TDC の操作による PUF ステート復元攻撃の 難易度評価のためのシミュレーション

山下 晃平^{1,a)} 李 陽¹ 菅原 健¹

概要: Physically Unclonable Function (PUF) とは、半導体集積回路の製造によって生じる個体の物理的な特性のランダムなばらつきを積極的に取り出す技術である。暗号モジュールにおける静的リバースエンジニアリング対策として近年期待されている。最近、PUFのID(ステート)生成の際に Time-to-Digital Converter を用いる PUF に対し、 クロックを操作することでステートをバイアスし、現実的な計算量でステートを復元する攻撃が提案された。本稿では、その攻撃の実現に至るために、どの程度のクロック操作能力の水準を有する必要があるのか計算機シミュレーションで評価する。これは、著者らによる先行研究 [18] を進めたものであり、クロック操作の最大偏向の評価を行った。

キーワード:時間-デジタル変換器,フィジカリーアンクローナブルファンクション,故障注入攻撃,シグナルインジェクション攻撃

Simulation-Based Evaluation of PUF State Recovery Attack using TDC

Kohei Yamashita^{1,a)} Yang Li¹ Takeshi Sugawara¹

Abstract: Physically unclonable function (PUF) generates a device-unique identifier by using the chip's physical characteristics caused by the manufacturing variation of semiconductor integrated circuits. PUF is now an indispensable building block for cryptographic modules as an efficient countermeasure against reverse-engineering attacks. Recently, a new attack was proposed for PUFs that use a time-to-digital converter (TDC) for digitizing the device-unique physical quantity. An attacker manipulates the TDC's clock to bias the generated PUF ID (state), thereby enabling an exhaustive search with a practical effort. In this paper, we evaluate the relationship between the attacker's capability on clock manipulation and the efficiency of the state-recovery attack through simulation. This work is based on our previous work [18], and we evaluate the maximum deviation of clock frequency.

Keywords: Time-to-Digital Converter, Physically Unclonable Function, Fault Injection Attack, Signal Injection Attack

1. はじめに

暗号は、情報を隠しながら通信を行う秘匿通信や、認証 のため必要不可欠な技術である。暗号の秘密は鍵に宿るた め、安全な鍵管理が重要な課題である。秘密鍵を安全に保 管するために、暗号処理に必要なハードウェアー式をモ ジュール化する利用法がよくとられる。最近では、マイクロコントローラに暗号モジュールを搭載した製品が発売されている [1]. 暗号モジュールは、正規の利用者からの攻撃を受けることを想定する。暗号モジュールが正規の利用者から攻撃される場合、攻撃者の手元で動作するので、プローブを当てて消費電力を解析したり、故意に異常な動作を誘発する等の物理的な接触を伴って攻撃される [2], [3].特に、電源が投入されていない状態のチップを開封して、電子顕微鏡で不揮発性メモリを観察することで、記録され

¹ 電気通信大学 情報理工学域
Department of Informatics, The University of Electro-Communications

a) yamashita@uec.ac.jp

た情報を直接見るような静的リバースエンジニアリングは、秘密鍵を直接見ることができるので、強力な攻撃である [4], [5].

Physically Unclonable Function (PUF) は、半導体集積 回路の製造ばらつきから、チップ固有の ID を取り出す技術である。暗号モジュールにおけるビルディングブロックとして近年期待されている技術である [6]、[7]. PUF の ID (以下、ステートと呼ぶ)を、デバイス固有の秘密鍵(PUF鍵)として利用できる。さらに、PUF鍵で事前共有鍵をくるむことで、PUFを鍵保管庫として利用することができる。この鍵保管庫は個体に電源を投入した動作時しか生成されないため、静的リバースエンジニアリングへの対策になる [8]. 実際、最近では、マイクロコントローラに PUFによる鍵保管庫を搭載した製品が発売されている [9].

応用と並行して、PUFへの攻撃もよく研究がされてきた、特に本稿と関連の深い攻撃手法として、PUFの挙動を操作することで、小さい計算量でステートを復元する攻撃がある [10], [11]. 特に、文献 [11] は、ReRAM-PUF (Resistive Randam Access Memory PUF) などのステート生成に利用される Time-to-Digital Converter (TDC) のクロックを操作することで、生成されるステートの 0 と 1 の割合に偏りを誘発する。偏りのあるステートを利用することで、本来に秘密するべきステートを少ない計算量で復元することができる。

