修士論文

リングオシレータベースの真性乱数生成器に対する電磁波を用いた物理攻撃に関する研究

大須賀 彩希

2019年03月15日

奈良先端科学技術大学院大学
情報科学研究科

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

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）
藤川 和利 教授　（副指導教員）
藤本 大介 助教　（副指導教員）

リングオシレータベースの真性乱数生成器に対する電磁波を用いた物理攻撃に関する研究*

大須賀 彩希

内容梗概

リングオシレータ（RO）を使用した真性乱数生成器（TRNG）はデジタル回路のみで構成可能なことから、多くのデバイスで使用されている。そのため、TRNGに対する攻撃によりセキュリティの低下が生じた場合、多くのシステムへの影響が生じる。これまで、上述のTRNGへの物理攻撃として、デバイスに特定周波数の電磁波を印加することで、乱数性を大きく低下させる周波数注入攻撃が提案されている。しかし、これまでの研究は攻撃の理論に着目した研究であり、どのようなデバイスが攻撃への脆弱性を持つのかについては十分に議論されていなかった。

本論文では実際のデバイスにおけるROベースのTRNGに対するセキュリティ評価を行うために、(1) デバイスへの物理的な接近や侵襲・改変が困難な環境下において、(2) 乱数性低下検知機構を実装したTRNGに対する周波数注入攻撃の実現可能性について検討を行う。実験では、実際のデバイスを模したROベースのTRNGを構成し、電磁波印加攻撃を行うことで、従来攻撃の対象外とみなされていた機器についても脅威の対象となることを示した。更にこうした脅威を評価するためのセキュリティ評価手法や対策技術についても検討を行った。

キーワード

真性乱数生成器, サイドチャネル攻撃, 意図的電磁妨害, ヘルステスト

*奈良先端科学技術大学院大学 情報科学研究科 修士論文, 2019年03月15日.

Study on physical attack using electromagnetic wave against ring oscillator based true random number generator*

Saki Osuka

Abstract

True random number generators (TRNGs) based on ring oscillators (ROs) are employed in many devices because they can be constructed by digital circuits. If an RO-based TRNG is attacked and its security is compromised, many systems are affected. Among the physical attacks against TRNGs, frequency injection attacks degrade randomness by introducing a sinusoidal wave of a specific frequency to the device. However, previous studies have focused on the theory of attacks, and the kind of devices that are vulnerable to attacks has not been fully discussed.

In this thesis, I evaluated the security of RO-based TRNG in actual devices. Specifically, I investigated the probability of an attack against (1) a TRNG implemented in an environment where it is difficult to physically access or modify/invade the device, and (2) a TRNG in which a randomness degradation detection mechanism is implemented. In the experiments, I investigated whether it is possible to attack RO-based TRNGs by introducing electromagnetic waves, and demonstrated/showed a realistic threat against equipment that was considered safe from/invulnerable to conventional attack. I also examined the security evaluation method and countermeasures to the attack.

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 15, 2019.

Keywords:

True random number generator, Side-channel attack, Intentional Electromagnetic Interference, Health test

目 次

図 目 次

1. 序論

1.1 セキュリティにおける TRNG の重要性と物理攻撃の可能性

現代では、PC や携帯電話などの情報通信機器が広く普及し、インターネットや情報通信技術への社会の依存度が高まるに従い、情報セキュリティの確保は重要な課題となっている。暗号技術は情報セキュリティの確保に利用され、公開鍵暗号や共通鍵暗号を用いた暗号プロトコルによって、情報の機密性や完全性、可用性は担保されている。暗号プロトコル中では、秘密鍵やノンス、ソルト、ワンタイムパッド、初期化ベクトルなど、様々な秘密情報が用いられる。これらの秘密情報には乱数を用いることが多く、セキュリティで使用される乱数は、生成した乱数列の再現が困難であること、乱数列の一部や中間値から乱数列の予測が困難であること、乱数が一様に分布していることが求められる。乱数は乱数生成器によって生成され、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ため、予測困難な乱数の生成は暗号の基盤技術の一つとなっている。

乱数生成器は、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）の二つに分類される。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が再現される。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 は熱雑音などの物理的なランダム要因から乱数を生成するため、再現性が低く予測困難な乱数となる。そのため、セキュリティ分野での需要が高い。

TRNG のエントロピー源として、ユーザーのマウス操作を利用するもの [1] から原子の放射線崩壊を専用のデバイスで観測するもの [2] など様々な物理現象のランダム性を利用した TRNG が提案されている。なかでも、スループットの高さやデジタル回路のみで構成できる実装の容易さから、リングオシレータ（RO: Ring Oscillator）から生じるクロックジッタをエントロピー源として乱数を生成

するTRNGが広く研究されている[3, 4, 5, 6, 7, 8, 9]。ROをエントロピー源とするTRNGは、IntelのPC[10]やスマートカード[11, 12]などにも組み込まれ、広く普及している。そのため、ROベースのTRNGの乱数性が低下した場合、多くのシステムに影響が生じる可能性がある。

一方で、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[13, 14]。こ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。物理攻撃によるセキュリティの低下はROベースのTRNGにも及んでおり、エントロピー源であるROに対して物理攻撃を行うことで乱数性を低下させる攻撃の可能性が指摘されている。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など様々な攻撃が提案されているが、なかでもROに対して電磁波を印加することで乱数性を低下させる攻撃は、攻撃によって乱数性が大きく低下し、乱数に周期性が現れる可能性[15]やビットを大きく偏らせる可能性[16, 17]が指摘されており、この攻撃は乱数の予測を容易にすることからセキュリティに対する重大な脅威であると考えられている。そのため、本論文ではROをエントロピー源とするTRNGに対する電磁波印加による物理攻撃に対するセキュリティについて論ずる。

1.2 ROベースのTRNGに対するセキュリティ評価とその問題点

周波数注入攻撃はROベースのTRNGに対する電磁波印加による主な攻撃手法である。この攻撃は、TRNGに特定の周波数の正弦波を印加することでエントロピー源であるROのエントロピーを抑制し、乱数性を低下させる。すでに、スマートカードなどに実装されたROベースのTRNGに対して、この攻撃を行うことで生成された乱数の乱数性を大きく低下させ、秘密情報のパターンを大きく削減する可能性が示されている[15]。この攻撃は秘密情報の予測を容易にし、暗号プロトコル全体のセキュリティを大きく低下させる可能性があり、対策の実施が検討されてきた。

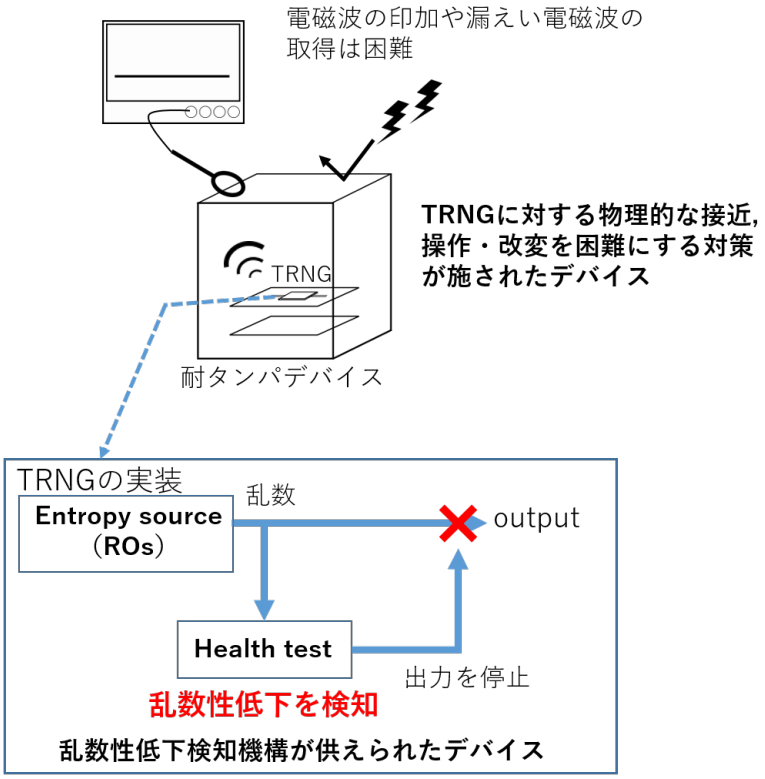


図 1.1: 従来の周波数注入攻撃では攻撃が困難なデバイス

一般的に、暗号デバイスに攻撃への対策技術を実装するには、デバイスの実装を考慮することに加えて、暗号デバイスがどのような環境下で運用され、攻撃者がデバイスに対してどの程度の操作を加えることが可能かを想定し、実行可能性のある攻撃手法について対策を施していくことが重要であると考えられる。RO ベースの TRNG に対する周波数注入攻撃では、機器に対して電磁波を印加することで乱数性を低下させ、乱数性が低下したビット列が暗号プロトコル中で使用されることで、システム全体のセキュリティを低下させることを前提としているため、攻撃の可否は、(1) 乱数性を低下させる電磁波印加手法と (2) 攻撃によって生じた乱数性低下が後段の暗号処理に伝搬するかに依存する。そのため、実際のデバイスに対してセキュリティ評価を行うには、上記の 2 点を考慮して、攻撃の実現可能性を評価する必要がある。

一方、従来の周波数注入攻撃では、特に IC チップを内蔵したスマートカード

に対する攻撃シナリオを想定し、デバイスに対する物理的な接近や侵襲・改変を前提とした攻撃の可能性について議論が行われてきた。そのため、筐体に覆われた機器や、筐体や IC パッケージに開封検知機構を備えたデバイスといった、機器への接近や改変が困難なデバイスについては、電磁波の印加は困難であり、周波数注入攻撃の実現は難しいと考えられてきた（図 1.1）。これに対して、近年では暗号ハードウェアに対する接近や改変が不可能な条件であっても実行可能な電磁波印加手法が提案されており、従来は脅威の範囲外とみなされてきた機器に対する攻撃の実現可能性については議論の余地が残る。

加えて、従来想定されてきた TRNG は乱数を生成するモジュールのみで構成された最も単純な TRNG である。一方、米国のセキュリティ基準である NIST SP800-90B [18] や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[19] では、TRNG の設計要件として、乱数の品質を検証するヘルステストの実装を推奨している。ヘルステストは乱数性の低いビット列を検知し、乱数の出力を停止するため、ヘルステストが実装されていた場合、従来の周波数注入攻撃による乱数性低下の脅威は無効化される可能性が高いと考えられてきた（図 1.1）。しかし、周波数注入攻撃に対するヘルステストの有効性について十分な検証はされておらず、仮にヘルステストを実装した TRNG に対して周波数注入攻撃が成立した場合、これまで未対策であった多くの機器にも対策を施す必要が生じる。

このことから、実際のデバイスに対して周波数注入攻撃の影響範囲を評価するには、これまで十分に議論されていなかった (1) 攻撃対象の機器にどの程度接近可能であり、侵襲や改変を施すことが可能か、(2) 乱数性低下を検知する機構など攻撃を困難化する実装が施されているか、について攻撃の実現可能性を検証することが重要であると考えられる。

1.3 研究目的

従来の周波数注入攻撃に対する研究は、攻撃の理論に着目した研究であり、実際のデバイスに対する攻撃の実現可能性については十分に議論されておらず、電磁波印加や漏えい電磁波の計測が困難な耐タンパデバイスやヘルステストが実装

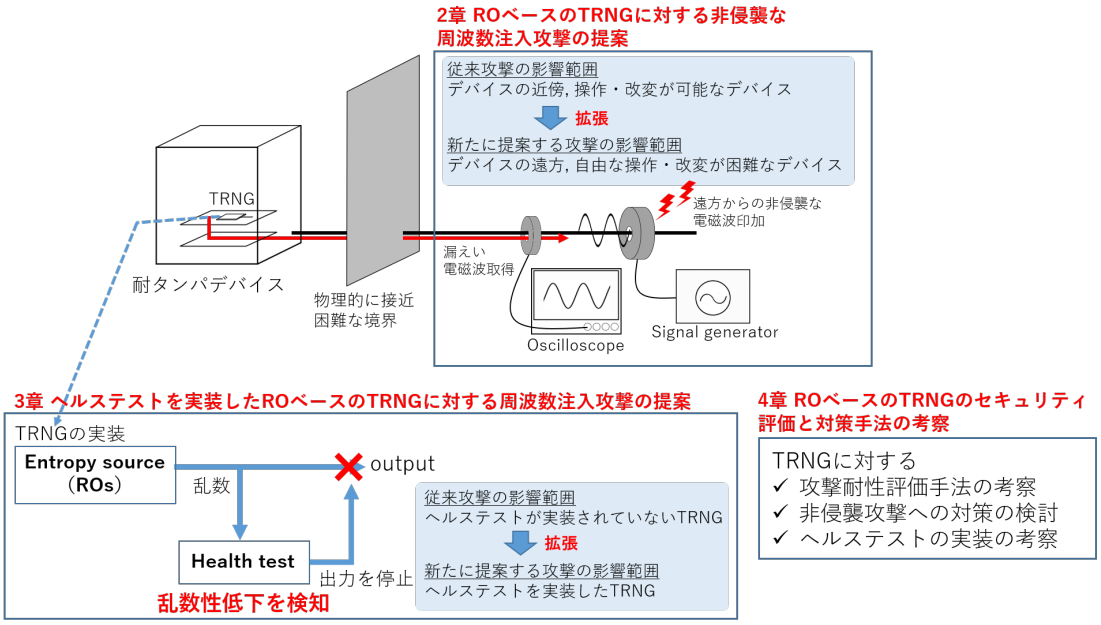


図 1.2: 本論文の構成

されたデバイスについては攻撃が困難であるとみなされてきた。これに対して、本論文では、実際のデバイスに対して周波数注入攻撃を困難化する問題を、電磁波印加自体を困難化する要因と乱数性低下の検出により攻撃自体を無効化する要因に分類し、それぞれについて周波数注入攻撃を拡張し、実際のデバイスにおける RO ベースの TRNG に対する周波数注入攻撃の脅威の範囲を明らかにすることを目的とする（図 1.2）。具体的には、 (1) デバイスへの物理的な接近や侵襲・改変が困難な環境下において、(2) ヘルステストを実装した TRNG に対する乱数性低下攻撃の実現可能性について検討を行う。実験では、RO ベースの 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 RO 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。そして、電磁波の印加時間を制御することでエントロピー源である RO のエントロピーを操作し、出力される TRNG の乱数性を変化させることでヘルステストをパスするような乱数性低下を引き起こすこと

