾値をとったとしても出力ビットを推定することは困難であると考えられる。また、特徴量は図 4.14 に示したものに比べて小さく、本章で提案した対策によってサイドチャネル情報の変化が抑制されたことが確認できる。

以上より、本章で提案した対策技術の実装によって TERO-based TRNG の出力ビットを示すサイドチャネル情報の漏えいを抑制可能であると考えられる。

4.4 結言

本章では、漏えい情報が TRNG の予測不可能性に与える影響に対して評価を行った。エントロピー源となるオシレータのエントロピー評価として、APD 測定を利用したエントロピー評価手法を提案し、実験を通じて、周波数注入攻撃による TRNG の乱数性の低下が、APD 測定によって RO のエントロピーの低下として推定できる可能性を示した。周波数注入攻撃では、印加した電磁波によってエントロピー源となる RO の発振がロックされる現象を利用しているため、攻撃によって RO の発振周波数が変化する可能性がある。そのため、実験で示したように Multi-channel APD による評価と RO の発振周波数における APD の評価を組み合わせることで、効率良く RO のエントロピーを評価できると考えられる。

また、TRNG から生じる情報漏えいに対する予測不可能性の低下を評価するために、出力ビットの推定を行った。機器外部から出力ビットに応じて変化する T flip-flop を漏えいモデルとして利用することで、出力ビットに依存した回路動作の変化を反映した電磁放射の計測によって、出力ビットが高い精度で推定可能であることを示した。

5. 結論

本論文の各章のまとめは以下のとおりである。

1 章では、情報通信技術の発展に伴うセキュリティが重要となるデバイスの拡大について述べたのちに、暗号プリミティブの一つである真正乱数生成器の重要と、脆弱性への影響について述べた。そして、TRNG に対する従来研究の問題について述べたのちに、本論文が取り組む課題と目標について述べた。

2 章では、TRNG の概要と暗号モジュールに対する物理攻撃について基礎的な概要を述べ、電気的外乱を使用した物理攻撃に対して TRNG のセキュリティ評価を行うことを示した。

3 章では、電気的外乱を使用した物理攻撃が TRNG の一様性・再現不可能性に与える影響について評価を行った。電気的外乱によるエントロピー源への影響の評価を行うために、機器外部から非侵襲に電気的外乱を与えることで、一様性を統計的に有意に低下可能であることを実証した。更に、電気的外乱はエントロピー源に対して、時間方向に高い分解能で影響を与えることが可能であることから、TRNG の出力ビットを操作可能な外乱を一時的に与えることで一様性・再現不可能性を低下可能であることを示した。

4 章では、TRNG から生じる漏えい情報が予測不可能性に与える影響について評価を行った。まず、オシレータのエントロピー低下を評価する技術について検討を行い、APD 測定によって、周波数領域においてもエントロピーを評価できる可能性について示した。更に、機器外部から出力ビットに応じた回路動作の変化を取得することで Digitization 部分から乱数ビットを取得可能な漏えいモデルを提案し、実験により TRNG の電磁放射を観測することで出力ビットを推定可能であることを示した。

本論文では、TRNG のセキュリティ評価を行う上で重要である、物理攻撃への乱数性の影響評価を行った。オシレータベースの TRNG に対する電気的外乱と漏えい情報が一様性・再現不可能性・予測不可能性に与える影響について評価を行い、実験によりこれらの乱数性が低下することを示した。本論文で扱った TRNG の乱数性評価は TRNG のモデルとして重要な、エントロピー源とデジタル化処理を評価したものである。そのため、今後の課題として Health test や Post-processing も