TDC を用いた攻撃の成否は、クロック操作の精度にかかっている。そのため。文献 [11] では、攻撃者のクロック操作能力に関するパラメータを提案している。1 つ目のパラメータは、最大周波数偏向であり、「TDC のクロックを正常値から最大でどの程度までずらすことができるか」ということを意味する。2 つ目のパラメータは、周波数分解能であり、「TDC のクロックを変化させる周波数のステップ」を意味する。これらのパラメータとステート復元攻撃の難易度に関する評価事例は、筆者らが行った先行研究だけである [18]。

1.1 課題とアプローチ

ステート復元攻撃の実現に至るためには、攻撃者は十分なクロック操作能力(最大周波数偏向と周波数分解能)を有する必要がある。攻撃のリスクを正しく評価するためには、攻撃の成功に必要なクロック操作能力を評価することが必要である。本研究は、そのようなクロック操作能力を計算機シミュレーションで評価する。本シミュレーションは著者らによる先行研究 [18] を進めたものであり、先行研究では、周波数分解能 δ_{step} の評価を行ったので、本稿では、最大周波数偏向 δ_{max} の評価を行う。

1.2 貢献

本稿の貢献は以下の通りである:

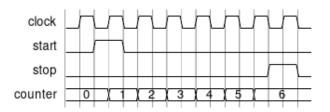


図 1 カウンタベース Time-to-Digital Converter

- (1) ReRAM PUF ステート復元攻撃において,クロック操作の能力の一つである最大周波数偏向の評価を行った.
- (2) 攻撃者は、最大周波数偏向はどの程度の水準を有する必要があるのか示した.

2. 準備

2.1 Time-to-Digital Converter

Time-to-Digital Conveter (TDC, 時間-デジタル 変換器)とは、時間差を測定してデジタル値に変換する回路である [12]. TDC は、時間差をそのまま利用する測距や医用画像処理などへの応用に加えて、トランスデューサと併用することで様々な物理量を測定する際にも応用される.特に、本稿と関連の強い応用例として、電気抵抗を測定する際にも TDC が用いられる.

TDC の実装方式はいくつかあるが、最も代表的な実装方式の 1 つとして、カウンタベース TDC (以下、単に TDC と呼ぶ) がある [12]. 図 1 に TDC の変換の仕組みを示す。 TDC はスタートパルスからストップパルスの入力時間の間に、何回分のクロックエッジが訪れるかを数えることで、時間差をクロックエッジのカウント数に変換する。クロック周波数が f_{clk} で、パルスの入力パルスの入力時間の差が τ 秒の時、 TDC は $|f_{clk} \cdot \tau|$ を出力する。

2.2 Physically Unclonable Function

Physically Unclonable Function(PUF) とは、半導体集積回路の製造によって生じる個体の物理的な特性のランダムなばらつきを積極的に取り出す技術である。デバイス固有の ID を生成するビルディングブロックとして、暗号モジュールを始めとする応用が進んでいる [6], [7]. 本稿では、PUFのIDのことを「ステート」と呼ぶ。ステートは、製造ばらつきを積極的に取り出すことで生成されるのでノイズが混ざることがあるが、ファジー抽出器 [13] によりエラー訂正を行うことで、ノイズの無い ID として利用できる。

2.2.1 PUF による鍵保管庫

PUF の応用例として、暗号モジュールにおける鍵保管庫として利用する方式がある。ステートから生成した鍵(PUF 鍵)を k_{PUF} とする。これを用いて事前に共有した秘密鍵kを暗号化して不揮発性メモリに記録する:

$$c_k = \operatorname{Enc}_{k_{PUF}}(k). \tag{1}$$

このようにして得た暗号文 c_k は不揮発性メモリに記録しておく.この処理は,製品出荷時における登録フェーズで1 度だけ行う.次に起動した時,まず PUF 鍵を復元し,さらにそれを用いて秘密鍵 k を復元する.

暗号モジュールは,正規の利用者から攻撃される場合,攻撃者の手元で動作するので,物理的な接触を伴う攻撃にさらされる.例えば,電源が投入されていない状態のチップを開封して,電子顕微鏡などで不揮発性メモリを観察することで,記録された情報を直接見るような静的リバースエンジニアリングは,鍵を直接見ることができる強力な攻撃である [4], [5]. PUF による鍵保管庫は,このような静的リバースエンジニアリングへ耐性を持つ.なぜなら,チップに電源を投入した後でなければ, PUF 鍵も秘密鍵も出現しないからである.

2.3 ReRAM-PUF

ReRAM は、電気抵抗を用いる不揮発性メモリの一方式である。ReRAM の各セルは、高抵抗状態と低抵抗状態のいずれかにあり、抵抗値の高低により 1 ビットの値を保持する。ただし、一方の状態(たとえば低抵抗状態)にあるセルの中でも、小さな抵抗値のばらつきがある。そのばらつきを PUF に利用したのが ReRAM-PUF である [14], [15], [16].

