# A Theoretical Model to Link Uniqueness and Min-Entropy for PUF Evaluations

# A Theoretical Model to Link Uniqueness and Min-Entropy for PUF Evaluations

Chongyan Gu, *Member, IEEE,* Weiqiang Liu, *Senior Member, IEEE,* Neil Hanley, Robert Hesselbarth, and Máire O'Neill, *Senior Member, IEEE*

**Abstract**—Physical unclonable functions (PUFs) are security primitives that enable the extraction of digital identifiers from electronic devices, based on the inherent silicon process variations between devices which occur during the manufacturing process. Due to the intrinsic and lightweight nature of a PUF, they have been proposed to provide security at a low cost for many applications, in particular for the internet of things (IoT). Many metrics have been proposed to evaluate the security and performance of PUF architectures, two of which are uniqueness and min-entropy. The uniqueness of a PUF response evaluates its ability to differentiate between different physical devices, while the min-entropy estimation is a measure of how much uncertainty the PUF response contains. The min-entropy is a lower-bound of real entropy. When the uniqueness of a PUF design is close to the optimal, it is unclear if this also implies that the design has a significantly high entropy; hence it would be useful to ascertain the minimum uniqueness required to achieve a given entropy. To date, a thorough investigation of the relationship between uniqueness and entropy for PUF designs has not been conducted. In this paper, this relationship between the uniqueness and entropy is explored, and for the first time, to the authors' knowledge, the relationship between them is modeled. To verify this model, both simulated and hardware-based experimental results are performed, with a test-bed containing $184$ Xilinx Artix-7 FPGA based Basys3 boards providing a large data set for granular results. The experimental results demonstrate that the proposed model accurately estimates the relationship between uniqueness and min-entropy, with both the theoretical analysis and software simulations closely matching the experimental results.

**Index Terms**—Entropy, Physical Unclonable Functions, Uniqueness.

## 1 Introduction

The internet of things (IoT) has revolutionized our lives through remote health care, autonomous vehicles, smart homes, *etc.*. However, it also brings security and privacy issues by opening up new attack vectors for criminal hackers to exploit for, *e.g.* the distributed denial-of-service (DDoS) attack on Dyn used over $10,000$ Internet of things (IoT) devices, taking down Twitter, SoundCloud, Spotify, Reddit and a host of other sites [1]. The IoT is expected to have a large impact on a wide range of markets, from wearable health-care devices to embedded systems in smart cars, many of which will be underpinned by devices which are limited with regards to computation and power consumption. Conventional security approaches based on computationally complex cryptographic algorithms, are typically too resource intensive to implement on these resource constrained devices. Additionally, an attacker will likely have physical access to many of these embedded IoT devices allowing implementation attacks such as side-channel analysis (SCA) or fault analysis (FA) to be performed [2]. Hence, it is important to evaluate alternative, low-cost, security approaches to secure lightweight IoT devices.


- *C. Gu, N. Hanley and M. O'Neill are the Centre for Secure Information Technologies (CSIT), Institute of Electronics, Communications & Information Technology (ECIT), Queen's University Belfast (QUB), U.K., BT3 9DT.*
  *E-mail: {cgu01,n.hanley}@qub.ac.uk, m.oneill@ecit.qub.ac.uk*
- *W. Liu, is with College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, 211106.*
  *E-mail: liuweiqiang@nuaa.edu.cn*
- *R. Hesselbarth is with the Fraunhofer Institute for Applied and Integrated Security (AISEC), Munich, Germany.*
  *E-mail: robert.hesselbarth@aisec.fraunhofer.de*


Physical unclonable functions (PUFs) are a security primitive which utilise the inherent process variations present during manufacturing in order to generate a unique digital fingerprint that is intrinsic to the device itself [3]. As this natural variation between the devices is outside the control of the manufacturer, they are inherently difficult to clone, as well as providing certain additional tamper-evident properties [4], [5]. These properties have a number of advantages over current state-of-the-art alternatives, opening up interesting possibilities for higher level security protocols such as secure non-volatile key storage or lightweight device authentication, for both application-specific integrated circuit (ASIC) and field programmable gate array (FPGA) based designs. Hence, PUFs are potentially a very promising candidate for increasing the security of IoT devices.