含めて TRNG の物理攻撃に対する乱数性への影響評価を行うことが求められる。また、本研究ではオシレータを使用した TRNG に対する乱数性評価を行ったが、他の TRNG に対してもエントロピー源への電気的外乱や漏えい情報による乱数性の低下が実現する可能性がある。このことから、オシレータを使用した TRNG 以外の TRNG に対しても、本論文で扱った一様性・再現不可能性・予測不可能性への物理攻撃による影響評価は有効であると考えられる。また、セキュリティにおける乱数性は重要であり、乱数性の低下による暗号の危殆化が問題視されることから、暗号プロトコルにおける乱数の使用方法（暗号鍵生成、ノンス、ワンタイムパッド等）も含めた、TRNG の安全性評価が重要となると考えられる。

謝辞

末筆ながら、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。ここに心より感謝申し上げます。

本学岡田実教授及び中島康彦教授には、研究を進めるにあたり有益なご助言・ご討論を頂き、心より御礼申し上げます。

本学藤本大介助教、Kim Youngwoo 助教には、研究方針の策定や、研究活動においての多くのご支援、ご助言を賜り、学会参加においても多大なご支援をいただきました。厚く御礼申し上げます。

国立研究開発法人産業技術総合研究所松本勉教授、川村信一様をはじめとするサイバーフィジカルセキュリティ研究センターの皆様には、研究活動や論文執筆においての多くのご支援を頂き、厚く御礼申し上げます。

ルーヴァン・カトリック大学 Ingrid Verbauwhede 教授とそのグループの皆様には、研究活動においての多くのご支援と研究を進めるにあたり有益なご助言・ご討論を頂き、厚く御礼申し上げます。

最後に、日ごろの研究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 2 年版情報通信白書” ，2020. [Online]. Available: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.pdf, last accessed: 2021/12/22.

[2] 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.

[3] 電子情報通信学会知識ベース.“1 群（信号・システム）-3 編（暗号理論）-14 章 サイドチャネル攻撃と耐タンパー技術,” 2019.07.05, [Online]. Available: https://www.ieice-hbkb.org/files/01/01gun_03hen_14.pdf, Last accessed: 2021/12/22.

[4] L. Bello, ”DSA-1571-1 openssl – predictable random number generator,” Debian Security Advisory (2008), [Online]. Available: http://www.debian.org/security/2008/dsa-1571, last accessed 2019/12/11.

[5] S.D. Simone, ”Poor Random Number Generation Makes 1 in Every 172 RSA Certificates Vulnerable,” InfoQ, [Online]. Available: https://www.infoq.com/news/2019/12/rsa-iot-vulnerability/, last accessed 2021/11/20.

[6] D. Petro and A. Cecil, ”You’re Doing IoT RNG,” Bishop Fox, https://bishopfox.com/blog/youre-doing-iot-rng, last accessed 2021/11/20.

[7] Rohe, M. 2003.“RANDy-A True-Random Generator Based on Radioactive Decay.” Technical report, Saarland University, pp.1-36, 2003.

[8] Gisin, Nicolas, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. 2002.“Quantum Cryptography.” Reviews of Modern Physics 74 (1): 145–95.

[9] Scarani, Valerio, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. 2009. “The Security of Practical Quantum Key Distribution.” Reviews of Modern Physics 81 (3): 1301–50.

[10] Diamanti, Eleni, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. 2016. “Practical Challenges in Quantum Key Distribution.” Npj Quantum Information 2 (1): 1–12.

[11] Harayama, Takahisa, Satoshi Sunada, Kazuyuki Yoshimura, Peter Davis, Ken Tsuzuki, and Atsushi Uchida. 2011. “Fast Nondeterministic Random-Bit Generation Using on-Chip Chaos Lasers.” Physical Review. A 83 (3): 031803.

[12] Petrie, C. S., and J. A. Connelly. 2000. “A Noise-Based IC Random Number Generator for Applications in Cryptography.” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 47 (5): 615–21.

[13] Hu, Yue, Xiaofeng Liao, Kwok-Wo Wong, and Qing Zhou. 2009. “A True Random Number Generator Based on Mouse Movement and Chaotic Cryptography.” Chaos, Solitons & Fractals 40 (5): 2286–93.