ReRAM の各セルの抵抗値は対数正規分布に従うとされており、それぞれ独立に抵抗値を計測できる。測定した抵抗値をあらかじめ較正された閾値を用いて二値化することで1ビットの値を得ることができる。この計測を各セルに対して繰り返すことで、多ビットのステートを生成できる。

2.3.1 ReRAM 抵抗値の TDC による測定

ReRAM-PUFには、抵抗値の測定にTDCを用いるものがある。例えば、吉本らのReRAM-PUF [16]では、図2に示す回路で抵抗値を時間に変換し、その上でTDCでデジタル値を得る。この手法は、RC回路においてキャパシタに蓄積された電荷を抵抗を通して放電したとき、キャパシタの電圧が閾値に達するまでに要する時間が抵抗値によって異なることを利用する。

まず、キャパシタ C を 電圧 V_0 で充電し、その後で測定対象の抵抗 R を通して放電する。放電開始と同時に TDC での時間測定をスタートし、キャパシタの電圧が閾値 V_{TH} まで下がった時点で時間測定をストップする。 時刻 t におけるキャパシタの電圧は、 $V(t) = V_0 \cdot \exp\left(\frac{-t}{RC}\right)$ なので、これが閾値 V_{TH} まで低下するのに要する時間 t_R は

$$t_R = -RC \cdot \log(\frac{V_{TH}}{V_0}) \tag{2}$$

である. 放電時間 t_R と 抵抗値 R が比例関係にあるため,適切な係数を定めれば,放電時間 t_R から抵抗値 R を求めることができる. 放電時間 t_R をクロック周波数 f_{clk} で動作する TDC で計測して得るデジタル値 c_R は次のように

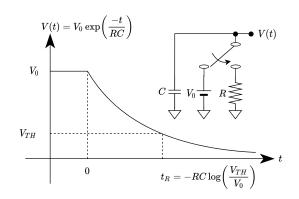


図 2 抵抗値 - 時間変換器 [16]

なる:

$$c_R = \lfloor t_R \cdot f_{clk} \rfloor. \tag{3}$$

ReRAM-PUF の 1 ビット分のステート b_R は、この c_R を閾値 c_{TH} で二値化することで得る:

$$b_R = \begin{cases} 0 & (c_R < c_{TH}) \\ 1 & (otherwise) \end{cases} \tag{4}$$

なお、この閾値 c_{TH} は、抵抗値ばらつき分布の中央値となるようにあらかじめ較正しておく、以上の計測を複数のセルに対して繰り返すことで、ReRAM PUF のステートを生成できる。

TDC へのシグナルインジェクションを用いた PUF ステート復元攻撃 [11]

この章では、本稿の評価対象であるステート復元攻撃 [11] について述べる。この攻撃は、ReRAM-PUF のビルディングブロックである TDC のクロックを操作することでステートをバイアスすることで、少ない計算量でステートを復元する手法である。

3.1 攻撃者モデル

攻撃者の目的は、PUF による鍵保管を有する暗号モジュールにおける PUF ステート \vec{M}_{PUF} を復元することである。攻撃者は、デバイスへの物理的に接触して、TDCのクロック周波数 f_{clk} を任意に操作できるものとする。また、攻撃者は、ステート \vec{M} を直接観測することはできないが、暗号モジュールにクエリ Q を送ると、 \vec{M} と Q に対応するレスポンス X を得ることができるものとする:

$$X \leftarrow \text{Dev}(\vec{M}, Q).$$
 (5)

ただしここで、Dev は、次の手順を抽象化している:

- (1) ステート \vec{M} から PUF 鍵 k_{PUF} を復元する.
- (2) 暗号化された秘密鍵 c_k を PUF 鍵で復号して秘密鍵 k を復元する.
- (3) k を用いて Q を暗号化/復号した値を返す.

3.2 TDC へのシグナルインジェクション

TDC のクロック周波数を任意に操作できる攻撃者は, TDC の計測値を任意に操作である [11], [17]. さらに, TDC によって計測される抵抗値を操作することもできる [11].