In order to evaluate and compare PUFs designs from a security viewpoint, a number of metrics have been suggested [6], two of which we examine further here; uniqueness and entropy. *Uniqueness* is the ability to distinguish between different devices based on its PUF response to the same challenge. As these PUF instantiations are identical, the difference between the responses is based entirely on the manufacturing process variation. While uniqueness tells us how well the PUF can distinguish between devices, thus giving us an indication of how random the responses are, it does not provide us with the actual entropy available, which is required to formalize security parameters [7].

In order to estimate the entropy of a PUF, a number of methods have been proposed. The context-tree weighting (CTW) lossless compression algorithm is employed to esti-

TABLE 1
An Overview of Uniqueness, Min-entropy and CTW Ratio Results.

| Type | Uniqueness | Min-entropy | CTW Ratio | Sample size |
|---|---|---|---|---|
| SRAM-NXP [9] | 0.49 | 0.75 | 99.1 | 20 |
| SRAM-TSMC [9] | 0.50 | 0.76 | 100 | 20 |
| DFF [9] | 0.50 | 0.77 | 100 | 20 |
| Buskeeper [13] | 0.50 | 0.82 | 99 | 194 |

mate the *upper bound* of entropy (*i.e.* best case) [8], [9], [10], [11], [12]. Min-entropy is another metric widely employed to evaluate the *lower bound* of unpredictability of a response [9], [11], [13], [14], [15]. It estimates the lower bound (*i.e.* worst case) as described in the National Institute of Standards and Technology (NIST) specification 800-90 [16]. The actual entropy is expected to be somewhere between these two bounds.

Table 1 provides an overview of some previously reported results for the metrics of various PUF designs [17]. It is reasonable to assume that as the randomness of the PUF response increases, the hamming distance (HD) between the responses tends to the ideal of $0.5$. Although the uniqueness results are very close to the ideal value of $0.5$, the min-entropy results are not as close to their optimal value of $1$. The CTW ratio represents the ratio of response information before compression and after compression. Ideally, CTW is expected to be 100%, *i.e.* it is difficult to compress the response due to its randomness. Except for the results from Simons *et al.* [13], the results in Table 1 are only evaluated over a small number of experimental devices.

A combination of uniqueness and robustness using mutual information was proposed to analyse the entropy of PUFs [18], while a conditional entropy calculation was also employed to determine whether a MUX PUF is linear [19]. However, a thorough investigation of the relationship between uniqueness and entropy for PUF designs has not yet been conducted. When the uniqueness of a PUF design is close to the optimal, it is unclear if the design has a sufficiently high entropy. It is also interesting to consider what is the minimum uniqueness required to achieve a given entropy. Moreover, as it is not accurate to empirically calculate the entropy over a small sample size, a model to detail the relationship between uniqueness and entropy is of practical relevance.

In the context of a security evaluation, worst-case analysis is preferable to best-case. Hence, in this paper, we focus on developing a theoretical link between the uniqueness and min-entropy, and verifying its feasibility with both software simulations and hardware-based experimental analysis. Specifically, our research contributions are summarized as follows.

- A novel model explaining the link between uniqueness and min-entropy has been proposed, which can be used to estimate the relationship between them. To the best of the authors' knowledge, this is the first time this link has been investigated.
- A software simulation is conducted to evaluate the feasibility and performance of the proposed model. The simulation results show that the proposed model can accurately estimate either uniqueness or min-entropy, given the other.
- A hardware experiment based on a ring oscillator (RO)-PUF, implemented on a large scale testbed of $184$ Xilinx Artix-7 FPGA based Basys3 boards, is presented. The empirical min-entropy and uniqueness experimental results are $0.73$ and $0.48$, respectively, which match with both theoretical analysis and software simulation.
- The duration of the RO acquisition time significantly impacts the robustness of the PUF responses. Therefore, the effect of varying the duration of the RO on the proposed model is also investigated. It shows that the proposed method accurately estimates the trend and lower bound of the relationship between uniqueness and min-entropy.