[14] Camara, Carmen, Honorio Martín, Pedro Peris-Lopez, and Luis Entrena. undefined 2020. “A True Random Number Generator Based on Gait Data for the Internet of You.” IEEE Access 8: 71642–51.

[15] Sunar, Berk, William J. Martin, and Douglas R. Stinson. 2007. “A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks.” IEEE Transactions on Computers. Institute of Electrical and Electronics Engineers 56 (1): 109–19.

[16] Baudet, Mathieu, David Lubicz, Julien Micolod, and André Tassiaux. 2011. “On the Security of Oscillator-Based Random Number Generators.” Journal

of Cryptology. The Journal of the International Association for Cryptologic Research 24 (2): 398–425.

[17] Kohlbrenner, Paul, and Kris Gaj. 2004. “An Embedded True Random Number Generator for FPGAs.” In Proceedings of the 2004 ACM/SIGDA 12th International Symposium on Field Programmable Gate Arrays, 71–78. FPGA ’04. New York, NY, USA: Association for Computing Machinery.

[18] Fischer, Viktor, and Miloš Drutarovský. 2003. “True Random Number Generator Embedded in Reconfigurable Hardware.” In Cryptographic Hardware and Embedded Systems - CHES 2002, 415–30. Springer Berlin Heidelberg.

[19] Varchola, Michal, and Milos Drutarovsky. 2010. “New High Entropy Element for FPGA Based True Random Number Generators.” In Cryptographic Hardware and Embedded Systems, CHES 2010, 351–65. Springer Berlin Heidelberg.

[20] Valtchanov, Boyan, Alain Aubert, Florent Bernard, and Viktor Fischer. 2008. “Modeling and Observing the Jitter in Ring Oscillators Implemented in FPGAs.” In 2008 11th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems, 1–6. ieeexplore.ieee.org.

[21] Cherkaoui, Abdelkarim, Viktor Fischer, Alain Aubert, and Laurent Fesquet. 2013. “A Self-Timed Ring Based True Random Number Generator.” In 2013 IEEE 19th International Symposium on Asynchronous Circuits and Systems, 99–106. ieeexplore.ieee.org.

[22] Yang, Bohan, Vladimir Rožic, Miloš Grujic, Nele Mentens, and Ingrid Verbauwhede. 2018. “ES-TRNG: A High-Throughput, Low-Area True Random Number Generator Based on Edge Sampling.” IACR Transactions on Cryptographic Hardware and Embedded Systems, August, 267–92.

[23] Bagini, Vittorio, and Marco Bucci. 1999. “A Design of Reliable True Random Number Generator for Cryptographic Applications.” In Cryptographic Hardware and Embedded Systems, 204–18. Springer Berlin Heidelberg.

[24] Bucci, M., L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo. 2003. “A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC.” IEEE Transactions on Computers. Institute of Electrical and Electronics Engineers 52 (4): 403–9.

[25] Chen, Xiaoming, Lin Wang, Boxun Li, Yu Wang, Xin Li, Yongpan Liu, and Huazhong Yang. 2016. “Modeling Random Telegraph Noise as a Randomness Source and Its Application in True Random Number Generation.” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 35 (9): 1435–48.

[26] Jun, Benjamin, and Paul Kocher. 1999. “The Intel Random Number Generator.” Cryptography Research Inc. White Paper 27: 1–8.

[27] Fischer, Viktor, and David Lubicz. 2014. “Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG.” In Cryptographic Hardware and Embedded Systems – CHES 2014, 527–43. Springer Berlin Heidelberg.

[28] Kocher, Paul, Joshua Jaffe, and Benjamin Jun. 1999. “Differential Power Analysis.” In Advances in Cryptology — CRYPTO ’99, 388–97. Springer Berlin Heidelberg.