が可能なことを示す。

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 TRNG やヘルステストを実装した TRNG 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。提案手法による攻撃に対抗するためには従来検討されてきた開封検知の実装など侵襲攻撃を想定した対策技術とは異なる対策が求められることから、本稿では、TRNG への非侵襲な攻撃に対する対策手法や攻撃耐性評価手法についても議論する。

1.4 本論文の構成

本論文の構成は以下の通りである。

第二章では、電磁波印加が困難なデバイスに対する周波数注入攻撃の可能性を検討するために、(1) デバイスへの物理的な接近や侵襲・改変が困難な環境下における非侵襲な周波数注入攻撃を提案する。そして、CMOS インバータを用いて RO ベースの TRNG を作成し、電源線を通じた電磁波印加とサイドチャネル情報の取得により、自由な操作・改変が困難なデバイスに対してもデバイス遠方から非侵襲に周波数注入攻撃を実現する可能性があることを実証する。

第三章では、第二章に引き続いて、実際のデバイスに対する現実的な脅威の可能性について検証するため、(2) ヘルステストを実装した TRNG に対する乱数性低下攻撃を提案する。実験では、実際のデバイスを模した環境として、FPGA（Field-programmable gate array）上に実装された ERO-TRNG（Elementary RO-based TRNG）と TRNG on-the-fly テストに対して、複数の信号源を用いて電磁波を印加し、更に電磁波印加時間を制御することでヘルステストをパス可能な乱数性低下を引き起こす攻撃が可能であることを実証する。

第四章では、RO ベースの TRNG に対する周波数注入攻撃のセキュリティ評価手法を考察した後、非侵襲攻撃への対策技術やヘルステストの実装についての検討を行う。

第五章では、本論文の結論を述べる。

2. ROベースのTRNGに対する非侵襲な周波数注入攻撃の提案

本章では、従来の周波数注入攻撃では考慮されてこなかった、RO ベースの TRNG に対する現実的な脅威の可能性について論ずるため、まず、(1) デバイスへの物理的な接近や侵襲･改変が困難な環境下における周波数注入攻撃の可能性について検討を行う。具体的には、CMOS インバータを用いて RO ベースの TRNG のモデルとなるデバイスを作成し、電源線を通じて電磁波印加とサイドチャネル情報の取得を行うことで、デバイス遠方から非侵襲に周波数注入攻撃を実現する可能性があることを実証する。

2.1 提案手法

従来の周波数注入攻撃では、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物理的な接近や侵襲・改変を行い、TRNG に対して特定の周波数の正弦波を印加することで、乱数性を低下させてきた。一方、デバイスへの物理的な接近や侵襲・改変が困難な環境下において攻撃を実現するには、機器に対して遠方から非侵襲に電磁波印加を行い、TRNG の乱数源となる RO のエントロピーを抑制する必要がある（図 2.1）。そのため、①「TRNG に対する非侵襲な電磁波印加による RO のエントロピー抑制手法」が必要となる。続いて、TRNG の乱数性を低下させるには、攻撃条件を決定する必要がある。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適切な攻撃条件を選択してきた。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である。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、適切な注入周波数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、注入周波数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、②「TRNG の乱数性を低下させる攻撃条件を非侵襲に決定する手法」を実現する必要がある。

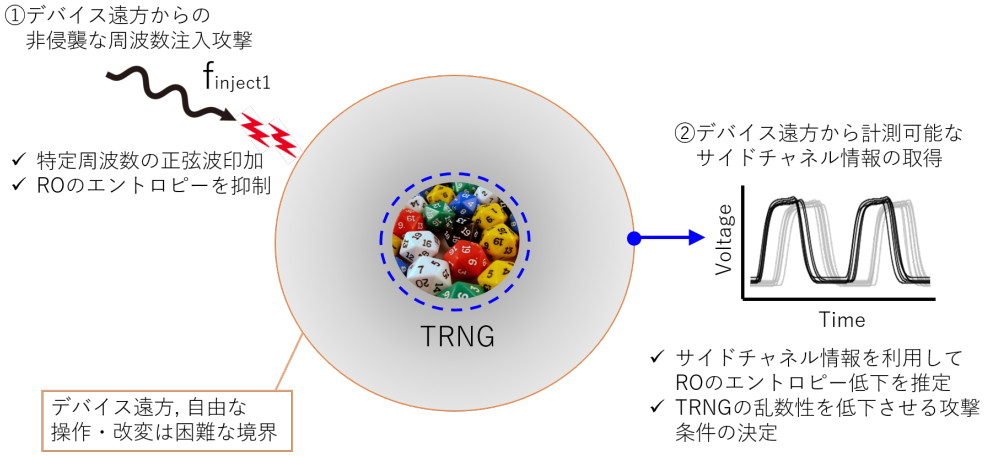


図 2.1: 非侵襲な周波数注入攻撃のイメージ

そこで本節では、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界を印加し、乱数性を低下させる手法を提案する。

以下では、提案手法により RO ベースの TRNG の乱数性が低下する原理を説明するとともに、サイドチャネル情報を用いて乱数性の低下を推定する手法について述べる。

2.1.1 周波数注入攻撃によるジッタの抑制

現在、広く使用されている RO ベースの TRNG の構成は Sunar らによって基本的な原理の提案がされた [3]（図 2.2）。この RO ベースの TRNG は任意の奇数値をとる n1, …, nr 個のインバータから成る r 個の RO をエントロピー源とし、RO のエントロピーは別の RO または外部クロックによってトリガされる D フリップフロップなどでサンプリングされ、XOR（Exclusive OR）ゲートなどによって集約されることで乱数性をもつ 1 ビットを生成する。RO のエントロピーは RO の出力信号のランダムノイズであるジッタによって生じ、このジッタによって TRNG が生成するビット列に乱数性が生じる。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

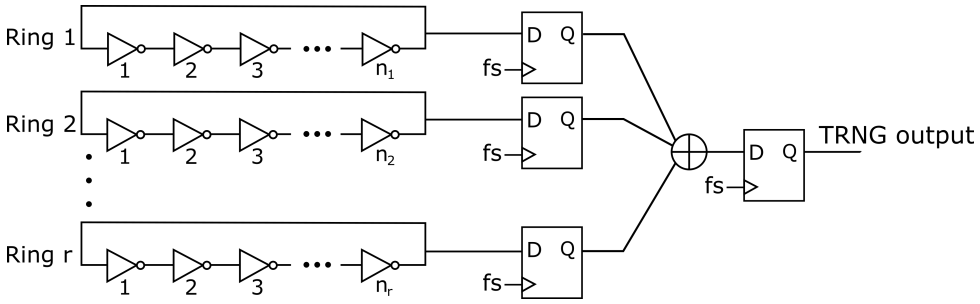
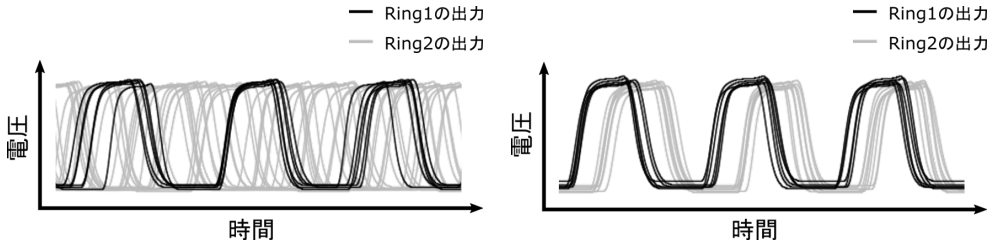


図 2.2: RO ベースの TRNG の基本的な構成



(a) 高エントロピー時　　(b) 低エントロピー時

図 2.3: エントロピーの変化による RO の出力信号の変化

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 2.3(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、TRNG の出力は高い乱数性を持つようになる。

これに対し、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、振動タイミングが揃えられる引き込み現象を利用する。この現象により、各 RO のジッタは注入した正弦波の位相にロックされ、RO のエントロピーが低下する [20]。位相の同期は、各 RO の遷移タイミングのばらつきを抑制するため、RO は図 2.3(b) のようにゆらぎが減少する。そして、ゆらぎの減少により RO 間の出力パターンが減少し、TRNG の乱数性は低下する。

2.1.2 RO の内部状態に依存したコモンモード電流の観測

本節では攻撃対象の 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（EMC）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 [21, 22, 23]。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 [24] 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。

しかし、コモンモード電流による RO の内部状態を含む信号には、エントロピー源となる全ての RO の内部状態を含み、各 RO の出力信号の時間領域波形を独立して取得することは難しいと考えられる。そのため、これまで使用されてきた、各 RO の出力信号の時間領域におけるジッタの測定といった RO のエントロピー評価手法を用いることは難しい。このことから、本手法では周波数領域においてエントロピー源となる全ての RO のエントロピーが低下した状態を推定する。

RO のエントロピーは時間領域においては 2.1.1 節で示したように、遷移タイミングのゆらぎであるジッタとして現れる。この遷移タイミングのゆらぎ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 [25]。一方、RO のエントロピーが低下した場合は、時間領域ではジッタが抑制され、周波数領域では発振周波数近傍の位相雑音が低減する。そのため、乱数源である複数の RO のエントロピーが高い状態では、複数の RO の位相雑音によるスペクトルの広がりと RO 間の相互作用によって生じたノイズにより、多数のピークが観測される。一方、エントロピー源となる全ての RO のジッ

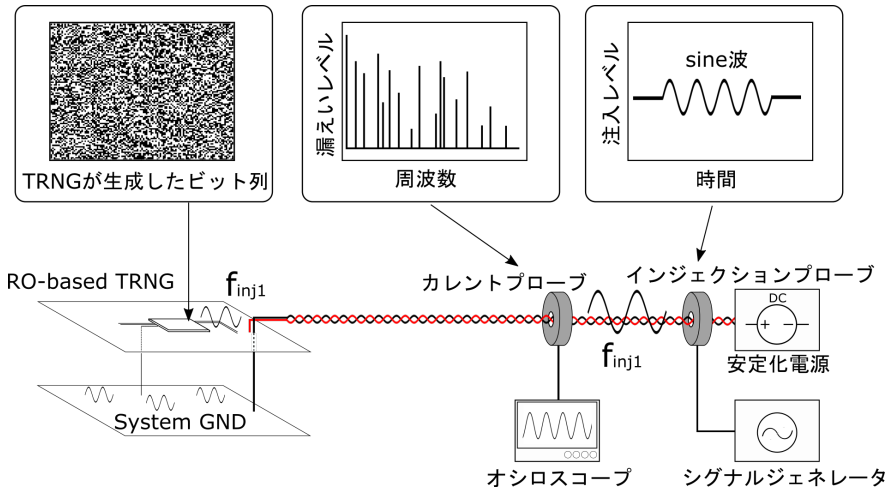


図 2.4: 遠方からの RO ベースの TRNG に対する周波数注入攻撃のイメージ

タが抑制され、TRNG の乱数性が低下する場合は、位相雑音や RO の相互作用によるノイズの低減により、ピーク数が減少すると考えられる。この変化を利用することで、TRNG の乱数性を遠方から非侵襲に推定できる可能性が高い。

図 2.4 に本稿で提案する手法の概要を示す。まず、電源線にクランプしたインジェクションプローブに電圧を印加することにより、電源線上に誘導される妨害波電流を暗号デバイスの基板上に伝搬させ、IC モジュールの VDD/GND 間の電圧を振動させる。これにより、前節で示した原理により RO のジッタを抑制する。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、前述した RO のロックによる内部状態の変化を示す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。

本手法の利点は、デバイスに対して接近や改変を行う必要がない点や、電磁波印加による攻撃の痕跡を残さずに攻撃を実現可能である点などがあげられる。また、本手法は市販されている一般的な実験機器のみを用いて実現可能である。加えて、機器への侵襲や改変といった高度な技術力を必要としないため、従来の周波数注入攻撃と比べて実行が容易であることも利点としてあげられる。

2.2 ROベースのTRNGに対する遠方からの非侵襲な周波数注入攻撃の実証

本節では、遠方からROのエントロピーを低下させる事が可能な攻撃信号を注入可能であることと、前節に示した手法を用いてサイドチャネル情報からROの内部状態が取得可能であることを示したのち、実際にサイドチャネル情報のみを用いて、TRNGの乱数性を推定可能であることを示す。

正弦波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。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、オシロスコープによってROの内部処理の変化を確認する。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。

2.2.1 実験条件

11段のROと9段のROから構成されるROベースのTRNG（図2.5）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2.6に実験セットアップを表2.1に実験に使用した機器を示す。TRNGの乱数性を失わせる攻撃信号の注入は、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