TABLE 2
List of Parameters.

| Symbol | Definition |
|---|---|
| $m$ | The number of devices, indexed by $\{i, j\}$ |
| $n$ | The bit-length, indexed by $\{b\}$ |
| $\mathsf{R}_i$ | The response from the $i^{th}$ device |
| $\mathsf{R}_{i,b}$ | The $b^{th}$ response bit from the $i^{th}$ device |
| $\mathrm{HD}(\mathsf{R}_i, \mathsf{R}_j)$ | The HD between the responses from devices $i$ and $j$ |
| $\mathrm{HW}_b$ | The hamming weight (HW) of the $b^{th}$ bit over $m$ devices |

The rest of this paper is organised as follows. Section 2 describes the basic concept of uniqueness and min-entropy. Section 3 presents the proposed theoretical model. The experimental setup is described in Section 4. The experimental analysis of both the software simulation and the hardware implementation of a RO PUF are presented in Section 5. Finally, conclusions are drawn in Section 6.

## 2 Preliminaries

In this work the link between uniqueness and min-entropy is explored. In order to explain these two concepts, some definitions are outlined in Table 2 and illustrated in Fig. 1.

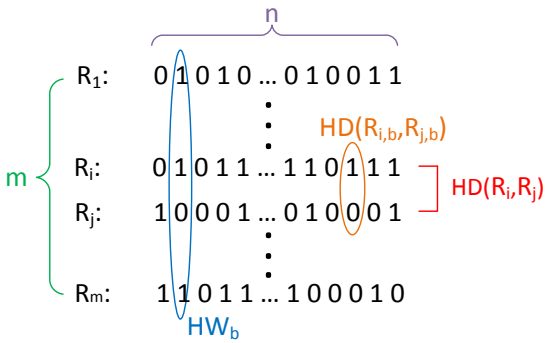


Fig. 1. Definitions used in this work.

Some basic mathematical functions, *e.g.* HD and HW, are utilised to calculate the PUF metrics, which will be

introduced in this section. The function $\mathsf{HD}(\mathsf{R}_i, \mathsf{R}_j)$ over two $n$-bit responses, $\mathsf{R}_{i,b}$ and $\mathsf{R}_{j,b}$, is calculated as

$$\mathsf{HD}(\mathsf{R}_i, \mathsf{R}_j) = \sum_{b=1}^{n} \mathsf{HD}\left(\mathsf{R}_{i,b}, \mathsf{R}_{j,b}\right) \tag{1}$$

The function $\mathsf{HW}_b$ is defined as:

$$\mathsf{HW}_b = \sum_{i=1}^{m} \mathsf{R}_{i,b} \tag{2}$$

### 2.1 Uniqueness

Uniqueness represents the ability of a PUF to uniquely distinguish a device from a population of identical devices. It measures the inter-chip variation by evaluating the HD between a group of $m$ devices. When $m$ is sufficiently large, this can then be extrapolated to the population of devices as a whole. Ideally, for a well designed PUF architecture, the expected HD between any two devices for a randomly selected challenge should be close to $0.5$, indicating that approximately half the response bits are different between the two devices.

Accordingly, uniqueness can be expressed as shown in (3).

$$\mathsf{U} = \frac{2}{m\left(m-1\right)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{\mathsf{HD}\left(\mathsf{R}_i, \mathsf{R}_j\right)}{n} \tag{3}$$

where a PUF circuit is implemented on $m$ devices, each device $i$ returning a response $R_i$ for a randomly selected challenge $C$ which is applied to all devices; then the uniqueness is defined as the expected HD between any two of the $k$ devices.

Subsequently combining with (1) gives:

$$\begin{aligned} \mathsf{U} &= \frac{2}{m\left(m-1\right) \times \mathsf{n}} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \sum_{b=1}^{n} \mathsf{HD}\left(\mathsf{R}_{i,b}, \mathsf{R}_{j,b}\right) \\ &= \frac{1}{n} \sum_{b=1}^{n} \left( \frac{2}{m\left(m-1\right)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \mathsf{HD}\left(\mathsf{R}_{i,b}, \mathsf{R}_{j,b}\right) \right) \end{aligned} \tag{4}$$

This allows the uniqueness for each bit, $\mathsf{U}_b$, to be calculated independently according to (5).

$$\mathsf{U}_b = \frac{2}{m\left(m-1\right)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \mathsf{HD}(\mathsf{R}_{i,b}, \mathsf{R}_{j,b}) \tag{5}$$

Assuming the uniqueness per bit, $\mathsf{U}_b$, is independent and identically distributed (IID)[1];

$$\mathsf{U} = \frac{1}{n} \sum_{b=1}^{n} \mathsf{U}_b \tag{6}$$

It is clear that where the uniqueness for each bit $\mathsf{U}_b$ is close to $0.5$, then the overall uniqueness $\mathsf{U}$ will also tend to the optimal. However, conversely a value of $\mathsf{U} = 0.5$ does not guarantee that the individual bits are well balanced, and a hidden bias can exist. Hence, the uniqueness of the individual bits should also be examined when evaluating a PUF response.