[29] E. Brier, C. Clavier and F. Olivier, “Correlation power analysis with a leakage model.” Cryptographic Hardware and Embedded Systems - CHES 2004, vol. 3156 of Lecture Notes in Computer Science, pp. 16–29, 2004.

[30] Hayashi, Yu-Ichi, Takeshi Sugawara, Yoshiki Kayano, Naofumi Homma, T. Mizuki, A. Satoh, T. Aoki, and S. Minegishi. 2009. “An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current.” IEICE Proceedings Series 14 (21P1-5).

[31] R. J. Anderson and M. G. Kuhn, "Low cost attacks on tamper resistant devices." in Proc. International Workshop on Security Protocols, pp. 125–136, 1998.

[32] D. Boneh, R. DeMillo, and R. Lipton, "On the importance of eliminating errors in cryptographic computations." Journal of Cryptology, vol. 14, no. 2, pp. 101–119, Nov. 2001.

[33] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in Proc. CRYPTO, pp. 513–525, 1997.

[34] Nakamura, Ko, Yu-Ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone. 2015. "Method for Estimating Fault Injection Time on Cryptographic Devices from EM Leakage." In 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), 235–40. ieeexplore.ieee.org.

[35] Markettos, A. Theodore, and Simon W. Moore. 2009. "The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators." In Cryptographic Hardware and Embedded Systems - CHES 2009, 317–31. Springer Berlin Heidelberg.

[36] Bayon, Pierre, Lilian Bossuet, Alain Aubert, and Viktor Fischer. 2016. " Fault Model of Electromagnetic Attacks Targeting Ring Oscillator-Based True Random Number Generators." Journal of Cryptographic Engineering 6 (1): 61–74.

[37] Bayon, Pierre, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. 2012. "Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator." In Constructive Side-Channel Analysis and Secure Design, 151–66. Springer Berlin Heidelberg.

[38] Cao, Yang, Vladimir Rožić, Bohan Yang, Josep Balasch, and Ingrid Verbauwhede. 2016. “ Exploring Active Manipulation Attacks on the TERO Random Number Generator. ” In 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), 1–4. ieeexplore.ieee.org.

[39] M.S. Turan, E. Barker and J. Kelsey, K. Mckay, M.Baish and M. Boyle, “ Recommendation for the entropy sources used for random bit generation, ” Technical Report SP800-90B, National Institute of Standards and Technology, USA, 2018.

[40] W. Killmann and W. Schindler. A proposal for: Functionality classes for random number generators, version 2.0. Technical report, Bundesamt fur Sicherheit in der Informationstechnik (BSI), Bonn, 2011.

[41] Rukhin, Andrew, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. 2001. “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. ” Booz-allen and hamilton inc mclean va. https://apps.dtic.mil/sti/citations/ADA393366.

[42] NIST, FIPS PUS 140-2, “Security requirements for cryptographic modules ”

[43] G. Marsaglia, “ DIEHARD, ” (http://stat.fsu.edu/ geo/diehard.html, http://stat.fsu.edu/pub/diehard/)

[44] Boneh, Dan, Richard A. DeMillo, and Richard J. Lipton. 1997. “ On the Importance of Checking Cryptographic Protocols for Faults. ” In Advances in Cryptology — EUROCRYPT ’ 97, 37–51. Springer Berlin Heidelberg.

[45] Petura, Oto, Ugo Mureddu, Nathalie Bochard, Viktor Fischer, and Lilian Bossuet. 2016. “ A Survey of AIS-20/31 Compliant TRNG Cores Suitable for FPGA Devices. ” In 2016 26th International Conference on Field Programmable Logic and Applications (FPL), 1–10. ieeexplore.ieee.org.

[46] McNeill, J. A. 1997. “Jitter in Ring Oscillators.” IEEE Journal of Solid-State Circuits 32 (6): 870–79.