3.2.1 TDC の計測値の操作

攻撃者は、 TDC のクロック周波数を正常な f_{clk} から f'_{clk} に偏向して動作させる:

$$f'_{clk} = (1 - \delta) \cdot f_{clk}. \tag{6}$$

ここで, δ は 正常値からのずれを表す周波数偏向である. クロック $f_{clk}^{'}$ で動作する TDC は, 正常値 $\lfloor \tau \cdot f_{clk} \rfloor$ の代わりに,操作された値 $\lfloor \tau \cdot f_{clk}^{'} \rfloor$ を出力する.ただし,

$$\tau \cdot f'_{clk} = (1 - \delta) \cdot \tau \cdot f_{clk} \tag{7}$$

である. 式 (7) より, 攻撃者は周波数偏向 δ を通して TDC の出力を操作できることができる [11], [17]. なお, クロック周波数 f_{clk} は十分大きく設計することを鑑みて, 床関数 $[\cdot]$ は以降の議論では簡単のために無視するもの する.

3.2.2 ReRAM セルの抵抗値の操作

攻撃者が選ぶクロック周波数偏向 δ に合わせて、 TDC の出力を操作できることを悪用して、ReRAM 抵抗値の操作が可能である [11].

対象の ReRAM セルの抵抗値を R とする. 抵抗値—時間変換器は,この抵抗値を時間 t_R に変換する(式 (2)). 正常なクロック f_{clk} で動作する TDC は, t_R を $c_R = t_R \cdot f_{clk}$ とカウントする.一方で,攻撃者により注入されたクロック f'_{clk} で動作する TDC は, t_R を $c'_R = t_R \cdot f'_{clk}$ とカウントする.このとき,

$$c_R' = t_R \cdot f_{clk}' = t_R \cdot (1 - \delta) \cdot f_{clk} = c_R \cdot (1 - \delta) \quad (8)$$

であるため、攻撃者はクロック周波数偏向 δ を操作することで、計測値を操作できる [11].

3.2.3 ReRAM PUF ステートのバイアス

ReRAM セルの抵抗値を操作することで、結果的に、生成されるステートにおける 0 と 1 の頻度をバイアスできる。前述の通り、ReRAM PUF は、閾値 c_{TH} で計測値を二値化して 1 ビット分のステート b_R を生成する:

$$b_R = \begin{cases} 0 & (c_R' < c_{TH}) \Leftrightarrow (c_R < c_{TH}/(1 - \delta)) \\ 1 & (otherwise) \end{cases}$$
 (9)

攻撃者は、N 個の ReRAM セルの抵抗値を計測するあいだ,クロック $f'_{clk}=(1-\delta)\cdot f_{clk}$ を維持する.これは,閾値をずらすことと等価である(式 (9) を参照).その結果として生じるステートにおける 0 と 1 の頻度は,周波数偏向 δ に応じた偏りを持つ [11].

Algorithm 1 TDC Experiment [11]

Require: クロック周波数偏向 δ , クエリ Q

Ensure: $V \supset x \supset X$

- 1: set the clock frequency $f'_{clk} = f_{clk} \delta \cdot f_{clk}$
- 2: Invoke PUF key generation \triangleright the PUF state becomes M_{δ}
- 3: Get a responce $X \leftarrow \text{Dev}(\vec{M}, Q)$
- 4: return M_{δ_0}

3.2.4 攻撃者による計測手順 (TDCE)

攻撃が行う計測 TDC Experiment(TDCE) [11] をアルゴリズム 1 に示す.攻撃者は, TDC のクロックを正常値 f_{clk} から $f'_{clk}=(1-\delta)\cdot f_{clk}$ に操作することで,PUF に偏りのある誤りステート \vec{M}_δ を生じさせることができる.攻撃者はステート \vec{M} を直接観測することはできないが,暗号サービスを介して間接的にアクセスできる.すなわち,暗号モジュールにクエリ Q を送ると, \vec{M}_δ と Q に対応するレスポンス X を得ることができる.

攻撃対象デバイスは二値化の閾値 c_{TH} を較正することができるが、較正タイミングによって TDC への偏向クロックの注入のタイミングを変えなければならないことに注意が必要である。閾値の較正が頻繁に行われない場合、例えば工場出荷時の較正等の場合、閾値は攻撃の始終において一定であるので、攻撃者はデバイスの電源投入前の段階で偏向クロックを注入し始めることができる。一方で、閾値の較正が頻繁に行われる場合、例えば、電源投入時に毎回中央値を算出する場合、攻撃者はデバイスの電源投入後、較正が終了した後で、偏向クロックを注入しなければならない。

3.3 ステート復元攻撃 [11]

ステート復元攻撃は、ReRAM-PUFのビルディングブロックである TDC のクロックを操作することでステートをバイアスすることで現実的な計算量でステートを復元する攻撃手法である [11].