1. While this is the goal for a PUF architecture, in practice this is not assured and must be carefully examined for a given design.

### 2.2 Min-entropy

Min-entropy is a measure of the lower bound of the unpredictability of the response, *i.e.* the entropy provided in the worst case scenario. The commonly used method in the literature to calculate this employs the method outlined in NIST specification 800-90 [16] for evaluating the min-entropy of a binary source. The $n$-bit responses of $m$ devices have an occurrence probability at each bit of $p_1$ and $p_0$ for the values of 1 and 0, respectively. $p_1$ and $p_0$ are calculated by $\frac{\mathsf{HW}_b}{m}$ and $1 - \frac{\mathsf{HW}_b}{m}$, respectively, where $\mathsf{HW}_b$ is the number of 1's in $m$ devices. The maximum probability, $p_{b\,\mathsf{max}} = \mathsf{max}\left(p_0, p_1\right)$, is used to estimate the min-entropy per bit as outlined in (7).

$$\tilde{\mathsf{H}}_{\mathsf{min},b} = -\log_2\left(p_{b\,\mathsf{max}}\right) \tag{7}$$

where,

$$p_{b\ \mathsf{max}} = \begin{cases} \frac{\mathsf{HW}_b}{m} & \mathsf{HW}_b > \frac{m}{2} \\ 1 - \frac{\mathsf{HW}_b}{m} & \mathsf{HW}_b \leq \frac{m}{2} \end{cases} \tag{8}$$

The full min-entropy of the design is then given by (9), and is calculated by averaging the estimated min-entropy of each bit. The ideal case where $\tilde{\mathsf{H}}_{min} = 1$, is returned when the probability of a given bit being equal to 0 or 1 is equal, *i.e.* $p_{b\,\mathsf{max}} = 0.5$, hence $\mathsf{HW}_b = \frac{m}{2}$.

$$\tilde{\mathsf{H}}_{\mathsf{min}} = \frac{1}{\mathsf{n}} \sum_{b=1}^{n} \tilde{\mathsf{H}}_{\mathsf{min},b} \tag{9}$$

## 3 Model for Relationship between Uniqueness and Min-entropy

To build up a model for uniqueness and min-entropy, the relationship between the HW and uniqueness is first obtained. Following (5), let $\mathsf{HD}_b$ be the HD between each pair of $m$ devices for a single bit $b$ of the $n$-bit response.

$$\mathsf{HD}_b = \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \mathsf{HD}(R_{i,b}, R_{j,b}) \tag{10}$$

The uniqueness per bit $\mathsf{U}_b$ from (5) can then be represented as:

$$\mathsf{U}_b = \frac{2}{m\left(m-1\right)} \cdot \mathsf{HD}_b \tag{11}$$

The HD can be considered as a sum of the appearance of pair (0,1) between each of the $m$ devices for each bit. It can be represented as $q(m-q)$, where $q$ is the number of 1's in the $m$ devices, and $\mathsf{HW}_b = q$ in this case. Hence, the HD is related to the HW according to (12);

$$\mathsf{HD}_b = \mathsf{HW}_b \cdot \left(m - \mathsf{HW}_b\right) \tag{12}$$

Therefore, the uniqueness for a single bit in (11) can be expressed as:

$$\mathsf{U}_b = \frac{2}{m\left(m-1\right)} \cdot \left(\mathsf{HW}_b \cdot \left(m - \mathsf{HW}_b\right)\right) \tag{13}$$