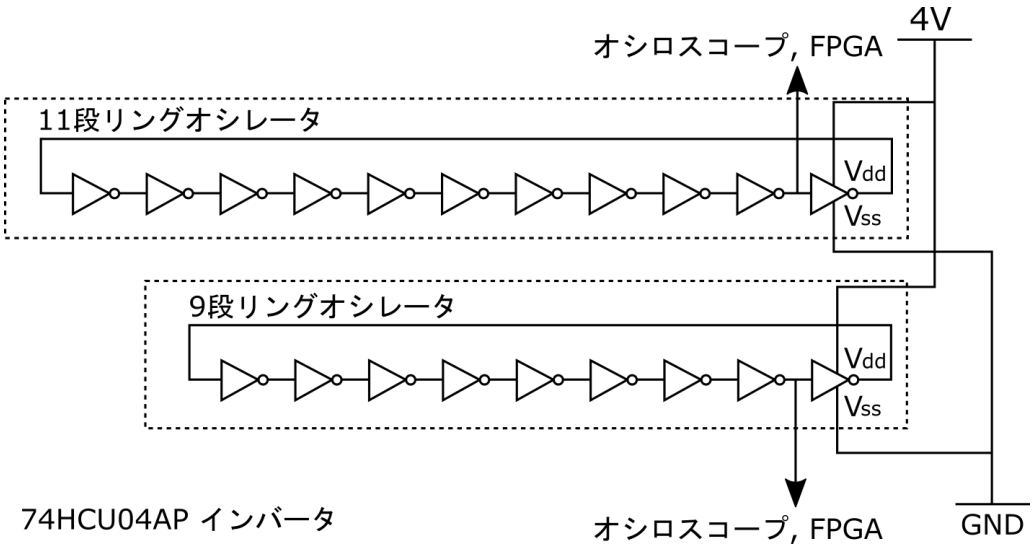


図 2.5: 実験に使用した RO ベースの TRNG の構成

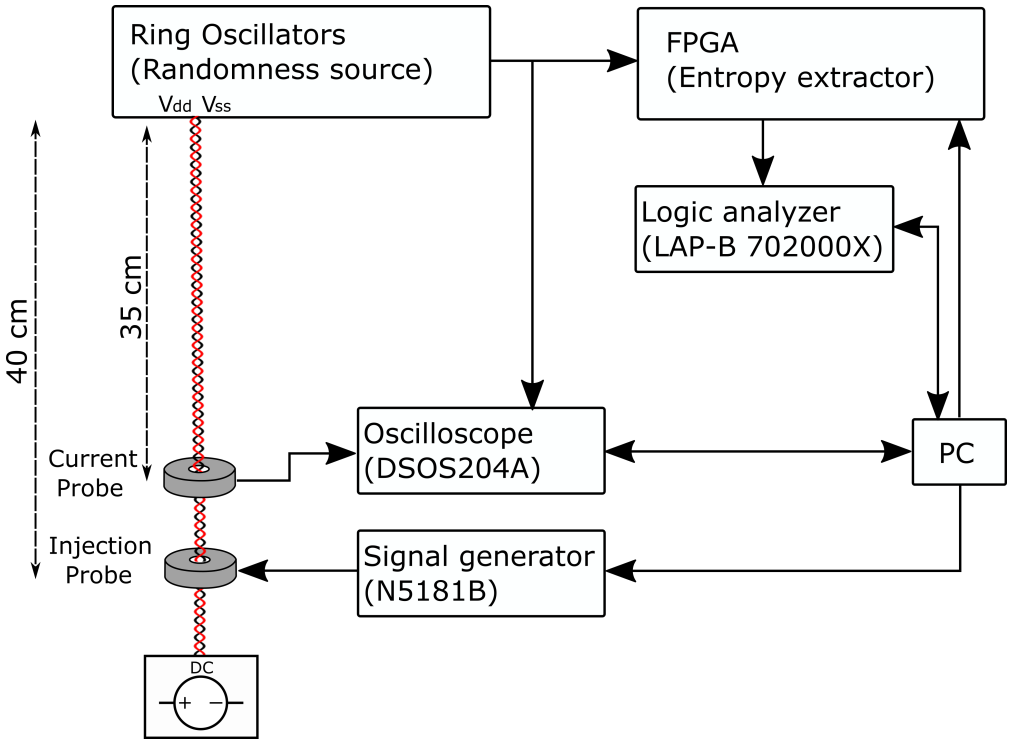


図 2.6: 実験セットアップ

表 2.1: 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

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。

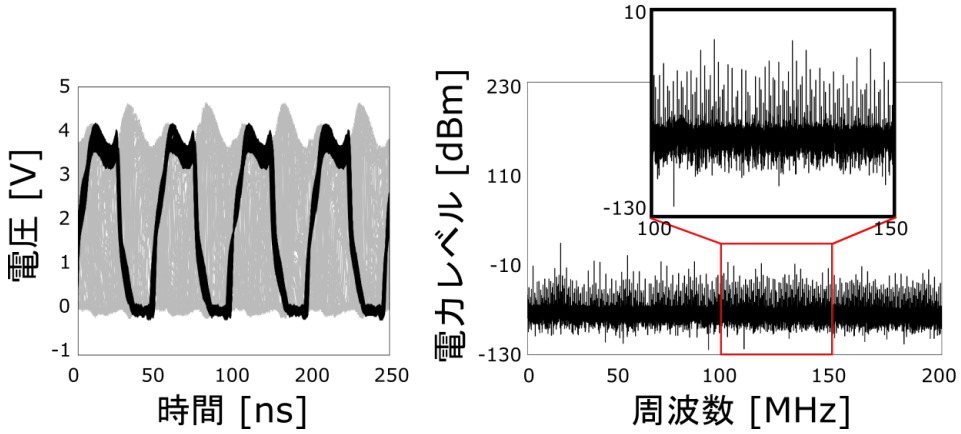
また、本実験では、カレントプローブを対象の TRNG モジュールから約 35 cm 離れた位置に、インジェクションプローブを約 40 cm 離れた位置に設置する。

2.2.2 周波数注入時のコモンモード電流のスペクトル変化

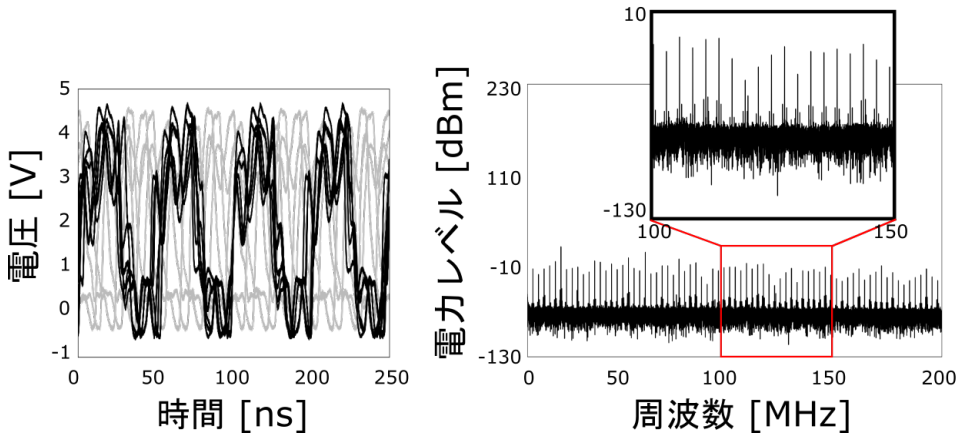
本節では、遠方から攻撃を行うための基礎検討として、RO をロックする攻撃信号を機器外部から注入可能であることと RO の内部状態の変化がコモンモード電流の変化として現れ、それが機器外部で計測できることを実証する。

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。ここで、注入した電磁波の振幅は 25.2 dBm で、注入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 2.7 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



(a) 32.3 MHz injection



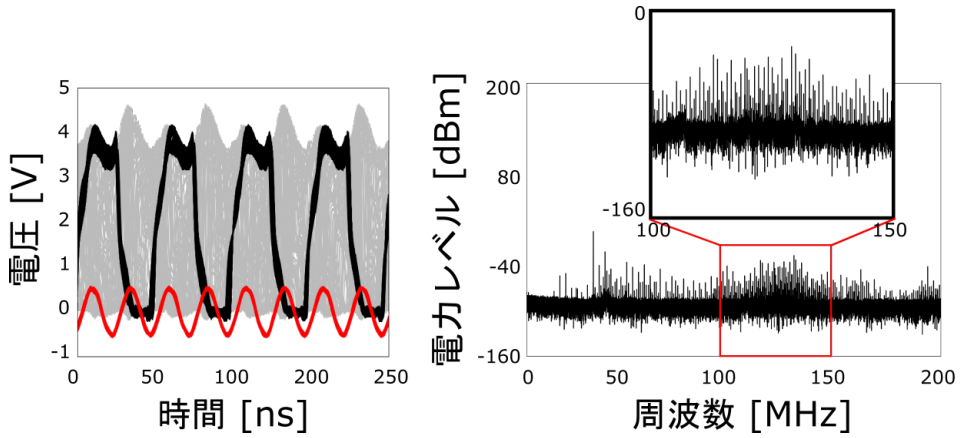
(b) 57.0 MHz injection

図 2.7: 電磁波印加時の RO の出力信号

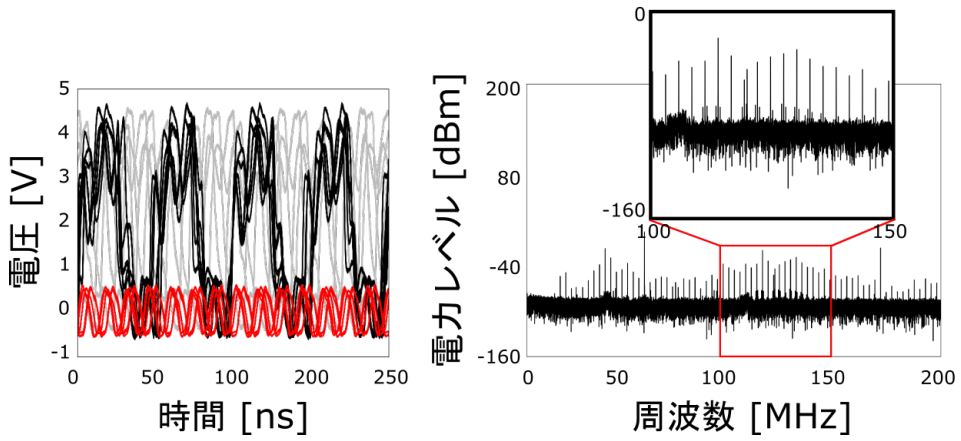
11 段 RO（黒線）にトリガをかけ、取得したデータを 100 波形重ねている。後方のグレー線は 9 段 RO の信号波形を示している。図 2.7(a) は 32.3 MHz を注入した結果を示している。この結果では 11 段 RO に対して、9 段 RO の信号波形が多数のパターンをとり、波形のゆらぎが大きいことが確認できる。これは、図 2.3(a) に示したように 11 段 RO に対して 9 段 RO の遷移タイミングがばらついていることを示す。このことから、32.3 MHz で正弦波を注入した場合、RO はロックされないことが確認できる。一方、57.0 MHz を注入した際の観測を示す図 2.7(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、遠隔からの（モジュールからの距離 40 cm 程度）電磁波印加によって RO をロックする攻撃信号が注入可能であることが確認できる。

続いて、コモンモード電流から攻撃による RO のエントロピー低下を観測する手法について検討を行う。図 2.8 の時間領域波形は、図 2.7 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、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 2.7(a), (b) の右図に左図の周波数スペクトルを示す。図 2.7(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 2.7(a) では、2.1.2 節で示したようにジッタ及び 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 2.7(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 2.8 から確認でき、特に 100-150 MHz の範囲で非ロック時（図 2.8(a)）/ ロック時（図 2.8(b)）の差が明確に観測された。



(a) 32.3 MHz injection



(b) 57.0 MHz injection

図 2.8: 電磁波印加時のコモンモード電流波形

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たことから、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。

2.2.3 コモンモード電流の観測に基づく TRNG の乱数性の推定

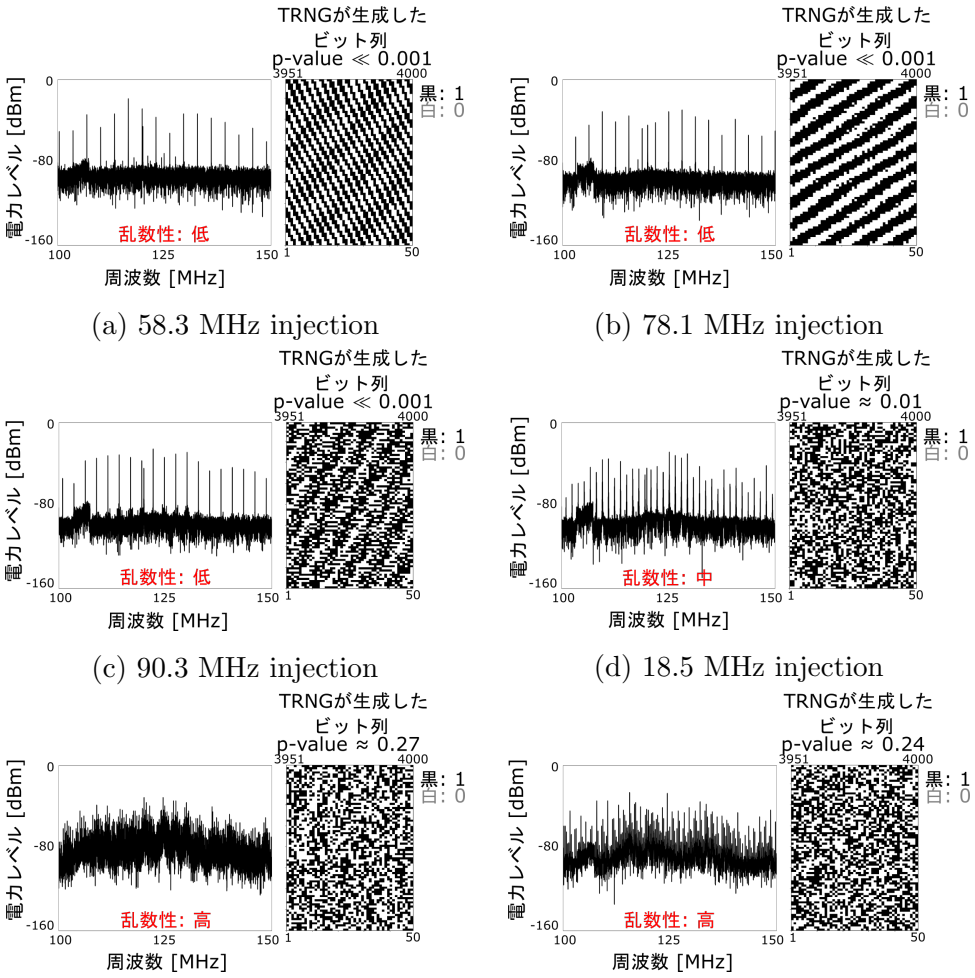
本節では、前節で得られた結果に基づきコモンモード電流をサイドチャネル情報として用いることで TRNG の乱数性低下が推定できることを示す。