[47] Mesgarzadeh, B., and A. Alvandpour. 2005. “A Study of Injection Locking in Ring Oscillators.” In 2005 IEEE International Symposium on Circuits and Systems, 5465–68 Vol. 6. ieeexplore.ieee.org.

[48] Hajimiri, A., S. Limotyrakis, and T. H. Lee. 1999. “Jitter and Phase Noise in Ring Oscillators.” IEEE Journal of Solid-State Circuits 34 (6): 790–804.

[49] Drewniak, J. L., Fei Sha, T. P. Van Doren, T. H. Hubing, and J. Shaw. 1995. “Diagnosing and Modeling Common-Mode Radiation from Printed Circuit Boards with Attached Cables.” In Proceedings of International Symposium on Electromagnetic Compatibility, 465–70. ieeexplore.ieee.org.

[50] Hockanson, D. M., J. L. Drewniak, T. H. Hubing, T. P. Van Doren, Fei Sha, and M. J. Wilhelm. 1996. “Investigation of Fundamental EMI Source Mechanisms Driving Common-Mode Radiation from Printed Circuit Boards with Attached Cables.” IEEE Transactions on Electromagnetic Compatibility 38 (4): 557–66.

[51] Hubing, Todd H. 2003. “Printed Circuit Board EMI Source Mechanisms.” https://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=2221&context=ele_comeng_facwork.

[52] Wada, Shinpei, Yuichi Hayashi, Daisuke Fujimoto, Naofumi Homma, and Youngwoo Kim. 2021. “Measurement and Analysis of Electromagnetic Information Leakage From Printed Circuit Board Power Delivery Network of Cryptographic Devices.” IEEE Transactions on Electromagnetic Compatibility 63 (5): 1322–32.

[53] Delvaux, Jeroen. 2019. “Refutation and Redesign of a Physical Model of TERO-Based TRNGs and PUFs.” IACR Cryptol. ePrint Arch. 2019: 810.

[54] Mureddu, Ugo, Nathalie Bochard, Lilian Bossuet, and Viktor Fischer. 2019. “Experimental Study of Locking Phenomena on Oscillating Rings Implemented in Logic Devices.” IEEE Transactions on Circuits and Systems. I, Regular Papers: A Publication of the IEEE Circuits and Systems Society 66 (7): 2560–71.

[55] Ker, Ming-Dou, and Kuo-Chun Hsu. 2003. “Latchup-Free ESD Protection Design with Complementary Substrate-Triggered SCR Devices.” IEEE Journal of Solid-State Circuits 38 (8): 1380–92.

[56] Wiklundh, K. 2006. “Relation between the Amplitude Probability Distribution of an Interfering Signal and Its Impact on Digital Radio Receivers.” IEEE Transactions on Electromagnetic Compatibility 48 (3): 537–44.

[57] Matsumoto, Yasushi, “On the Relation Between the Amplitude Probability Distribution of Noise and Bit Error Probability.” IEEE Transactions on Electromagnetic Compatibility 49 (4): 940-941

[58] Ishida, Kai, Sazu Arie, Kaoru Gotoh, Eisuke Hanada, Minoru Hirose, and Yasushi Matsumoto. 2018. “Electromagnetic Compatibility of Wireless Medical Telemetry Systems and Light-Emitting Diode (LED) Lamps.” Przeglad Elektrotechniczny 94 (2): 25–28.

[59] Dichtl, Markus. 2003. “How to Predict the Output of a Hardware Random Number Generator.” In Cryptographic Hardware and Embedded Systems - CHES 2003, 181–88. Springer Berlin Heidelberg.

[60] Tebelmann, Lars, Michael Pehl, and Vincent Immler. 2019. “Side-Channel Analysis of the TERO PUF.” In Constructive Side-Channel Analysis and Secure Design, 43–60. Springer International Publishing.