Switching the terms around and solving the quadratic allows us to calculate $\mathsf{HW}_b$ as a function of $\mathsf{U}_b$ as shown in (14);

$$\mathsf{HW}_b = \frac{m}{2} \cdot \left(1 \pm \sqrt{\frac{2 \cdot \mathsf{U}_b + m - 2 \cdot \mathsf{U}_b \cdot m}{m}}\right) \tag{14}$$

thus allowing us to derive the relationship between the uniqueness $\mathsf{U}_b$ and the min-entropy $\tilde{\mathsf{H}}_{\mathsf{min}.b}$ from (7). For the first min-entropy probability condition of (8), (14) can be substituted in allowing us to calculate it as a function of the uniqueness:

$$\begin{aligned} \mathsf{HW}_b &> \frac{m}{2} \\ \frac{m}{2} \cdot \left(1 \pm \sqrt{\frac{2 \cdot \mathsf{U}_b + m - 2 \cdot \mathsf{U}_b \cdot m}{m}}\right) &> \frac{m}{2} \\ \mathsf{U}_b &> \frac{m}{2 \cdot (m-1)} \end{aligned} \tag{15}$$

The above transformation process can also be used for the second condition in (8). Hence, we can calculate the min-entropy in (7) as a function of uniqueness by using the probability $p_{b\,\mathsf{max}}$ of a response bit as defined in (16).

$$p_{b\,\mathsf{max}} = \begin{cases} \frac{1}{2} \cdot \left(1 + \sqrt{\frac{2 \cdot \mathsf{U}_b + m - 2 \cdot \mathsf{U}_b \cdot m}{m}}\right) & \mathsf{U}_b > \frac{m}{2 \cdot (m-1)} \\ 1 - \frac{1}{2} \cdot \left(1 + \sqrt{\frac{2 \cdot \mathsf{U}_b + m - 2 \cdot \mathsf{U}_b \cdot m}{m}}\right) & \mathsf{U}_b \leq \frac{m}{2 \cdot (m-1)} \end{cases} \tag{16}$$

It can be seen that the min-entropy is not only related to the uniqueness but also the number of devices $m$. The dependency on $m$ is shown in Fig. 2, where it can be seen that the uniqueness when measured bit-wise tends to the ideal value of $0.5$ as $m$ increases. Therefore, we can see that when $m \lesssim 200$ an estimation of the entropy provided by a given bit will have an inherent bias. As the uniqueness is generally calculated over the full response vector, this can return a value of $0.5$, masking individual bit biases.

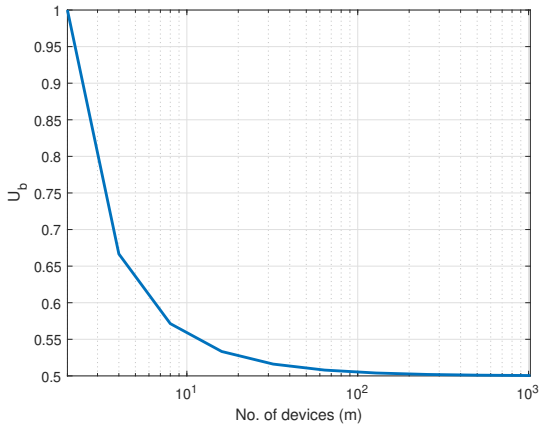


Fig. 2. The uniqueness as a function of the number of devices.

Fig. 3 shows the relationship between uniqueness and min-entropy when calculated per bit over a varying number of devices. As the uniqueness increases, the related min-entropy grows accordingly as expected. However, when the number of devices used for calculations is small, *e.g.* $m = 10$, the maximum min-entropy is $0.6$, considerably lower than the ideal value of $1$.

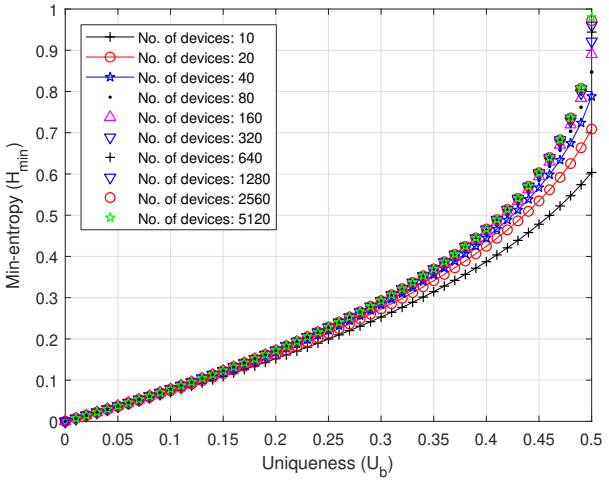


Fig. 3. The relationship between uniqueness and min-entropy for different numbers of devices. It is derived by using the proposed relationship model as shown in (7) and (16).