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 2.8(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 2.9 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 [26]。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れる。

図 2.9(a)-(c) 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 2.9(a)-(c) 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 2.9(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 2.9(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



(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 2.9: サイドチャネル情報を使用した乱数性推定と攻撃結果

た、図に示した注入周波数以外にも、図 2.8(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印加によって非侵襲に 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。

2.3 まとめ

本章では、デバイスへの物理的な接近や侵襲・改変が困難な環境下における非侵襲な周波数注入攻撃の可能性を実証するため、デバイス遠方からの電磁波印加と TRNG から生ずるコモンモード電流をサイドチャネル情報として乱数性を判定する手法を提案した。そして、CMOS インバータで構成される RO ベースの TRNG のモデルに対して、提案手法による攻撃を行い、実際に乱数性を低下させることで、デバイスに対する物理的な接近や侵襲が困難なデバイスに対しても非侵襲に RO ベースの TRNG の乱数性を低下させる攻撃が可能であることを示した。

本手法による遠隔からの非侵襲な周波数注入攻撃は、従来は攻撃の対象外とみなされてきた機器にも影響する可能性があるため、必要があれば適切な対策手法を適用すべきであると考えられる。

3. ヘルステストを実装した RO ベースの TRNG に対する周波数注入攻撃の提案

本章では第二章に引き続いて、従来の周波数注入攻撃では考慮されてこなかった、RO ベースの TRNG に対する現実的な脅威の可能性について論ずるため、(2) ヘルステストを実装した TRNG に対する乱数性低下攻撃の実現可能性について検討を行う。具体的には、実際のデバイスを模した環境として、FPGA 上に実装された TRNG に対する攻撃を行う。ヘルステストを実装した ERO-TRNG に対して、複数の信号源を用いて電磁波を印加し、電磁波印加時間を制御することでヘルステストをパス可能な乱数性低下を引き起こす攻撃が可能であることを実証する。

本章では、ヘルステストを実装した TRNG に対する周波数注入攻撃の実現可能性を示すため、電磁波の印加が容易な機器を仮定し、ボード上の改変を行って攻撃を実行したが、前章で示した理論を用いることで、非侵襲に周波数注入攻撃を実現できると考えられる。

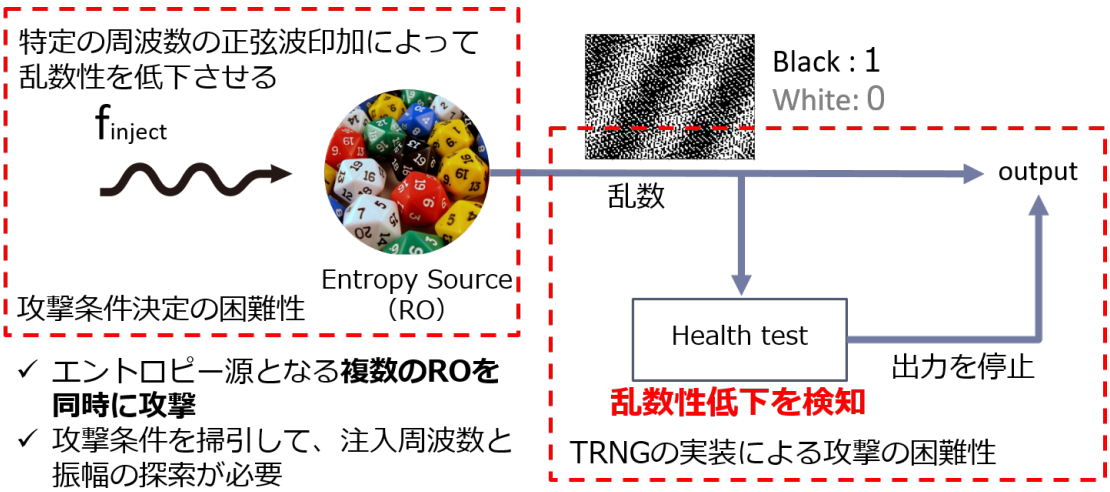


図 3.1: 実際のデバイスにおける従来の周波数注入攻撃を困難化する要因

3.1 提案手法

従来の周波数注入攻撃では、特定の周波数の正弦波印加により複数の RO のエントロピーを同時に低下させることで、TRNG の乱数性を低下させていた。しかし、複数の RO を同時に攻撃可能な攻撃条件を解析的に求めることは難しく、従来の周波数注入攻撃では、TRNG の乱数性を低下させる攻撃条件を探索するのに、注入周波数や振幅の掃引を必要としていた。そのため、実際のデバイスに対して攻撃を行うには、攻撃条件の探索に時間がかかり、攻撃が困難化していた（図 3.1）。このことから、実際のデバイスに対する攻撃可能性を検討するには、①電磁波印加条件を高速に決定可能な攻撃手法の検討が必要となる。

また、実際のデバイスにおいては乱数性低下を検知するヘルステストの実装が推奨されており、従来の周波数注入攻撃による乱数性低下はヘルステストにより、検知されると考えられる。そのため、ヘルステストを実装した TRNG に対して乱数性低下の脅威を引き起こすには、②電磁波印加タイミングの制御によるヘルステストをパス可能な乱数性低下が必要となる。

そこで本節では TRNG の乱数性を低下させる攻撃条件を高速に推定可能な攻撃手法と共に、電磁波の印加タイミング制御によりヘルステストに合格可能な乱数性低下を引き起こす手法を提案する。

3.1.1 複数の正弦波印加による乱数性低下と確率密度による攻撃条件推定

従来の周波数注入攻撃では、単一の周波数を持つ正弦波の印加によって、乱数源となる全ての RO のエントロピーを同時に低下させ、乱数列や RO の内部状態を含む信号を用いて、乱数性を低下させる攻撃条件を決定してきた。しかし、複数の RO のエントロピーを同時に抑制する攻撃条件を探索するには、印加する電磁波の周波数や振幅を掃引する必要があり、これは実際のデバイスに対する周波数注入攻撃の実現を困難化している。

これに対して、各 RO のエントロピーを抑制可能な攻撃条件をそれぞれ探索し、複数の信号源を用いて各攻撃条件を満たす電磁波を印加することができれば、攻撃条件の探索にかかるコストを大幅に削減できる可能性がある。特に、発

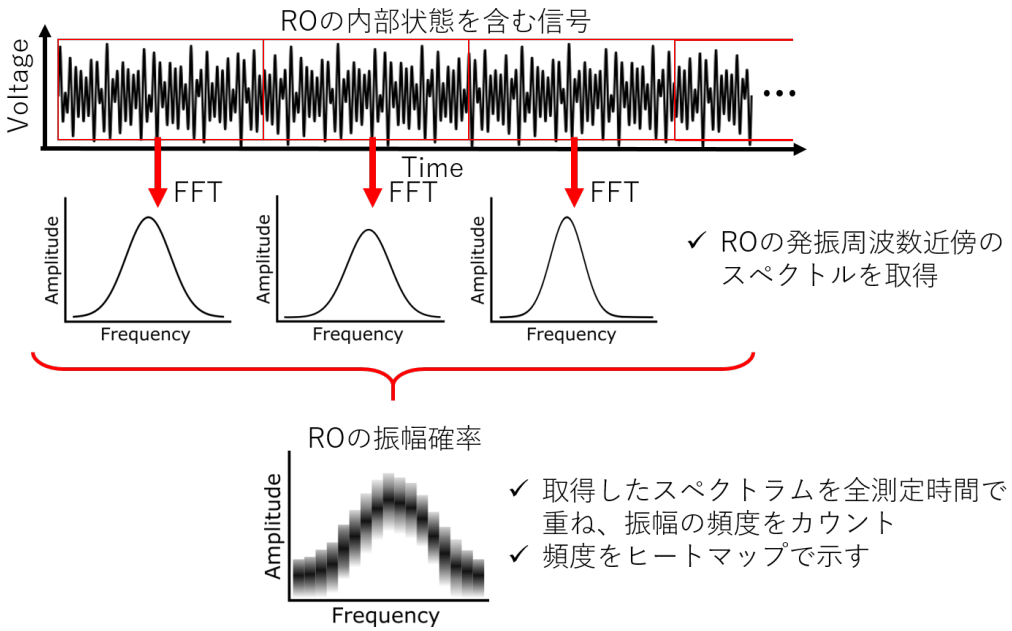
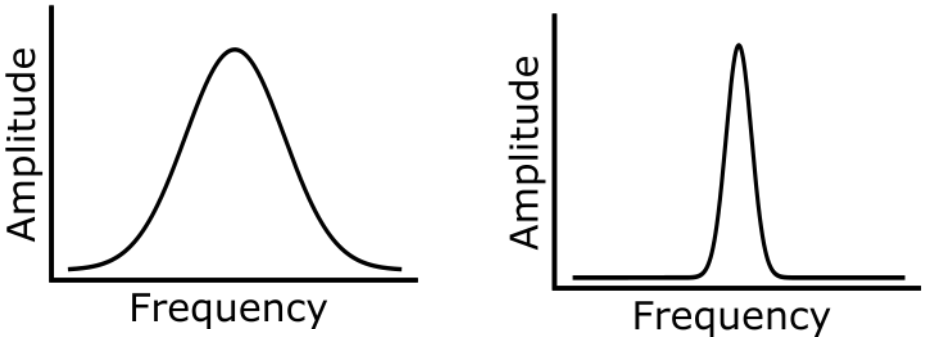


図 3.2: 振幅の確率密度測定のイメージ

振周波数の基本波、または、その高調波の注入は、引き込み現象により RO がもつジッタを効率よく抑制できる可能性が高い。そのため、各 RO の発振周波数の基本波またはその高調波近傍の周波数を探索することで、RO をロック可能な攻撃条件を容易に決定できる可能性がある。また、印加する電磁波の振幅については、周波数領域における伝達効率を考慮することが重要となる。印加した電磁波が TRNG を実装した IC モジュールに到達するまでの伝達効率が高い場合、効率よく VDD/GND 間の電圧を振動させることが可能であり、少ない電力で RO のエントロピーを抑制することができる。

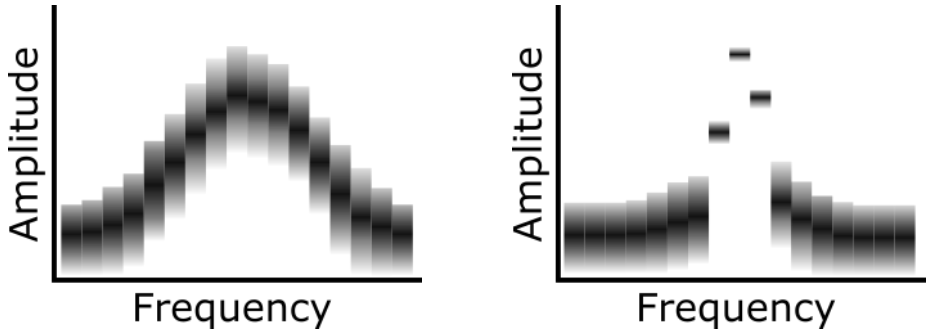
このことから、単一の RO のエントロピー低下を推定しながら、伝達効率の高い周波数帯で各 RO の発振周波数の基本波またはその高調波近傍の周波数の電磁波印加を行うことで、TRNG の乱数性を低下可能な攻撃条件を容易に決定できる可能性がある。以下では、2.1 節で用いた RO の内部状態を含むコモンモード電流の観測を応用した、周波数領域における各 RO のエントロピー推定手法について説明する。

周波数領域において、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



(a) 高エントロピー時　　(b) 低エントロピー時

図 3.3: 周波数領域における RO のエントロピーの変化



(a) 高エントロピー時　　(b) 低エントロピー時

図 3.4: 振幅の確率密度における RO のエントロピーの変化

効に調べる手法として、振幅変動の測定が知られている。測定時間中に生じた振幅の変動を確率的にとらえることで、RO のエントロピーといった確率的な事象についても評価できる可能性がある。振幅変動を確率的にとらえるには、振幅に対する確率密度を求める必要がある。振幅の確率密度は、連続した時間領域波形を適当なフレーム毎に FFT 処理をし、得られたスペクトラムを全測定時間で重ね、振幅の頻度をカウントすることで得られる（図 3.2)。振幅の変動が大きいほど、各周波数に対する振幅の確率分布の裾が広がる。

続いて、RO の出力信号のエントロピーの変化について述べる。RO のエントロピーは周波数領域では 2.1 節に示したように、位相雑音として現れ、図 3.3(a) のように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 [25]。一