[61] Iokibe, Kengo, Tetsuo Amano, Kaoru Okamoto, and Yoshitaka Toyota. 2013. “Equivalent Circuit Modeling of Cryptographic Integrated Circuit for Infor-

mation Security Design.” IEEE Transactions on Electromagnetic Compatibility 55 (3): 581–88.

[62] Iokibe, Kengo, Tomonobu Kan, and Yoshitaka Toyota. 2020. “A Study on Evaluation Board Requirements for Assessing Vulnerability of Cryptographic Modules to Side-Channel Attacks.” In 2020 IEEE International Symposium on Electromagnetic Compatibility Signal/Power Integrity (EMCSI), 528–31. ieeexplore.ieee.org.

[63] Suresh, Vikram B., Daniele Antonioli, and Wayne P. Burleson. 2013. “On-Chip Lightweight Implementation of Reduced NIST Randomness Test Suite.” In 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 93–98. ieeexplore.ieee.org.

[64] Yang, Bohan, Vladimir Rožić, Miloš Grujić, Nele Mentens, and Ingrid Verbauwhede. 2017. “On-Chip Jitter Measurement for True Random Number Generators.” In 2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 91–96. ieeexplore.ieee.org.

[65] Yang, Bohan, Vladimir Rožić, Nele Mentens, Wim Dehaene, and Ingrid Verbauwhede. 2016. “TOTAL: TRNG on-the-Fly Testing for Attack Detection Using Lightweight Hardware.” In 2016 Design, Automation Test in Europe Conference Exhibition (DATE), 127–32. ieeexplore.ieee.org.

[66] Vaskova, Anna, Celia López-Ongil, Enrique San Millán, Alejandro Jiménez-Horas, and Luis Entrena. 2011. “Accelerating Secure Circuit Design with Hardware Implementation of Diehard Battery of Tests of Randomness.” In 2011 IEEE 17th International On-Line Testing Symposium, 179–81. ieeexplore.ieee.org.

研究業績

論文誌

1. S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs and I. Verbauwhede, "EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage", IEEE Transactions on Electromagnetic Compatibility, vol. 61(4), pp. 1122-1128. 2018, (3 章).

2. S. Osuka, D. Fujimoto, Y. Hayashi, " Electromagnetic Side-channel Analysis against TERO-based TRNG", IEEE Transactions on Electromagnetic Compatibility （投稿中）, (4 章).

3. S. Kawamura, Y. Komano, H. Shimizu, S. Osuka, D. Fujimoto, Y. Hayashi, K. Imafuku, "Efficient Algorithms for Sign Detection in RNS Using Approximate Reciprocals", IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, vol.104.1, pp.121-134, 2021, (2 章).

国際学会

1. S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs and I. Verbauwhede, “Fundamental Study on Non-invasive Frequency Injection Attack against RO-based TRNG”, 2018 Joint IEEE EMC & APEMC, 2018.5.15, (3 章).

2. S. Osuka, D. Fujimoto, N. Homma, A. Beckers, J. Balasch, B. Gierlichs, I. Verbauwhede, Y. Hayashi,“Fundamental Study on Randomness Evaluation Method of RO-Based TRNG Using APD”, EMC Sapporo & APEMC 2019, 2019.6.4, (4 章).

3. S. Osuka, D. Fujimoto, A. Beckers, B. Gierlichs, I. Verbauwhede, Y. Hayashi, “A Study on Output Bit Tampering of True Random Number Generators

Using Time-Varying EM Waves ”, 2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), 2021.9, (3 章).

4. A. Beckers, J. Balasch, B. Gierlichs, S. Osuka, M. Kinugawa, D. Fujimoto, Y. Hayashi, I. Verbauwhede, “ Characterization of EM Faults on ATmega328p ”, EMC Sapporo & APEMC 2019, FriAM2C.1, 2019.6.7, (3 章).