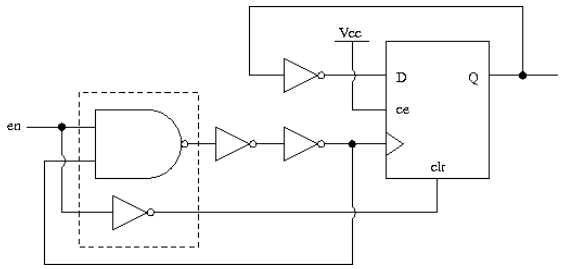


Fig. 4. Ring-oscillator architecture.

A ratio as shown in (17) is defined to clearly quantify the relationship between uniqueness and min-entropy.

$$\rho = \frac{\mathsf{H}_{\mathsf{min}}}{\mathsf{U}} \tag{17}$$

Ideally, for an ideal uniqueness of $0.5$ and min-entropy of $1$, the ratio $\rho$ is equal to $\frac{1}{0.5} = 2$.

## 4 Experimental Setup

To verify and demonstrate the efficiency of the proposed model, acquisitions are evaluated from both a hardware implementation and a software simulation of an RO PUF design.

### 4.1 Hardware Experiment

For the hardware experiment, a set of acquisitions taken from $m = 184$ Digilent Basys-3 boards containing a Xilinx Artix-7 FPGA [20] are recorded. A RO-PUF [21] is utilised to generate an $n$-bit response for each device, where $n = 64$. We implement the core RO on the FPGA, with the subsequent post-processing in software. The ROs are the entropy source of the PUF, while the post-processing can at best retain the existing entropy, it can never increase it hence does not need to be implemented in hardware. The design under test is a three stage RO, as shown in Fig. 4.

An *enable* input activates or stops the oscillator and an output buffered by a toggle flip flop is used to generate a

signal. It can compactly fit in a single Xilinx Artix-7 slice. We fix the physical placement and routing paths of the ROs over all the FPGAs.

Fig. 5 shows one module of the experimental setup, which consists of four modules in total, each of which holds 60 Basys-3 boards, 10 7-port USB hubs, a Raspberry PI-2, and power supply. The USB connection between the PI-2 and Basys3 boards powers the FPGA as well as providing a JTAG interface to program the FPGA with the design under test, and a UART interface to communicate with the configured design and receive the measurement results. The Raspberry-Pi communicates over a local area network (LAN) with a global experiment control server, which also stores the measured data. The array was built as part of the FP7-Sparks project, and a more detailed description can be found in [22].

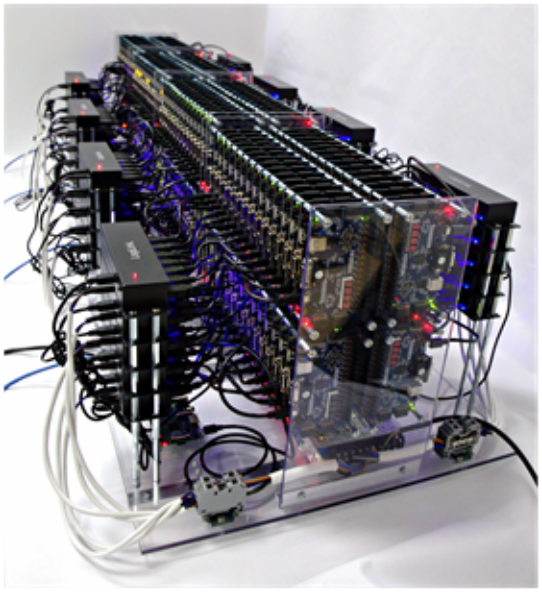

Fig. 5. The hardware testing platform.

### 4.2 Software Simulation

The software simulation is carried out in Matlab 2016™. A group of $m \times n$ arrays of responses is generated by using the algorithm shown in Algorithm 1, where $m$ is the number of devices and $n$ is the number of bits of each response. In this work, $m$ is set to $(1\,k \; or \; 10\,k)$ depending on the case study and $n$ is set to 64.