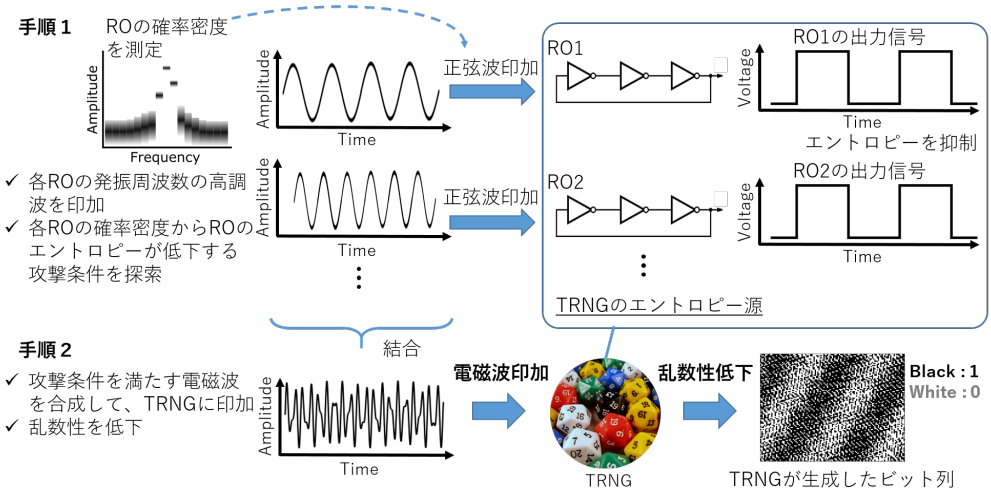


図 3.5: 複数の正弦波印加による周波数注入攻撃のイメージ

方、RO のエントロピーが低下した場合は、時間領域ではジッタが抑制され、周波数領域では発振周波数近傍の位相雑音が低減する（図 3.3(b)）。このエントロピーの変化を振幅の確率密度で表したものを図 3.4 に示す。横軸は周波数を縦軸は振幅を表し、ある周波数に対する振幅の確率密度をビットマップで示し、振幅の確率密度が高いものを黒、確率密度が低いものを白とした、ヒートマップで表している。RO が高エントロピーの時（図 3.4(a)）、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、振幅方向に確率密度分布の裾が広がる。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、分布の広がりは抑制される（図 3.4(b)）。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、TRNG の乱数性を低下可能な攻撃条件を決定できる可能性が高い。

図 3.5 に複数の正弦波印加による周波数注入攻撃の概要を示す。まず、TRNG のエントロピー源である複数の RO に対して、それぞれの RO のエントロピーを低下させる適切な攻撃条件を探索する。まず、手順 1 では、ある RO（RO1）に対して、発振周波数の基本波もしくは高調波を印加しながら、RO1 の確率密度を測定し、RO1 のエントロピーが低下する電磁波印加条件を探索する。続いて、別の RO（RO2）に対しても同様にエントロピーを低下させる攻撃条件を探索する。これを TRNG のエントロピー源である RO の数だけ繰り返すことで、TRNG を構成する全ての RO に対して、エントロピーを低下させる攻撃条件を決定するこ

とができる。続いて、手順 2 では、手順 1 で求めた各 RO に対する攻撃条件を満たす正弦波を生成し、合成した電磁波を TRNG に印加する。これにより、TRNG を構成する全ての RO のエントロピーは抑制され、TRNG の乱数性が低下する。

従来の周波数注入攻撃では全ての RO を同時に低下させる攻撃条件を探索するために攻撃条件を掃引する必要があったが、本手法を用いることで各 RO の発振周波数の基本波もしくは高調波近傍の周波数について振幅を変化させて探索すればよいため、探索空間が狭まり、攻撃条件の推定が容易となる。

3.1.2 電磁波印加時間制御によるヘルステストをパス可能な乱数性低下攻撃

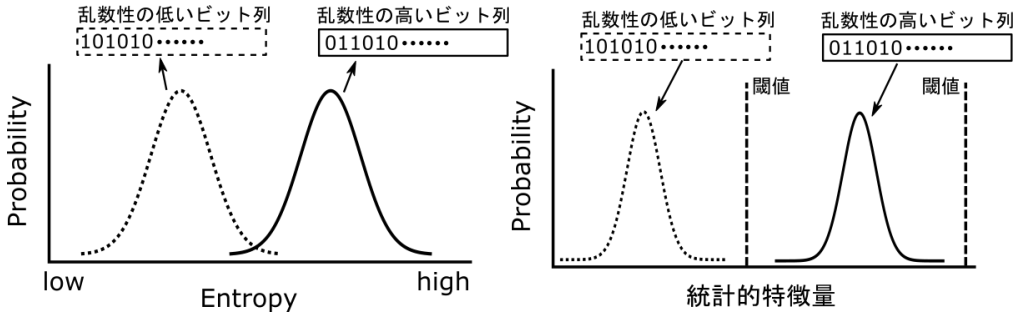
本節では、ヘルステストの概要を述べた後、攻撃対象である TRNG on-the-fly テストにおける、乱数性低下の評価手法について述べる。

従来の乱数性検定は、NIST の統計検定 [26] のようにソフトウェア上で大量のビット（10^6 ビット以上）に対して複数の統計検定を行うものであり、ハードウェア上に実装するにはコストが大きかった。そのため、近年ではハードウェア上で実装可能な軽量のヘルステストが複数開発されている [27, 28, 29]。ヘルステストには NIST の統計検定を簡素化したものなど様々な実装が存在する一方、全てのヘルステストが AIS-20/31 が定めた設計要件を満たしている訳ではない。

本論文で評価対象とする TRNG on-the-fly テスト [27] は、AIS-20/31 の設計要件を満たした乱数性の評価が可能なヘルステストの一つである。TRNG on-the-fly テストを用いることで、AIS-20/31 の設計要件を満たす様々な乱数性評価をコンパクトな回路規模で実現可能となる。以下に TRNG on-the-fly テストによる確率モデルを考慮した乱数性評価方法について説明する。

AIS-20/31 では、ヘルステストはエントロピー源の確率モデルに基づき、乱数列の統計的性質を評価するよう定めている [19]。TRNG on-the-fly テストでは、以下のように乱数列からエントロピー源の確率モデルを推定し、乱数性を評価している。

ビット列の乱数性は、図 3.6(a) のイメージ図のように、エントロピー源の確率モデルが反映される。乱数性の高いビット列は高いエントロピーの確率モデル（図 3.6(a) : 実線）から、乱数性が低いビット列は低いエントロピーの確率モデル（図



(a) エントロピー源の確率モデルと乱数性

(b) 確率モデルを反映した統計的特徴量の分布

図 3.6: TRNG on-the-fly テストの乱数性評価手法

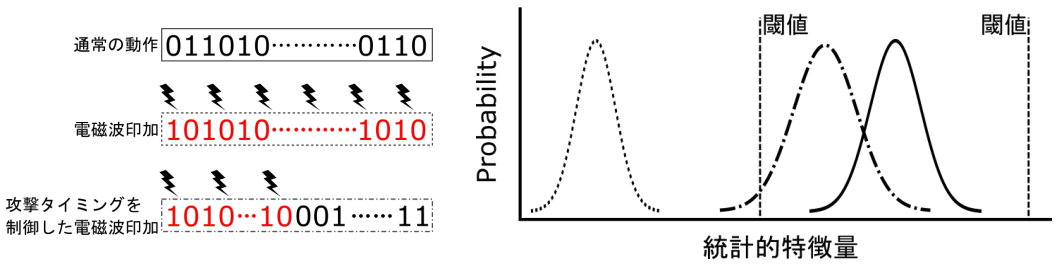


図 3.7: 電磁波印加タイミングの制御による乱数性と統計的特徴量の分布の変化

3.6(a)：点線）からそれぞれ生成される。これらの乱数列からエントロピーの確率モデルを推定するには、指標が必要となる。指標となる統計的特徴量にはビット列のバイアスやビット間の相関、特定のビットパターンの出現頻度など既存の統計検定 [7] を反映した様々な特徴量が提案されている [27]。ビット列から計算されるある統計的特徴量の分布がエントロピー源の確率モデルを効率よく推定可能なものを選択することで、図 3.6(b) のように乱数性の高いビット列（図 3.6(b)：実線）と乱数性の低いビット列（図 3.6(b)：点線）を有意に識別できる。

このように、TRNG on-the-fly テストでは、効率よくエントロピー源の確率モデルを推定する統計的特徴量を選択し、高エントロピー時の統計的特徴量の分布から得られる閾値によって、乱数性が高くヘルステストをパスするビット列と乱数性が低くヘルステストをパスしないビット列を識別する。乱数性の評価には、ある有意水準で乱数性を棄却する閾値を決定する。図 3.6(b) のような高エントロピー時の統計的特徴量の分布が正規分布に従う場合は、分布の平均値と標準偏差から閾値を決定する。AIS-20/31[19] や NIST SP800-20B[18] では、乱数性があるにもかかわらず、乱数性を棄却してしまう第一種の過誤を起こす確率を非常に低く定めるため、有意水準を 10^{-6} 以上のオーダーに定めることを求めている。

しかし、TRNG on-the-fly テストで推定される確率モデルは一回のヘルステストに使用する全てのビットの情報を含むため、推定された確率モデルは一回のヘルステストで使用する全てのビットに対して一様であるとみなされる。そのため、エントロピー源の確率モデルがビット列生成時に変化した場合は、適切に確率モデルを推定することは困難である。一方、周波数注入攻撃ではエントロピー源に電磁波を印加することでエントロピー源の確率モデルを変化させ、エントロピーを抑制することができる [15, 16, 17]。そのため、電磁波の印加タイミングを制御することで、エントロピー源の確率モデルを時間的に変化させれば、乱数性低下の検出困難化を引き起こすことができる可能性がある。

図 3.7 に本提案手法の概要を示す。まず、TRNG が攻撃を受けず、通常の動作を行う場合は、TRNG は乱数性の高いビット列を出力する。この時、ヘルステストで使用される統計的特徴量の分布は図 3.7 の実線のようになる。続いて、RO のエントロピーを低下させる電磁波をビット列が生成される全ての時間で印加した

場合、ヘルステストに使用する全ビットの乱数性が低下する。そのため、統計的特徴量の分布（図 3.7 : 点線）は乱数性が高いものと比べて、有意に変化する。このとき、乱数性を棄却する閾値を超えるため、ヘルステストをパスできない。これに対して、提案手法では電磁波印加タイミングを制御し、一部のビットのみに乱数性低下を引き起こす。これにより一部のビットは乱数性が低下するが、その他のビットについては高い乱数性をもつことになる。電磁波印加時と非印加時に生成されたビット列はそれぞれ乱数性の低い統計的特徴量の分布と乱数性の高い統計的特徴量の分布に従うが、全ビットに対して統計的特徴量が計算されることで、二つの分布とは異なる分布となる（図 3.7 : 一点鎖線）。電磁波の印加時間を変化させることで、この分布は変化するため、乱数性を棄却する閾値を超えない分布を選択できれば、ヘルステストによる乱数性低下の検知が困難な攻撃が可能となる。この時、閾値を超えずに乱数性を低下可能なビットの割合は、ヘルステストを行うビット長や有意水準、統計的特徴量の取り方と乱数性低下の生じ方によって異なる。

また、電磁波印加タイミングの制御には乱数生成のタイミングを示すトリガ信号の取得や電磁波印加時間を決定する必要がある。トリガ信号については周辺回路に伝導もしくは空間に放射された機器の内部状態を反映した電磁波によって、暗号モジュール中で生じる RO の動作開始に関連する信号を取得できる可能性があり、これを用いることで乱数生成のタイミングを推定可能である。既に、暗号処理に対する故障注入タイミングを制御可能なトリガ信号を機器外部から取得し、故障注入を行う手法 [24] や前章で示したように機器外部から RO の内部状態を含む信号の取得が可能であることから、トリガ信号の取得は容易であると考えられる。このトリガ信号に対して、電磁波印加時間を制御すれば、乱数性低下の検出を困難にする攻撃パラメタが決定可能であると考えられる。

3.2 ヘルステストを実装したROベースTRNGに対する周波数注入攻撃の実証

本章では、上述した原理と手法により、ヘルステストによる検知が困難な乱数性低下を引き起こすTRNGへの攻撃が可能であることを実験により示す。具体的には、電磁波の印加が容易なデバイスを仮定し、TRNGを実装するFPGAの実装を改変した後、印加する電磁波の振幅について基礎検討を行う。続いて、FPGAにTRNGを実装し、複数の正弦波印加により乱数性低下を引き起こすことが可能であることを示したのち、前述の乱数性低下を検知するヘルステストを実装したTRNGに対して電磁波の印加タイミングを制御した周波数注入攻撃を行うことで、乱数性が低下したビット列を出力させることが可能であることを示す。

3.2.1 リターン・ロス測定によるデバイスへの電磁波伝達効率の評価

本節では、実験に使用するFPGAに対して、印加する電磁波の伝達効率を評価するために、VNA（Vector Network Analyzer）を用いて、電磁波のリターン・ロスを測定し、印加する電磁波の振幅に関する基礎検討を行う。

本稿では、攻撃によってヘルステストに検知困難な乱数性低下を引き起こす理論を実証するため、電磁波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（図3.8）。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が駆動する1.2 Vの電源供給をレギュレータから分離し、1.2 V の電源をICに直接供給できるようにSMAポートを実装した。

TRNGが実装されたICモジュールに対する伝達効率の測定は難しいため、ここではFPGAのボードに対する入力電力の反射特性を評価した。測定では、FPGAボードに付加したSMAポートへの入力波に対するポートからの反射波をVNA（R&-S ZNB 8）によって測定することで、入力電力に対する反射電力の比であるリターン・ロスを取得した。これは入力電力に対して、反射電力がどの程度減衰したかをdBで示したものである。リターン・ロスが大きいほど、反射電力が小さくなり、FPGAのボード上に伝搬される妨害波の伝達効率が高くなる。一方、