アルゴリズム 2 にステート復元攻撃を示す。 δ_{max} は,最大周波数偏向であり,「TDC クロックを正常値から最大でどの程度まで変化させることができるか」ということを意味する。 δ_{step} は周波数分解能であり,「TDC クロックを変化させる際の周波数の刻み」を意味する。

攻撃は,バイアスされたステートから生成される出力の 記録と,その出力を用いたステート復元の2段階からなる.

STEP 1: データ収集

まず,クロック周波数を変化させながらデータ収集を行う.攻撃者は, TDC のクロックを偏向 δ_i だけ変化させて PUF を動作させ,偏りのあるステート \vec{M}_{δ_i} を生じさせる.この際, $\delta_{i+1}=\delta_i+\delta_{step}$ のように小さな刻みで偏向を変化させる,対応するステートの列 \vec{M}_{δ_i} を得る. δ_{step} を十分小さく取れば,隣接するステート \vec{M}_{δ_i} と $\vec{M}_{\delta_{i+1}}$ は,数ビット程度しか離れて

Algorithm 2 ステート復元攻撃 [11]

Require: 最大周波数偏向 δ_{max} , 周波数分解能 δ_{step}

Ensure: PUF ステート \vec{M}_{PUF}

- 1: Fix an arbitrary device query Q
- 2: Set $i \leftarrow 0$ and $\delta_0 \leftarrow 0$
- 3: repeat
- 4: Record $X_i \leftarrow \text{TDCE}(\delta_i, Q)$
- 5: Set $i \leftarrow i+1$
- 6: Set $\delta_i \leftarrow \delta_{i-1} + \delta_{step}$
- 7: until $\delta_i < \delta_{max}$
- 8: Record $X_i \leftarrow \text{TDCE}(\delta_{max}, Q)$
- 9: $\vec{M}_{\delta_{i+1}} = \vec{0}$
- 10: **for** j = i + 1 down to 1 **do**
- 11: Compute $\vec{M}_{\delta_{j-1}} = \text{Finder}(\vec{M}_{\delta_j}, Q, X_{j-1})$
- 12: **end for**
- 13: **return** \vec{M}_{δ_0}

いないごく似た値となる. 以上を, δ_i が δ_{max} に到達するまで繰り返す. 最後の偏差 δ_{max} によるステート $\vec{M}_{\delta_{max}}$ は, オールゼロに近い値であると期待する.

STEP 2: 探索

次に、記録した出力を用いてステートを復元する.隣接するステート間の距離が十分小さければ、現実的な時間で全探索を行うことができる.この時,Finderは、 \vec{M}_{δ_j} 近傍の全ステートの中から,出力が X_{j-1} となる $\vec{M}_{\delta_{j-1}}$ を全数探索するモデルである.この全探索を行うのが Finder である.すなわち,数ビット程度しか離れていないと期待する隣接ステート \vec{M}_{δ_j} から $\vec{M}_{\delta_{j-1}}$ を順番に全数探索して,少しづつ正常なステートに近づける.まず,オールゼロのステート $\vec{M}_{\delta_{i+1}}$ からはじめ,Finder を繰り返すことで,最終的に秘密のステートである $\vec{M}_{\delta_0} = \vec{M}_{PUF}$ を復元することができる.

4. シミュレーションによる攻撃難易度の評価

ステート復元攻撃 [11] の実現に至るためには、攻撃者は十分なクロック操作能力を有する必要がある。そこで、攻撃の成功に必要なクロック操作能力を、計算機シミュレーションで評価する。

4.1 実験の目的

周波数分解能 δ_{step} と最大周波数偏向 δ_{max} が、 攻撃者 のクロック操作能力を代表するパラメータである。それら のパラメータと、攻撃における探索空間の関係を以下にま とめる

周波数分解能 δ_{step} :

周波数分解能 δ_{step} は、隣接するステート間の距離を決める.ステートサイズが N ビットで、隣接するステート \vec{M}_{δ_j} と $\vec{M}_{\delta_{j-1}}$ のハミング距離が d ビットである時、探索空間は NC_d 通りである.これは組み合わせ数的に増加するため、 δ_{step} が大きいと(すなわち距

離 d が大きいと) 全探索が実行不可能になる.

最大周波数偏向 δ_{max} :

最大周波数偏向 δ_{max} は,探索の最初のステップで,オールゼロから $\vec{M}_{\delta_{max}}$ までの距離を決める.先の議論と同様に,探索空間は,この距離に対して組み合わせ数的に増加する.探索空間を小さくするためには $\vec{M}_{\delta_{max}}$ のハミングウェイトを小さくする必要があり,そのために, δ_{max} は十分に大きくなくてはならない.