国内学会（査読なし）

1. 大須賀彩希, 藤本大介, 林優一, 本間尚文, A. Beckers, J. Balasch, B. Gierlichs, I. Verbauwhede,“ サイドチャネル情報を用いた乱数生成器への非侵襲な周波数注入攻撃,”2018 年暗号と情報セキュリティシンポジウム（SCIS2018）, 1D2-4, 2018.1.23, (3 章).

2. 大須賀彩希, 藤本大介, 林優一, “ 真性乱数生成器に対する物理攻撃によるセキュリティ低下の検討 ”, ハードウェアセキュリティ夏のワークショップ, 2018.9.27.

3. 大須賀彩希, 藤本大介, 林優一, 本間尚文, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, ” 振幅確率分布を用いた真性乱数生成器の乱数性評価手法に関する基礎検討 ”, ハードウェアセキュリティフォーラム 2018, 2018.12.13, (4 章).

4. 大須賀彩希, 藤本大介, 林優一, 本間尚文, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, ” TRNG on-the-fly テストを実装したリングオシレータベースの真性乱数生成器への周波数注入攻撃”, 2019 年暗号と情報セキュリティシンポジウム（SCIS2019）, 滋賀, 2D4-3, 2019.1.23, (4 章).

5. 大須賀彩希, 真性乱数生成器に対する周波数注入攻撃時の出力ビット推定手法に関する基礎検討” ハードウェアセキュリティサマーセミナー, 2019.

6. 大須賀 彩希, 藤本 大介, 林 優一, ”TERO-based TRNG に対する周波数注入攻撃時の出力ビット推定手法に関する基礎検討,” ハードウェアセキュリティ研究会, 信学技報, vol. 119, no. 260, HWS2019-62, pp. 29-34, 2019 年 11 月., 2019.11.1, (4 章).

7. 大須賀 彩希, 藤本 大介, 林 優一, ”TERO-based TRNG の発振回数の変化から推定可能な出力ビットの評価 ,” ハードウェアセキュリティフォーラム 2019, 東京, 2019.12.6, (3 章).

8. 大須賀 彩希, 藤本 大介, 林 優一, ”単純電磁波解析を用いた TERO-based TRNG の出力ビット推定,” 2020 年暗号と情報セキュリティシンポジウム (SCIS2020), 3E3-4, 高知, 2020.1.30, (3 章).

9. 森本 康太, 藤本 大介, 大須賀 彩希, 川村 信一, 照屋 唯紀, 林 優一, “ RNS 表現によるバイナリ拡張ユークリッド互除法を用いたペアリング計算における逆元計算の高速実装に関する検討”, ハードウェアセキュリティ研究会, 2021.07.

受賞

1. 暗号と情報セキュリティシンポジウム 論文賞：大須賀彩希, ”サイドチャネル情報を用いた乱数生成器への非侵襲な周波数注入攻撃 ” 暗号と情報セキュリティシンポジウム, 2018.

2. 平成 30 年度ＮＡＩＳＴ最優秀学生賞

3. ハードウェアセキュリティサマーセミナー 最優秀ポスター賞：大須賀彩希, ”真性乱数生成器に対する周波数注入攻撃時の出力ビット推定手法に関する基礎検討” ハードウェアセキュリティサマーセミナー, 2019.

4. 2019 年ハードウェアセキュリティ研究会若手優秀賞：大須賀彩希, 藤本大介, 林 優一, “ TERO-based TRNG に対する周波数注入攻撃時の出力ビット推定手法に関する基礎検討 ”

5. ハードウェアセキュリティフォーラム 2019 優秀ポスター賞：大須賀彩希, 藤本大介, 林 優一, “ TERO-based TRNG の発振回数の変化から推定可能な出力ビットの評価 ”

6. 辻井重男セキュリティ論文賞 優秀賞：大須賀彩希, 藤本大介, 林優一, 本間尚文, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, “ EM Information Security Threats Against RO Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakagechain” 第５回辻井重男セキュリティ論文賞, 2020.