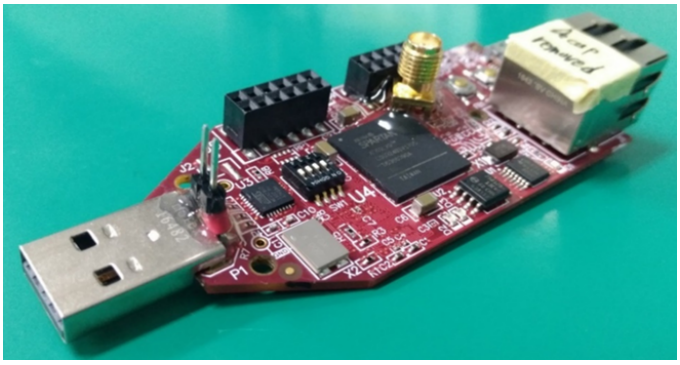


図 3.8: 改変した FPGA

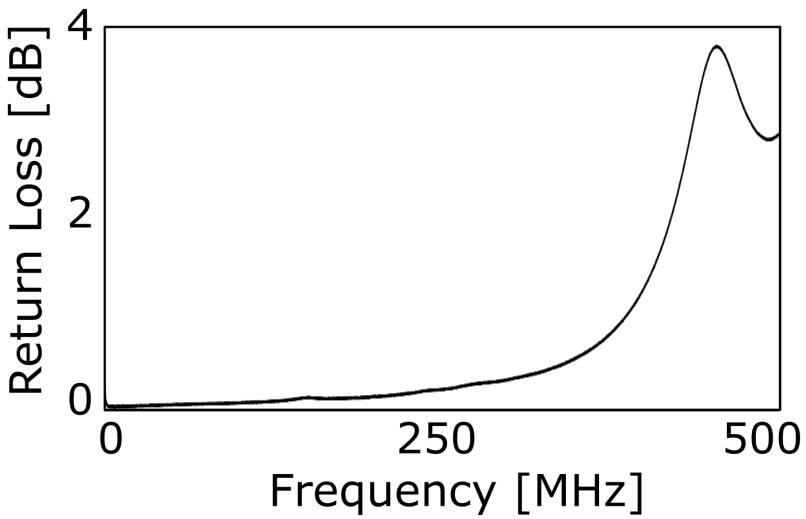


図 3.9: 攻撃対象の FPGA ボードのリターン・ロス

リターン・ロスが小さくなれば、反射電力が大きくなり、伝達効率が低くなることを示す。

図 3.9 に、改変した FPGA ボードに対して 0-500 MHz の周波数帯で測定したリターン・ロスを示す。図は妨害波の周波数に対するリターン・ロスを示している。低い周波数帯では、リターン・ロスの値が極めて小さいことが確認できる。これは入力電力に対して反射電力の減衰が小さく、入力電力がほぼ反射されることを示す。一方、高い周波数帯ではリターン・ロスが大きくなっていることから、反射電力が小さくなり、伝達効率が高くなっていることが確認できる。このことか

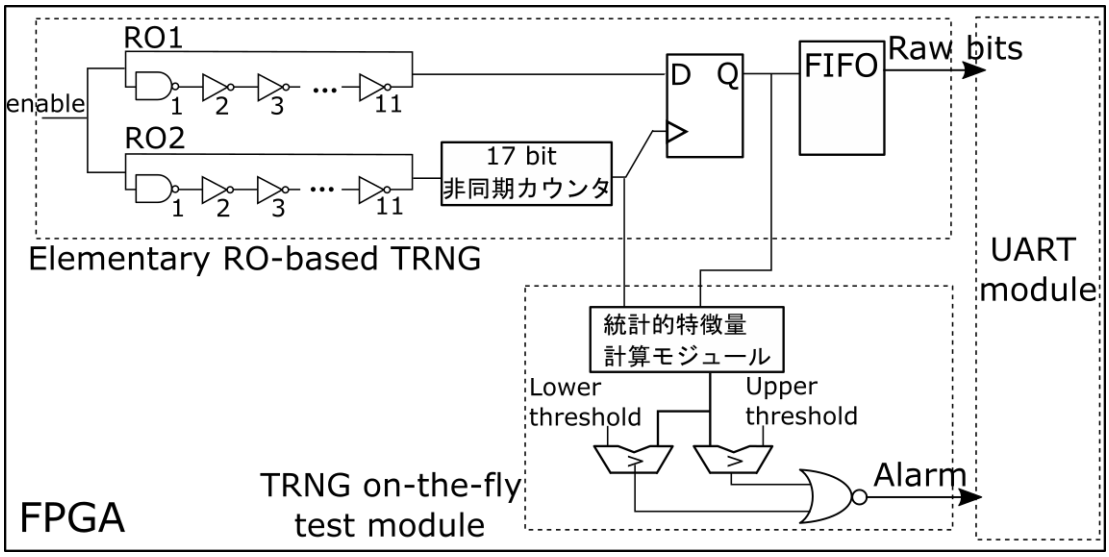


図 3.10: 攻撃対象の TRNG の実装

ら、印加する妨害波の周波数が低い場合は伝達効率が低いため、高い電力で妨害波を印加する必要があり、印加する妨害波の周波数が高い場合は伝達効率が高いため、必要となる電力が小さくなると予想される。但し、ここで測定したリターン・ロスはFPGA ボードに対する入力波の反射効率を評価したものであり、攻撃対象となる TRNG が実装された IC モジュールへの伝達効率を表すものではない。

3.2.2 ERO-TRNG の実装

実験に使用した FPGA の実装を説明する（図 3.10）。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、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、ヘルステストの結果と生成したビット列を UART モジュールから PC に送信する。

FPGA には RO をベースとした TRNG の中で回路の構成要素が最も少なく、他の RO ベースの TRNG の基本的なモデルとして考えられる Elementary RO-based TRNG (ERO-TRNG) [4] を実装し、攻撃対象のデバイスとして使用した。RO は共に 11 個の LUTs (Look-up tables) 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

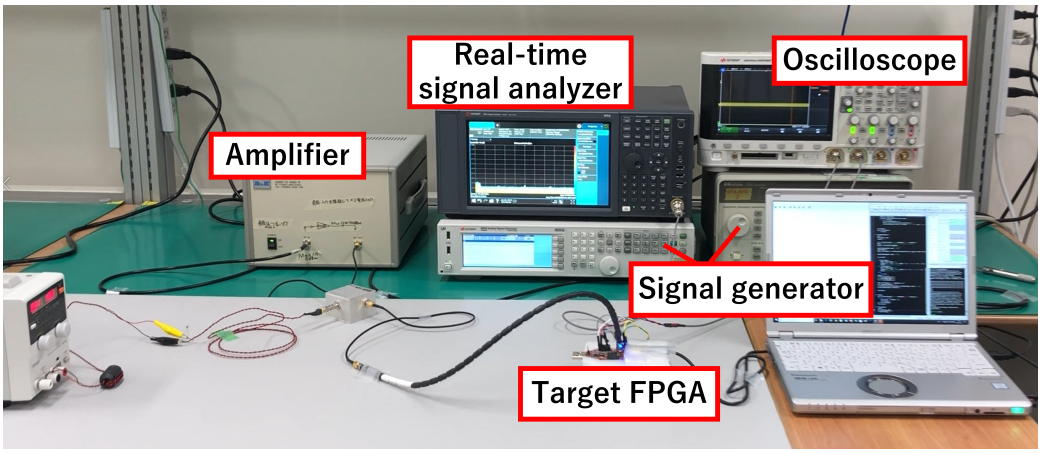


図 3.11: 実験セットアップ外観

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 RO1、サンプリングクロックを生成する RO を RO2 と呼ぶ。実装した TRNG の乱数性は事前に NIST の統計検定ツール [26] により確認した。

生成した乱数は TRNG on-the-fly テストモジュールにより、乱数性を検証する。一回のヘルステストで使用されるビット長が短いほど、乱数性低下を速く検知できることから、本稿では文献 [27] で使用された 512 ビットの乱数列に対して統計的特徴量をとり、乱数性を検証した。ヘルステストには隣接した 2 ビットの相関を評価可能な、重複しない 2 ビットの排他的論理和の総和とした。TRNG on-the-fly モジュールでは論理ゲートとカウンタを用いて、統計的特徴量を求めた後、コンパレータによって、閾値と比較して乱数性を検証する。閾値は事前に 512 ビットの乱数列を 8000 波形取得し、得られた統計的特徴量の分布から有意水準 10^{-9} となる [79, 177] とした。

3.2.3 実験セットアップ

図 3.11, 3.12 に実験セットアップを示す。ERO-TRNG と TRNG on-the-fly テストを実装した FPGA を攻撃対象のデバイスとする。実験には 3.2.1 節で使用した FPGA を使用した。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

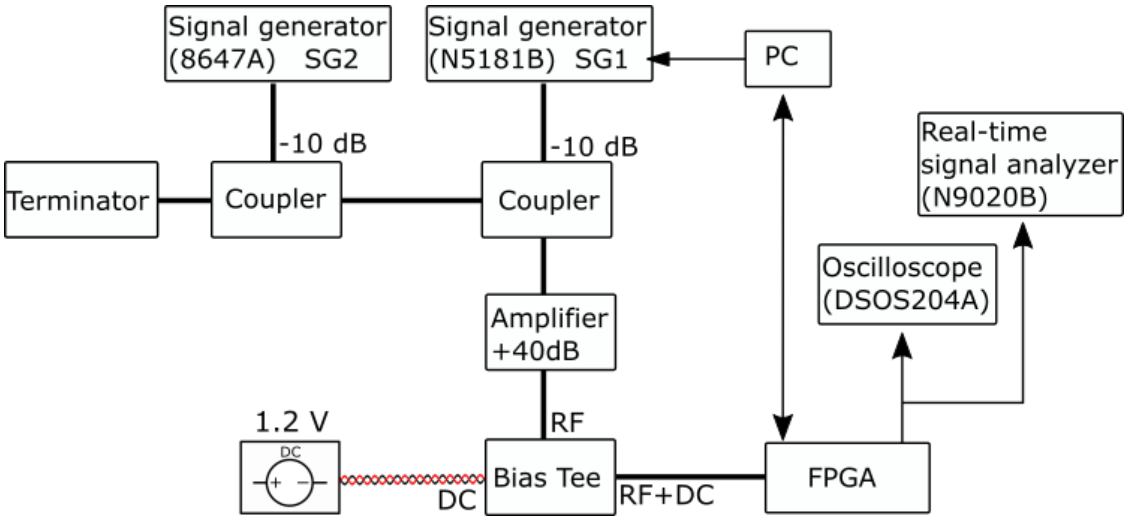


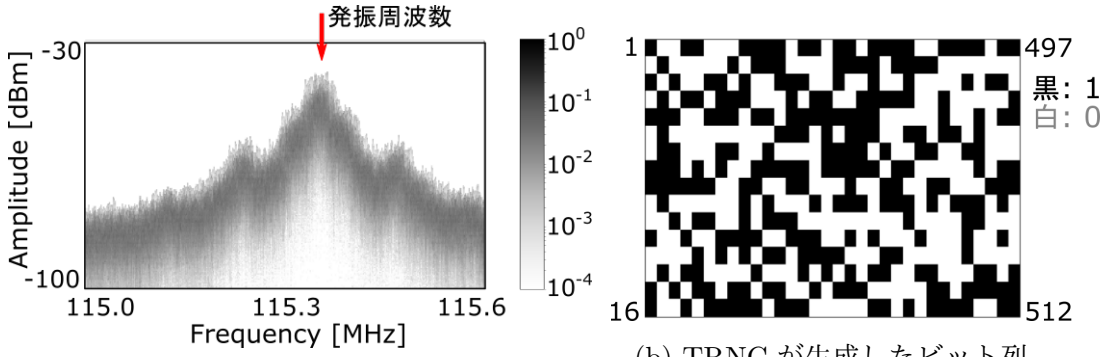
図 3.12: 実験セットアップのブロック図

ジェネレータを用いてそれぞれ生成する。これらの正弦波を方向性結合器とアンプ、Bias-Tee を介し、1.2 V の直流電流に合成し、改変した FPGA ボードの SMA ポートを介して FPGA に印加する。また、FPGA は PC から USB ケーブルを通じて給電される。

正弦波の印加タイミングの制御は、トリガ信号を得られたという仮定の下、印加する正弦波の振幅を変更する制御信号を PC からシグナルジェネレータに入力した。RO のエントロピーを評価するために、FPGA の I/O ピンから VDD/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、振幅確率を測定した。振幅確率は各 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。また、I/O ピンから出力した RO の出力信号とサンプリングクロックをオシロスコープによって時間領域で観測した。

3.2.4 周波数の異なる正弦波印加による TRNG の乱数性低下

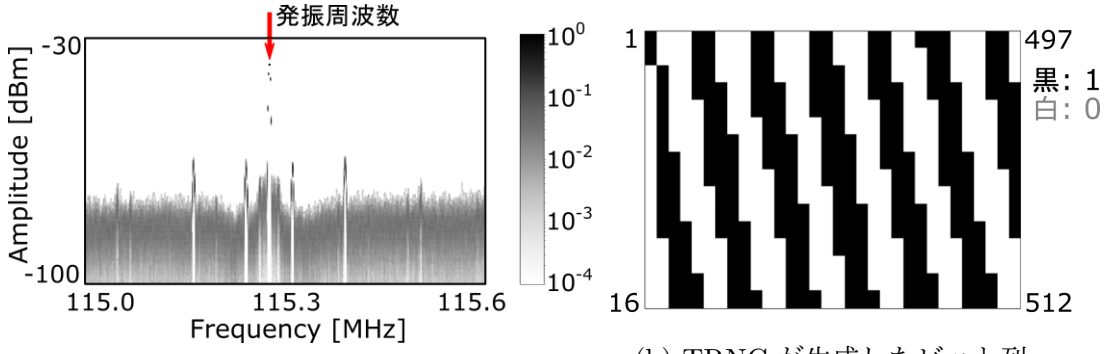
本節では、TRNG on-the-fly テストを実装した TRNG への攻撃の基礎検討として、RO の振幅の確率密度がエントロピーの低下を反映していることと、周波数の異なる正弦波印加により TRNG の乱数性を低下可能であることを示す。



(a) RO2 の振幅確率の分布

(b) TRNG が生成したビット列

図 3.13: 正弦波非印加時の振幅確率の分布とビット列



(a) RO2 の振幅確率の分布

(b) TRNG が生成したビット列

図 3.14: 正弦波印加時の振幅確率の分布とビット列

実験では、リアルタイムシグナルアナライザを用いて、VDD/GND 間の電圧スペクトルの振幅確率を観測することで RO のエントロピーを低下させる攻撃条件を探索した後、2 台のシグナルジェネレータから生成された周波数の異なる正弦波を印加しながら乱数生成を 100 回繰り返し、乱数列とヘルステストの結果を取得した。このとき、探索により決定した RO1 のエントロピーを抑制する正弦波の周波数は 219.0700 MHz、振幅は 30.5 dBm、RO2 のエントロピーを抑制する正弦波の周波数は 230.5512 MHz、振幅は 28.6 dBm であった。また、オシロスコープによって RO と非同期カウンタによって生成したサンプリングクロックを観測し、これらが正常に動作していることを確認しながら実験を行った。また、比較実験として正弦波非印加時のデータも同様に取得した。