以上の背景より,攻撃の成功に必要なパラメータを調べることは,攻撃の効率を評価する上で重要である.そこで,攻撃成功に必要な条件を計算機シミュレーションで評価する.なお,周波数分解能 δ_{step} の評価は先行研究 [18] で行ったため,本稿では,最大周波数偏向 δ_{max} の評価を行う.

4.2 隣接ステート間距離 d に対する計算時間

まず、ステート間のハミング距離と計算時間の関係を調べる。すなわち、ステートサイズが N ビットにおいて、 \vec{M}_{δ_j} と $\vec{M}_{\delta_{j-1}}$ ハミング距離が d ビット離れた時、 \vec{M}_{δ_j} から $\vec{M}_{\delta_{j-1}}$ の全数探索に要する時間を調べた。前述の通り、探索空間は $_N$ C $_d$ となる。この計算時間を調べるために、ステートサイズが N で d ビット離れた隣接ステートのペア(\vec{M}_{δ_j} , $\vec{M}_{\delta_{j-1}}$)を 3 ペア用意し、各ペアに対して 探索を行い、その探索に要した時間の平均値を調べた。

図 3 に、ステートサイズ N が N=128,256 ビットにおいて、ハミング距離が d ビット離れた候補を見つける計算機実験の実行時間を示す.これは、 Intel Core i5 2400 上に Python で実装したスクリプトで計算し、 10,000 秒で中断したものである.結果的には、10,000 秒で探索できた距離 d は、N=128 の場合, $d \leq 5$ であり,N=256 の場合, $d \leq 4$ であった.

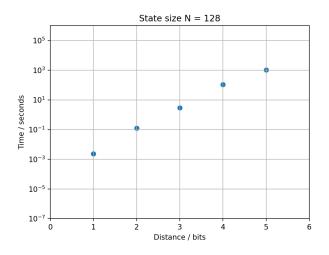
4.3 δ_{max} に対する距離

攻撃の成功に必要な最大周波数偏向 δ_{max} を調べる。実験で用いる抵抗値の確率分布として,吉本らの ReRAM PUF の論文に記載されたもの(出力平均 140, 標準偏差 31 の対数正規分布,中央値は 136.7)を用いる [16].

4.3.1 実験手順

ステートサイズが N ビットにおいて,最大周波数偏向 δ_{max} を変化させた時, $\vec{M}_{\delta_{max}}$ がオールゼロのステートから何ビット離れているか調べ,その相対度数を求めた.実験手順をアルゴリズム 3 に示す.

- (1) まず、対象の確率分布から N 個の標本を取り出す(3 行目). この操作は、対象の ReRAM メモリアレイから PUF として使用する N 個のセルを選択し、TDC で抵抗値を測定することに対応する.
- (2) 攻撃者の偏向クロック注入によって,ステートがバイ アスされることを模擬するため,TDC のクロックを



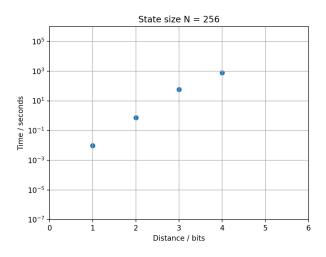


図 3 ステートサイズが N ビットにおいて、ハミング距離が d ビット離れた隣接するステートの探索に要した時間 [s]

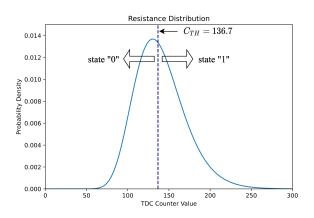


図 4 平均出力 140, 標準偏差 31 の対数正規分布

 δ_{max} 偏向したときのステート δ_{max} を生成する(4 行目). ステート生成手順(GenerateState)をアルゴリズム 4 に示す.GenerateState は,式 (9)による 2 値化を N ビットのステート全てに繰り返す操作である.

- (3) 次に、 δ_{max} のハミング重み d を求める(5 行目).この操作は、オールゼロのステートから δ_{max} の距離 d を求めることを意味する.また、重み d の出現頻度をカウントする(6 行目)
- (4) 最後に, P_i を 試行回数 600 で割ることで,相対度数 を求める (8 行目).
- (5) 以上を δ_{max} を変えながら繰り返す.