## 5 Experimental Analysis

Based on the analyses in Section 2, there are three important related cases to investigate:

- Case one: Given the estimated min-entropy of a PUF design, how well can it be used to distinguish between different devices, *i.e.* what uniqueness does it provide?
- Case two: Given the empirical uniqueness of a PUF design, how much min-entropy does it provide?
- For a RO-PUF, what is the relationship between uniqueness and min-entropy for different evaluation times. How do the experimental results match the proposed theoretical model?

**Algorithm 1** Response Generation Algorithm

```
procedure RESPONSE–GENERATION
    for prob = 0.1 to 0.5 do
        % prob is the probability of 0 and 1 in a response
        for i = 1 to m do
            % m is the number of devices
            R(m) ← RandomNumberGenerator(prob, n)
            % n is the number of bits of each response
        end for
        Uniqueness ← HammingDistance(R)
        Min-entropy ← (9)
    end for
end procedure
```

### 5.1 Case One - Uniqueness for a Given Min-entropy

To evaluate the uniqueness result under different min-entropy values, the probability of occurrence of 1 is set from 0.1 to 0.5 (or 0.5 to 0.9) with a step of 0.1, *i.e.* $p_{b\ max} \in [0.1 \ldots 0.5]$. The theoretical uniqueness value as a function of min-entropy is then calculated using (8) and (13) with these values of $p_{b\ max}$.

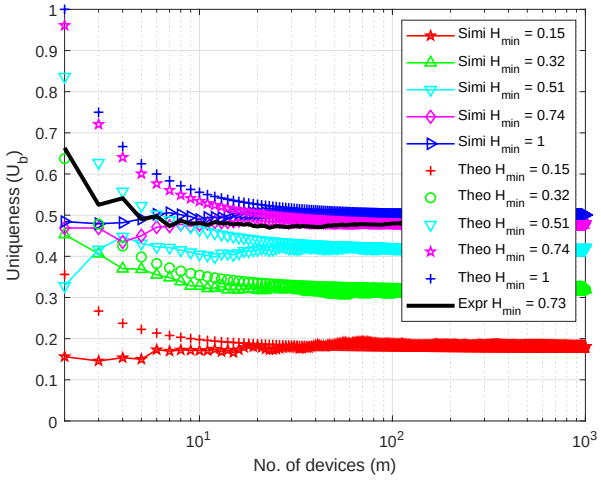


Fig. 6. The uniqueness results over different devices for a given min-entropy. The solid lines exhibit the results from software simulation (Simi), the lines with only markers represent the results from the proposed theoretical model (Theo), and the black line shows the experimental result (Expr) from 184 devices.

Fig. 6 shows the uniqueness results of the theoretical expectation and software simulation over an increasing number of devices $m$, with a specified min-entropy value $\mathsf{H}_{min}$; as well as the calculated values from the test-bed acquisitions. For the hardware results from the entire set of 184 FPGAs, the calculated uniqueness and min-entropy values are 0.48 and 0.73, respectively, with the estimated values closely following the theoretical expectation. The hardware-based experimental result presented in Fig. 6 matches both the theoretical and simulated results, as a solid line, particularly for a large number of devices. Hence, we can see that the theoretical model is verified by both simulated results and actual experimental results.

As previously mentioned, to achieve an optimal value for the min-entropy, $p_{b,\,\mathsf{max}}$ should tend towards 0.5; there-

fore the HW should be approximately $\frac{m}{2}$. Hence, from (13),

$$\begin{aligned} \mathsf{U}_b &= \frac{2}{m(m-1)} \cdot \frac{m}{2} \cdot \left(m - \frac{m}{2}\right) \\ &= \frac{m}{2 \cdot (m-1)} \end{aligned} \tag{18}$$

Assuming $m$ is large, as $m \to \infty$, the uniqueness $\mathsf{U}_b = 0.5$. This shows the benefit of a large test-bed in order to accurately estimate the uniqueness for a given min-entropy, with $m \gtrsim 150$ devices desirable.