図 3.13, 3.14 に正弦波非印加時と RO のエントロピーを低下させる正弦波印加時にリアルタイムシグナルアナライザによって計測した RO2 の振幅確率と TRNG が生成したビット列をそれぞれ示す。RO1 の振幅確率の分布は RO2 のものと同様の概形であったため、ここでは省略した。ビット列は左上を 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 32 列並べ、1 を黒、0 を白としたヒートマップで表した。図 3.13 は正弦波非印加時に取得した振幅確率とビット列である。図 3.13(a) では RO がもつエントロピーである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。また、生成されたビット列（図 3.13(b)）に明確な乱数性低下は確認されず、取得した全てのビット列でヘルステストにパスした。

一方、RO のエントロピーを低下させる周波数の異なる正弦波を印加した場合に観測された結果を図 3.14 に示す。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 3.14(a)）。このとき、TRNG が生成したビット列は図 3.14(b) のように明らかに乱数性が低下し、周期性を持つことが確認できる。また、実装したヘルステストはこの乱数性低下を検知し、取得した全てのビット列でヘルステストをパスしなかった。

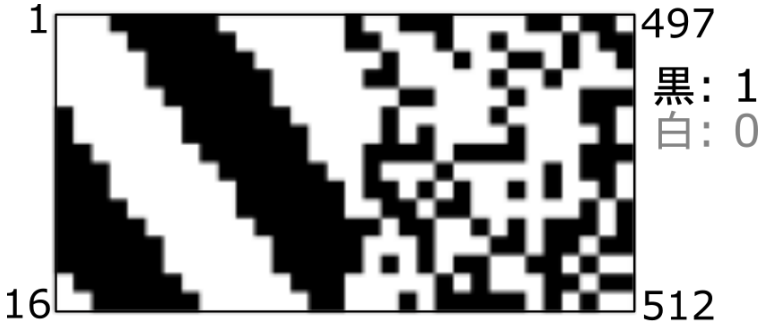
以上より、振幅確率を用いて各 RO のエントロピーを抑制可能な攻撃条件が決定可能であることと、その条件を用いた周波数の異なる正弦波の印加により、乱数性低下を引き起こすことが可能であることを確認した。

3.2.5 正弦波印加タイミングの制御による TRNG の乱数性の変化

本節では、電磁波印加タイミングを制御することで、乱数性を低下させるビット数を制御可能であること、それによりヘルステストが乱数性低下を検知する割合を操作可能であることを実証する。

実験では、トリガ信号を得られたという前提の下、印加する正弦波の操作を行った。具体的には、PC から TRNG を動作させる信号を送り、制御プログラム上で一定の遅延時間の後にシグナルジェネレータが生成する正弦波の振幅を 3 dB 低下させることで、RO1 のエントロピー抑制を中止した。簡単のため、操作するシ

(a) TRNG が生成したビット列（遅延時間 500 ms）



(b) TRNG が生成したビット列（遅延時間 300 ms）

(c) TRNG が生成したビット列（遅延時間 100 ms）

図 3.15: 正弦波印加時間の変化による乱数性の変化

表 3.1: 正弦波印加時間とヘルステストをパスした割合

遅延時間	ヘルステストをパスした割合
500 ms	0 %
300 ms	52 %
100 ms	100 %

グナルジェネレータは RO1 のエントロピーを抑制する正弦波を生成する 1 台のみとし、もう一台は常に一定の正弦波を印加し続けた。遅延時間は 500 ms, 300 ms, 100 ms の 3 条件とし、それぞれに対して 50 回の測定を行い、ビット列とヘルステストの結果を取得した。また、TRNG のエントロピーを低下させる正弦波の印加条件は事前に探索し、RO1 に対しては周波数 219.460 MHz、振幅 30.5 dBm、RO2 に対しては周波数 230.967 MHz、振幅 28.6 dBm とした。

図 3.15 に RO1 のエントロピーを抑制する正弦波の印加タイミングを制御した時の各遅延時間における代表的なビット列を示す。また、表 3.1 に各遅延時間においてビット列がヘルステストにパスした割合を示す。図 3.15(a) は遅延時間を 500 ms に設定したときの TRNG が生成したビット列である。ビット列に周期性がみられ、乱数性が低下していることが確認できる。また、多くのビットに乱数性低下がみられ、7 から 8 割程度のビットの乱数性低下が確認できる。この時、取得した 50 個のビット列の全てがヘルステストをパスすることはできなかった。続いて、遅延時間を 300 ms にしたときのビット列（図 3.15(b)）では、図 3.15(a) 同様の周期性が全ビットの約 5 割で確認できる。このとき、ヘルステストをパスした割合は 52 %であった。最後に、遅延時間を 100 ms に設定した条件では、図 3.15(c) のように全ビットの約 2 割のビットに他の条件と同様の乱数性低下が確認できる。このとき、全てのビット列で乱数性低下は検知されず、ヘルステストにパスした。

以上より、正弦波の印加時間を制御し、RO のエントロピーを抑制する時間を操作することで、TRNG の乱数性を低下させるビットの割合を変更可能であり、これによりヘルステストをパスするビットの割合を操作できることを実証した。

3.3 考察

本節では、3.2 節で述べた乱数性低下攻撃が、実デバイスのセキュリティに与える影響について考察を行う。

現在、広く一般に普及している暗号アルゴリズムである AES（Advanced Encryption Standard）[30] が実装された暗号ハードウェアに対するサイドチャネル攻撃の一つに、相関電力解析（CPA: Correlation Power Analysis）が存在する [14]。この攻撃は、暗号回路の動作に伴い生じる物理的な動作情報（消費電力等）を複数測定し、統計的に処理することで暗号処理時の中間値を予測し、秘密鍵を特定する攻撃手法である。この攻撃は秘密鍵の特定を容易にし、機密性を大きく低下させることから、これまでに攻撃に対する様々な対策技術が検討されてきた。

この CPA に対する対策手法の一つに乱数を利用して入力にマスクをかける、1st-order Boolean masking が存在する [31, 32, 33]。この対策手法は、演算に用いる値とランダムな乱数の排他的論理和をとることで、入力値に変換を施し、暗号処理時に生じる電力消費などのサイドチャネル情報と秘匿すべき情報であるマスキングされていないときの真の中間値との関係を独立にすることで、秘密鍵の特定を困難化する手法である。マスキングを用いることで、CPA によってサイドチャネル情報と中間値の関係を推定できたとしても、その中間値自体は真の中間値と無関係な値をとるため、秘密情報の解析が困難となる。マスキングに使用する乱数の生成は、暗号ハードウェアに組み込まれた TRNG の用途の一つである。

一方、この 1st-order Boolean masking による対策の性能は、マスクに使用する乱数の乱数性に依存することが知られている。既に、マスキングに使用する乱数列のビットに偏りがある場合や、連続する 4 ビットの出現頻度に偏りがある場合、CPA による鍵解読が成立する可能性が示されている [34]。本章で使用したような 512 ビットの乱数を生成し、ヘルステストを行うデバイスにおいて、生成した乱数列の最初の 128 ビットを AES-128 のマスキングに使用することを仮定した場合、本章で示した攻撃により図 3.15(b) のように乱数性低下が生じた場合、連続する 4 ビットの出現頻度に有意に偏りが存在することから、文献 [34] と同様に、CPA による鍵解読が実現する可能性が高い。このことから、本章で提案した攻撃手法による RO をエントロピー源とする TRNG の乱数性低下は CPA への対策手

法の一つである 1st-order Boolean masking を無効化し、鍵解読を容易にする可能性があると考えられる。

また、実験では単一の統計的特徴量を用いて乱数性評価を行うヘルステストに対して、乱数性低下の検知を困難化可能であることを実証したが、複数の統計的特徴量を用いたヘルステストについても同様の手法で攻撃が可能であると考えられる。加えて、周波数注入攻撃のようにエントロピー源に対して高速にエントロピーを変化させることができる攻撃であれば、同様の原理でヘルステストをパスすることができると考えられる。そのため、ヘルステスト実行時に乱数性が変化する可能性も踏まえて、ヘルステストを設計することが望ましいと考えられる。

3.4 まとめ

本章では、実際のデバイスを模した環境である FPGA 上に実装されたヘルステストを伴う TRNG に対する周波数注入攻撃の可能性を実証するため、複数の信号源を用いた正弦波の印加と電磁波印加時間の制御により、ヘルステストをパス可能な乱数性低下を引き起こす攻撃手法を提案した。そして、ERO-TRNG と TRNG on-the-fly テストを実装した FPGA に対して攻撃を行うことで、ヘルステストに検知されることなく、一部のビットに乱数性低下を引き起こすことが可能であることを示した。

本手法を用いた周波数注入攻撃は、従来は攻撃の対象外とみなされてきたヘルステストを実装した TRNG に対しても乱数性低下を引き起こすことから、攻撃に対する適切な対策手法を適用すべきであると考えられる。

4. ROベースのTRNGのセキュリティ評価と対策手法の考察

本章では、前章までに示した周波数注入攻撃による脅威に対して、RO ベースの TRNG に対するセキュリティ評価を行う手法と攻撃への対策手法に関して考察を行う。本論文におけるこれまでの議論に基づき、RO ベースの TRNG の攻撃耐性評価手法について検討した後、第二章で示した非侵襲攻撃に対する対策手法と第三章で示した乱数性低下攻撃を検知可能なヘルステストの構成について考察を行う。

4.1 ROベースのTRNGに対する攻撃耐性評価手法の検討

本節では、周波数注入攻撃に対して RO ベースの TRNG を実装した機器の攻撃耐性を評価する手法について検討を行う。

周波数注入攻撃に対する RO ベースの TRNG の攻撃耐性を評価するには、TRNG に対して印加する電磁波を掃引して、乱数性低下が生じるかを評価することが考えられる。従来の周波数注入攻撃では、単一の正弦波を印加することで複数の RO のエントロピーを同時に抑制し、TRNG の乱数性を低下させてきた。しかし、第三章で示したように各 RO のエントロピーを低下させる正弦波を推定し、複数の正弦波を同時に印加することで TRNG の乱数性を低下させる可能性が存在する。そのため、TRNG のセキュリティを評価するには、出力される乱数の乱数性を評価するのではなく、TRNG を構成する各 RO のエントロピーが低下する可能性について評価することが重要であると考えられる。

各 RO のエントロピーを評価するには、時間領域におけるジッタを評価する手法が存在する [25] が、各 RO の信号を独立に取得可能な出力を用意する必要がある。加えて、電磁波を印加することで、RO の出力信号に加えて印加した妨害波が観測され、ジッタを適切に評価できない可能性もある。また、デジタル回路上でジッタを評価する手法 [35, 36] 等も提案されているが、追加の回路を実装する必要があるため、簡易に攻撃耐性評価を行うことは難しい。

これに対して、第三章で示したROの確率密度を利用したエントロピー評価手法を拡張することで、独立したROの出力信号を必要とせず、周波数領域で観測するため攻撃による観測信号への影響を抑制可能であり、追加の回路実装を必要としない攻撃耐性評価が行うことができる可能性がある。既に、環境電磁工学（EMC）の分野では、確率密度の累積分布である振幅確率分布（APD: Amplitude Probability Distribution）測定を利用した、機器に対するノイズや電波の干渉といったEMC評価を行う試験法が存在する[37]。第三章で示したようにROのエントロピーが低下するとROの発振周波数近傍の確率密度の分布が大きく変化することから、理想的なAPD波形の変化と攻撃によるAPD波形の変化を比較し、閾値を設けることで、各ROのエントロピー低下を評価できる可能性がある。APD測定を行いながら、電磁波の印加条件を掃引し、各ROに対する攻撃条件を探索することで、攻撃による乱数性低下が発生し得るかを評価することができる。EMC評価に使用されるAPDを利用して乱数性の評価ができれば、EMC試験と同様にセキュリティ評価を実行できると考えられる。また、APD測定を利用した攻撃耐性評価手法で得られた各ROのエントロピーを抑制する攻撃条件から、次節で示す対策技術を適用することで周波数注入攻撃の対策が可能であると考えられる。

4.2 非侵襲な電磁波印加攻撃に対する対策技術の検討

本節では、二章で示した非侵襲な周波数注入攻撃への対策技術として、妨害波の伝達効率に着目した対策手法の検討を行う。

周波数注入攻撃によりROのエントロピーを抑制するには、印加する正弦波の周波数と振幅の二つの条件を適切に設定することが必要である。周波数の条件はROの発振周波数に依存し、特定周波数の正弦波印加によってエントロピーを抑制可能である。一方、振幅については、印加した電磁波がどの程度VDD/GND間の電圧を振動させるかが重要となり、この条件は印加した電磁波がICモジュールに到達するまでの伝達効率に依存する。伝達効率は周波数によって異なり、伝達効率の高い周波数の電磁波を印加することで、減衰が少なく効率よく伝達する一方、伝達効率が低い周波数の電磁波の印加は、減衰が大きくROのエントロピーを抑制することは難しくなる。このことから、電磁波印加を利用したTRNGへ

の攻撃への対策を検討する方針として、デバイスの設計段階においてROのエントロピーを抑制可能な周波数帯において高い伝達効率を持つ回路構成を避けることが望ましい。しかし、回路設計段階において、回路を搭載する基板もしくはデバイスの設置環境全体の伝達特性を考慮することは困難である。そのため、現実的には回路設計後にROのエントロピーを抑制可能な周波数を評価し、その周波数帯において妨害波を減衰させるフィルタを基板上もしくはハードウェアの実装環境において付加する方法が考えられる。

また、簡単な対策手法として、電源線やコミュニケーションケーブルにフェライトコアを巻き付け、妨害波を含むノイズの機器内部への侵入を防ぐ方法が考えられる。前節で検討した攻撃耐性評価手法によって、ROのエントロピーを低下させ得る周波数帯の伝達効率を低下させる特性を持つフェライトコアを設置することで、電磁波印加によるTRNGの乱数性低下を困難化できる。