4.3.2 結果

表 1 に,ステートサイズが N ビットにおいて,最大周波数偏向 δ_{max} を変化させた時, $\vec{M}_{\delta_{max}}$ とオールゼロのステートの距離の相対度数を示す.以下に,各ステートサイズにおける詳細を述べる:

ステートサイズ N=128

ステートサイズ N が 128 ビットの場合, セクション 4.2 の実験結果より, 10,000 秒で容易に探索可能

${f Algorithm}$ 3 δ_{max} に対する距離 d の分布調査

Require: 最大周波数偏向 δ_{max} , ステートサイズ N

Ensure: $\vec{M}_{\delta_{max}}$ のハミング重みの分布 P_i $(i=0,1,\ldots,N)$

1: $P_i \leftarrow 0 \quad (i = 0, 1, \dots, N)$

2: for i = 1 up to 600 do

3: $\vec{C} \leftarrow \text{Get } N \text{ samples from log-normal distribution}$

4: $\vec{M}_{\delta_{max}} \leftarrow \text{GenerateState}(\vec{C}, \, \delta_{max})$

5: $d \leftarrow \text{HammingWeight}(\vec{M}_{\delta_{--}})$

6: $P_d \leftarrow P_d + 1$

7: end for

8: $P_i \leftarrow P_i/600 \quad (i = 0, 1, ..., N)$

9: **return** P_i (i = 0, 1, ..., N)

Algorithm 4 ステート生成 GenerateState

Require: N 個の TDC の出力列 $\vec{C}=(c_1,c_2,\ldots,c_N),$ クロック周波数偏向 δ

Ensure: PUF ステート \vec{M}

1: $\vec{M} = (m_1, m_2, \dots, m_N)$

2: for i = 1 up to N do

3: if $c_i \cdot (1 - \delta) < C_{TH}$ then

4: $m_i \leftarrow 0$

5: **else**

6: $m_i \leftarrow 1$

7: end if

8: end for

9: return \vec{M}

な距離は $N \leq 5$ である. $\delta_{max} = 0.2$ の場合は, $\sum_{d=0}^5 P_d = 0.17$ % の確率で復元ができる. $\delta_{max} = 0.3$ の場合は, $\sum_{d=0}^5 P_d = 36.50$ % の確率で復元ができる. $\delta_{max} = 0.4$ の場合は, $\sum_{d=0}^5 P_d = 99.67$ % の確率で復元ができる. $\delta_{max} = 0.5$ の場合は, $\sum_{d=0}^5 P_d = 100.00$ % の確率で復元ができる.

ステートサイズ N=256

ステートサイズ N が 256 ビットの場合, セクション 4.2 の実験結果より, 10,000 秒で容易に探索可能な距離は $N\leq 4$ である. $\delta_{max}=0.3$ の場合は,

 $\sum_{d=0}^4 P_d = 0.5$ % の確率で復元ができる. $\delta_{max} = 0.4$ の場合は, $\sum_{d=0}^4 P_d = 89.83$ % の確率で復元ができる. $\delta_{max} = 0.5$ の場合は, $\sum_{d=0}^4 P_d = 100.00$ % の確率で復元ができる.

4.4 結論

本稿で復元に用いた筆者らの計算機は決して高価なものではないので、攻撃者も容易に十分な性能を持った計算機を準備でき、せいぜいその程度の計算機を有する攻撃者にとっては、ステートサイズが 128,256 ビットいずれの場合も、最大周波数偏向 $\delta_{max}=0.5$ を有することができれば、オールゼロから $\vec{M}_{\delta_{max}}$ の全数探索による復元は 100 % 可能である。また、式 (6) より、 $\delta_{max}=0.5$ の時、 クロックは正常な状態から 50% 遅くすることに対応する.

まとめ

本稿では、TDCへのシグナルインジェクションによる ReRAM PUF ステート復元攻撃の実現に至るために、どの 程度の最大周波数偏向のクロック操作能力の水準を有する 必要があるのか計算機シミュレーションで評価した. 攻撃 にかける現実的な時間を定めた上で、時間内に攻撃が完了 するために必要となる最大周波数偏向水準を示した. PUF ステートサイズが 128, 256 ビットにおいて、正常なクロックより 50% 遅くすることができれば、最大周波数偏向の クロック操作能力としては十分な水準であることを明らかにした.