4.3 電磁波印加時間制御による乱数性低下に耐性を持つヘルステストの考察

本節では、第三章に示した電磁波印加タイミング制御によるヘルステストをパス可能な乱数性低下攻撃に対して、耐性を持つヘルステストについて考察を行う。

ヘルステストに用いるビット列の一部にのみ生じた乱数性低下がTRNG on-the-flyテストによって評価困難である理由として以下の二つの要因が挙げられる。まず、有意水準が低いことである。3.1.2節で述べたように、NISTのSP800-90B[18]やAIS-20/31[19]では、ビット列が乱数性を持つにもかかわらず、乱数性を棄却してしまう第一種の過誤を起こす確率を低くするために、有意水準を低く設定している。その結果、実際には乱数性をもたないが、乱数性をもつと評価される第二種の過誤を起こす確率が高くなっている。このような有意水準が設定されている理由の一つとして、ヘルステストはエントロピー源の故障の検知を目的としており、このような高度な攻撃手法は想定していないことが要因として挙げられる。そのため、ヘルステストを設計する際には、TRNGの実装や攻撃によるエントロピー源の可制御性等を考慮して、攻撃の実現可能性を検討し、攻撃が実現する場

合は乱数性低下を生じるビット数が許容可能な範囲に収まるように、有意水準を設定するのが望ましい。

二つ目は、ビット列に対して一様に乱数性を評価しているため、乱数性の変化を検知することが難しいことである。乱数性はビット列に対して評価されるものであり、各ビットに対する乱数性の評価は難しい。そのため、ビット列に対するヘルステストでは 512 ビットといった複数ビットを合わせて乱数性を評価する必要がある。一方、エントロピー源を直接評価するヘルステストも提案 [38, 39] されており、このようなヘルステストを用いることで、エントロピーの低下自体を検知可能である。但し、この手法は各 RO に対して多数の遅延素子を必要とするため、TRNG よりも回路規模が大きくなる。

4.4 まとめ

本章では、前章までに示した実際のデバイスに対する周波数注入攻撃に対して、セキュリティ評価手法と対策手法を検討した。RO ベースの TRNG に対して、エントロピー源に着目して、攻撃耐性評価を行い、TRNG の乱数性を低下させる電磁波の周波数帯の伝達効率を低下させることで、攻撃に対する耐性が高まることが期待される。また、ヘルステストの実装についても考察を行い、ヘルステストに対して十分な回路規模が得られるのであれば、エントロピー源を直接評価するヘルステストを実装することで攻撃を防ぐことが期待できる。

5. 結論

本論文では、RO ベースの TRNG に対して実際のデバイスへの攻撃の実現可能性を評価するのに重要となる、(1) 攻撃対象の機器にどの程度接近可能であり、侵襲や改変を施すことが可能か、(2) 乱数性低下を検知する機構など攻撃を困難化する実装が施されているか、については十分に議論されていないことを指摘し、実際のデバイスに対する周波数注入攻撃の影響範囲について検討を行った。

第二章では、従来のセキュリティ評価では考慮されていない、デバイスへの物理的な接近や侵襲・改変が困難な環境下における周波数注入攻撃の可能性を指摘した。そして、デバイス遠方からの電磁波注入と TRNG から生ずるコモンモード電流をサイドチャネル情報として乱数性を判定する手法を提案し、CMOS インバータで構成される RO ベースの TRNG のモデルに対して攻撃を実証することで、デバイスに対する物理的な接近や侵襲が困難なデバイスに対しても攻撃の可能性があることを示した。

第三章では、ヘルステストを実装した TRNG に対する周波数注入攻撃の可能性を指摘し、実際のデバイスを模した環境において攻撃条件の推定が容易な電磁波印加手法と電磁波印加タイミングの制御によるヘルステストをパス可能な乱数性低下を引き起こす手法を提案した。実験では、ERO-TRNG と TRNG on-the-fly テストを実装した FPGA に対して攻撃を行うことで、ヘルステストに検知されることなく、一部のビットに乱数性低下を引き起こすことが可能であることを示した。

第四章では、前述の攻撃に対する TRNG のセキュリティ評価手法を議論した後、攻撃への対策手法とヘルステストの実装について検討を行った。

以上の議論より、本論文では、RO ベースの TRNG に対して、(1) デバイスへの物理的な接近や侵襲・改変が困難な環境下において、(2) ヘルステストを実装した TRNG に対する乱数性低下攻撃が実現可能であり、TRNG を実装する多くのデバイスに対して周波数注入攻撃が成立し得ることを示した。従来の RO ベースの TRNG に対するセキュリティ評価では、スマートカードなどを主な対象とし、ヘルステストが実装されていないことを前提として攻撃の実現可能性を評価してきたが、機器への侵襲が困難なデバイスやヘルステストが実装されたデバイ

スに対しても周波数注入攻撃が実現する可能性があり、これらの機器についても対策手法を適用すべきであると考えられる。攻撃への対策技術を講じるには、従来検討されていたような侵襲攻撃に対する対策も重要であるが、第四章で考察したようなEMCに関する知見を取り入れた外来ノイズ対策等の非侵襲攻撃への対策も検討する方が望ましい。また、実装するヘルステストについても第三章で示した電磁波印加時間の制御による周波数注入攻撃のような乱数性を変化させる攻撃が実現可能かを検討したうえで、適切な有意水準やヘルステストを考慮する必要があると考えられる。

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藤川和利教授には、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。

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。

本学藤本大介助教には、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。

仙台高等専門学校衣川昌宏助教には、日頃の研究活動において様々な御支援、御助言を頂き、感謝申し上げます。

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] Y. Hu, X.Liao, K. Wong and Q.Zhou, "A true random number generator based on mouse movement and chaotic cryptography," Chaos, Solitons & Fractals, vol.40, no.5, pp.2286-2293, 2009.

[2] M. Rohe, "RANDy-A true-random generator based on radioactive decay." Technical report, Saarland University, pp.1-36, 2003.

[3] B. Sunar, W.J. Martin, D.R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," IEEE Trans. Comput, vol.56(1), pp.109–119, 2007.

[4] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux, "On the security of oscillator-based random number generators," Journal of Cryptology, vol. 24, no. 2, pp. 398–425, 2011.

[5] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for FPGAs," in Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays. ACM, pp. 71–78, 2004.

[6] V. Fischer and M. Drutarovsky, "True random number generator embedded in reconfigurable hardware," in Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES2002), ser. LNCS, vol. 2523, Redwood Shores, CA, USA. Springer Verlag, pp. 415–430, 2002.

[7] M. Varchola and M. Drutarovsky, "New high entropy element for FPGA based true random number generators," in Cryptographic Hardware and Embedded Systems, CHES 2010. Springer, pp. 351–365, 2010.

[8] A. Cherkaoui, V. Fischer, A. Aubert, and L. Fesquet, "A self-timed ring based true random number generator," in IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC 2013), pp. 99–106, 2013.

[9] B. Yang, V. Rožić, M.Grujic, N. Mentens and I. Verbauwhede, "ES-TRNG: A High-throughput, Low-area True Random Number Generator based on Edge Sampling," IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES2018), pp.267-292, 2018.

[10] B. Jun and P. Kocher, "The Intel random number generator," Cryptography Research Inc. white paper, 1999.

[11] C.S. Petrie and J.A. Connelly, "A noise-based IC random number generator for applications in cryptography," IEEE transactions on circuits and systems, vol. 47, no. 5, 2000.

[12] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti and M. Varanonuovo, "A high-speed oscillator-based truely ransom number source for cryptographic applications on a smart card IC," IEEE transactions on computers, vol. 52, no. 4, 2003.

[13] P. Kocher et al., "Differential power analysis," Springer-Verlag, LNCS, vol. 1666, pp.388-397, 1999.

[14] 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.

[15] A.T. Markettos, S.W. Moore, "The frequency injection attack on ring-oscillator-based true random number generators," CHES, vol.5747, pp.317-331, 2009.

[16] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, P. Maurine, "Contactless electromagnetic active attack on ring oscillator based true random number generator", Constructive side-channel analysis and secure design, COSADE, Vol.7275, pp.151–166, 2012.

[17] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, “ Fault model of electromagnetic attacks targeting ring oscillator-based true random number generators, ” Journal of Cryptographic Engineering, vol.6, no.1, pp.61-74, 2016.

[18] 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.

[19] 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.

[20] B. Mesgarzadeh, A. Alvandpour, “ A study of injection locking in ring oscillators, ” Proc. IEEE International Symposium on Circuits and Systems, vol. 6, pp. 5465–5468, 2005.

[21] J. Drewniak, F. Sha, T. Van Doren, T. Hubing, J. Shaw, “ Diagnosing and modeling common-mode radiation from printed circuit boards with attached cables, ” Proc. IEEE Symp. Electromagn. Compat., pp. 465–470, 1995.

[22] D. Hockanson, J. Drewniak, T. Hu Bing, T. Van Doren, F. Sha, M. Wilhelm, “ Investigation of fundamental EMI source mechanisms driving common-mode radiation from printed circuit boards with attached cables, ” IEEE Trans. on

[23] Electromagnetic Compatibility, vol. 38, no. 4, pp. 557–566, 1996. T.H. Hubing, “ Printed circuit board EMI source mechanisms, ” Proc. IEEE Symp. Electromagn. Compat., vol. 1, pp. 1–3, 2003.

[24] Y. Hayashi, T. Sugawara, Y. Kayano, N. Homma, T. Mizuki, A. Satoh, T. Aoki, S. Minegishi, H. Sone, H. Inoue, “ An analysis of information leakage from a cryptographic hardware via common-mode current, ” EMC’09, pp. 17–20, 2009.

[25] A. Hajimiri., S. Limotyrakis and T.H. Lee, “ Jitter and phase noise in ring oscillators, ” IEEE Journal of Solid-State Circuits, Vol.34(6), pp.790–804, 1999.

[26] A. Rukhin, J. Sato, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, “ A statistical test suite for random and pseudorandom number generators for cryptographic applications ”, Technical Report SP800-22 Rev. 1a, National Institute of Standards and Technology, USA, 2010.

[27] B. Yang, V. Rožić, N. Mentens, W. Dehaene and I. Verbauwhede, “TOTAL: TRNG on-the-fly testing for attack detection using lightweight hardware. ” Proceedings of the 2016 Conference on Design, Automation & Test in Europe. EDA Consortium, pp.127-132, 2016.

[28] A. Vaskova, C. Lo´ pez-Ongil, E. San Milla´ n, A. Jime´ nez-Horas, and L. Entrena, “ Accelerating secure circuit design with hardware implementation of DIEHARD battery of tests of randomness, ” in 12th IEEE International On-Line Testing Symposium (IOLTS), 2011.

[29] V. B. Suresh, D. Antonioli, and W. P. Burleson, “On-chip lightweight implementation of reduced NIST randomness test suite, ” in Hardware Oriented Security and Trust (HOST), pp.93–98, 2013.

[30] National Institute of Standards and Technology(NIST),“An-noucing the ADVANCED ENCRYPTION STANDARD(AES), ” `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`, 2001.

[31] S. Chari, C.S. Jutla, J.R. Rao and P. Rohatgi, “ Towards Sound Approaches to Counteract Power-Analysis Attacks,” Advances in Cryptology - CRYPTO ’ 99, vol. 1666 of Lecture Notes in Computer Science, pp. 398–412, 1999.

[32] L. Goubin and J. Patarin, “ DES and Diffrential Power Analysis (The ” Duplication ” Method), ” Cryptographic Hardware and Embedded Systems

- CHES ' 99, vol. 1717 of Lecture Notes in Computer Science, pp. 158–172, 1999.

[33] C. Herbst, E. Oswald and S. Mangard, "An AES smart card implementation resistant to power analysis attacks," Applied Cryptography and Network Security - ACNS 2006, vol. 3989 of Lecture Notes in Computer Science, pp. 239–252, 2006.

[34] K.U. Leuven, "Report on the Security Evaluation of Cryptographic Algorithms and Countermeasures when non Ideal Hardware Building Blocks are Used," 2017.

[35] B. Valtchanov, A. Aubert, F. Bernard, and V. Fischer, "Modeling and observing the jitter in ring oscillators implemented in FPGAs," in DDECS, pp. 158–163, 2008.

[36] B. Yang, V. Rožić, M. Grujic, N. Mentens and I. Verbauwhede, "On-chip jitter measurement for true random number generators," 2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), pp. 91-96, 2017.

[37] K. Wiklundh, "Relation between the amplitude probability distribution of an interfering signal and its impact on digital radio receivers", IEEE Transactions on EMC, vol. 48(3), pp. 537-544, 2006.

[38] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux, "On the security of oscillator-based random number generators," Journal of Cryptology, vol. 24, no. 2, pp. 398–425, 2011.

[39] V. Fischer and D. Lubicz, "Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG," in CHES2014, pp. 527–543, 2014.

著者発表論文

1. S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, Arthur Beckers, Joseph Balasch, Benedikt Gierlichs and Ingrid 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, DOI: 10.1109/TEMC.2018.2844027, 2018.

2. 大須賀彩希, 藤本大介, 林優一, 本間尚文, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid 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）, 新潟, 1D2-4, 2018.1.23.

3. S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs, I. Verbauwhede,"Fundamental Study on Non-invasive Frequency Injection Attack against RO-based TRNG," 2018 Joint IEEE EMC & APEMC, Singapore, TU-PM-I-TC-05-1, 2018.5.15.

4. 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.

5. S. Osuka, D. Fujimoto, N. Homma, Arthur Beckers, Joseph Balasch, Benedikt Gierlichs, Ingrid Verbauwhede and Y. Hayashi, "Fundamental study on degradation of randomness in TRNG due to intentional electromagnetic interference," EMC Joint Workshop 2018, Daejon, 2018.11.22.

6. 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.

7. 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.