参考文献

- [1] NXP Semiconductors, "LPC55S6x MCU Family", NXP Semiconductors, 2019, https://www.nxp.com/docs/ en/fact-sheet/LPC55S6XFS.PDF
- [2] Mangard, S., Oswald, E., Popp, T.: Power analysis at-tacks - revealing the secrets of smart cards. Springer(2007)
- [3] Joye, M., Tunstall, M. (eds.): Fault Analysis in Cryptog- raphy. Information Security and Cryptography. Springer (2012)
- [4] Courbon, Franck, Sergei Skorobogatov, and Christopher Woods, "Reverse Engineering Flash EEPROM Memories Using Scanning Electron Microscopy," in Kerstin Lemke-Rust and Michael Tunstall, eds, Smart Card Research and Advanced Applications, Springer-Verlag, 2016, pp. 57-72.
- [5] Torrance, R., James, D.: The state-of-the-art in semiconductor reverse engineering. In: 2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 333–338 (2011)
- [6] Maes, R.: Physically Unclonable Functions Constructions, Properties and Applications. Springer (2013)
- [7] Tajik, S.: On the physical security of physically unclonable functions. Ph.D. thesis, Technical University of Berlin, Germany (2017)
- [8] Tuyls, Pim, Geert-Jan Schrijen, Boris Škorić, Jan van Geloven, Nynke Verhaegh, and Rob Wolters, "Read-

- Proof Hardware from Protective Coatings," Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2006, Lecture Notes in Computer Science, 4249, Springer-Verlag, 2006, pp. 369-383
- [9] NXP Semiconductors, "AN12324 LPC55Sxx usage of the PUF and Hash Crypt to AES coding", NXP Semiconductors, 2019, https://www.nxp.com/docs/ en/application-note/AN12324.pdf.
- [10] Zeitouni, S., Oren, Y., Wachsmann, C., Koeberl, P., Sadeghi, A.: Remanence decay side-channel: The PUF case. IEEE Transactions on Information Forensics and Security 11(6), 1106–1116 (2016)
- [11] T. Sugawara, T. Onuma, and Y. Li,"Signal injection attack on time-to-digital converter and its application to physically unclonable function,"Cryptology ePrint Archive, 2020/716, 2020, https://eprint.iacr.org/ 2020/716
- [12] Henzler, S. (ed.): Time-to-Digital Converters. Advanced Microelectronics. Springer (2010)
- [13] Guajardo, J., Kumar, S.S., Schrijen, G.J., Tuyls, P.: FPGA intrinsic PUFs and their use for IP protection. In: Cryptographic Hardware and Embedded Systems -CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings, pp. 63-80 (2007)
- [14] Chen, A.: Utilizing the variability of resistive random access memory to implement reconfigurable physical un-clonable functions. IEEE Electron Device Letters 36(2), 138–140 (2015). DOI 10.1109/LED.2014.2385870
- [15] Liu, R., Wu, H., Pang, Y., Qian, H., Yu, S.: A highly reliable and tamper-resistant RRAM PUF: Design and experimental validation. In: 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 13–18 (2016)
- [16] Yoshimoto, Y., Katoh, Y., Ogasahara, S., Wei, Z., Kouno, K.: A ReRAM-based physically unclonable function with bit error rate < 0.5% after 10 years at 125oC for 40nm embedded application. In: 2016 IEEE Symposium on VLSI Technology, pp. 1–2 (2016)
- [17] 小沼竜也, 李陽, 菅原健, "Time-to-Digital Converter へ の情報改ざん攻撃", 電子情報通信学会ソサイエティ大会, 2019.
- [18] 山下晃平, 李陽, 菅原健, "Time-to-Digital Converter へのシグナルインジェクションによる PUF ステート復元攻撃の難易度評価", 電子情報通信学会ソサイエティ大会, 2020.

表 1 ステートサイズ N と最大周波数偏向 δ_{max} に対するオールゼロからの距離 d の分布 [%]

N	δ_{max}	d = 0	d = 1	d = 2	d = 3	d = 4	d = 5	d = 6	d = 7	d = 8	d = 9	d = 10	$d \ge 11$
128	0.1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.00
128	0.2	0.00	0.00	0.00	0.00	0.00	0.17	0.00	0.00	0.17	0.33	0.50	98.83
128	0.3	0.33	1.00	4.33	4.67	11.50	14.67	19.67	11.33	12.33	9.00	5.33	5.83
128	0.4	29.67	36.33	21.67	9.33	2.67	0.00	0.17	0.17	0.00	0.00	0.00	0.00
128	0.5	92.17	7.50	0.33	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
128	0.6	99.50	0.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
128	0.7	99.83	0.17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
128	0.8	100.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
256	0.1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.00
256	0.2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.00
256	0.3	0.00	0.00	0.00	0.00	0.50	0.33	1.00	1.67	4.67	6.50	11.00	74.33
256	0.4	7.33	20.50	27.83	20.17	14.00	6.83	2.33	0.83	0.17	0.00	0.00	0.00
256	0.5	82.83	15.50	1.50	0.17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
256	0.6	99.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
256	0.7	99.83	0.17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
256	0.8	100.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00