### 5.2 Case Two - Min-entropy for a Given Uniqueness

In a similar manner, for a given uniqueness calculated from a PUF design, the expected min-entropy can now be calculated. In the software simulation, the uniqueness $\mathsf{U}_b$ is set from $0.18$ to $0.5$, derived once again from $p_{b\ max} \in [0.1 \ldots 0.5]$ similar to case one. A theoretical expectation is calculated by (7), (9) and (16) with these values of $\mathsf{U}_b$. In an ideal scenario, assuming the uniqueness of a given bit is $0.5$, $\mathsf{U_b} = 0.5$, $p_{b\ max}$ can be derived from:

$$\begin{aligned} p_{b\ max} &= 1 - \frac{1}{2} \cdot \left(1 + \sqrt{\frac{2 \cdot 0.5 + m - 2 \cdot 0.5 \cdot m}{m}}\right) \\ &= 1 - \frac{1}{2} \cdot \left(1 + \frac{1}{\sqrt{m}}\right) \end{aligned} \tag{19}$$

Assuming that $m$ is large, $m \to \infty$, where $p_{b\ max} \to \frac{1}{2}$, then the min-entropy $\mathsf{H}_{min} = 1$.

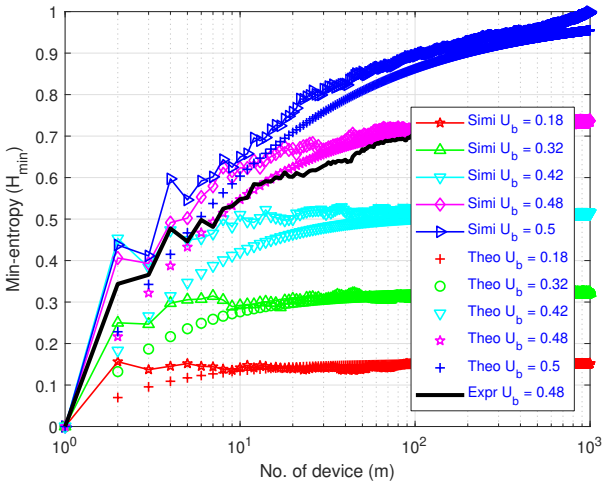


Fig. 7. The min-entropy results over different devices for a given uniqueness. The black line shows the results from the hardware experiment (Expr) over 184 devices. The other solid lines exhibit the results of the software simulation (Simi). The lines with only markers demonstrate the results of the proposed theoretical model (Theo).

Fig. 7 shows the min-entropy results calculated from the theoretical model and software simulations over an increasing number of devices $m$, with a specified uniqueness value $\mathsf{U}_b$; as well as the test-bed acquisitions. It can be seen that the higher the uniqueness value the closer the min-entropy is to the ideal value of 1. It also shows that the larger the number of devices $m$ the higher the min-entropy value (the lower-bound of real entropy) for a given uniqueness. The hardware-based experimental result presented as the black line in Fig. 7 matches both the theoretical and simulated results particularly for a large number of devices. Fig. 7 also shows the min-entropy results assuming $\mathsf{U}_b = 0.5$ calculated over $m$ different devices. Again, this shows the benefit of a large test-bed in order to accurately estimate the min-entropy for a given uniqueness.

### 5.3 Effect of RO Evaluation Times

When evaluating RO-based PUF designs, the length of time over which the RO frequency is estimated has a significant effect on the noise of the response. Generally, the longer the evaluation time, the less noise the response will have [22].

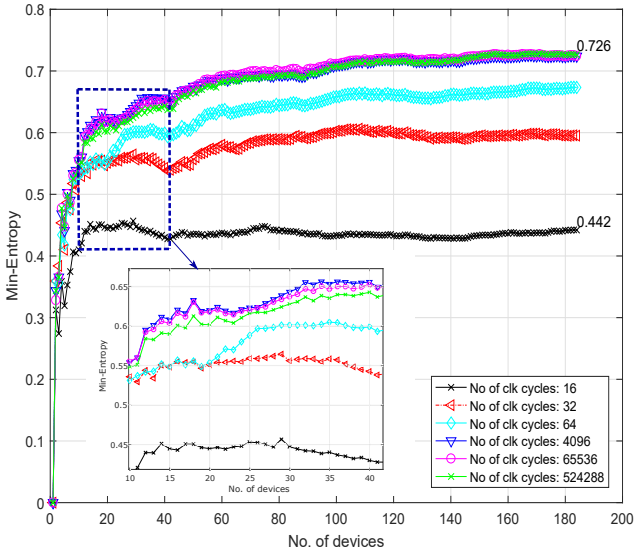


Fig. 8. The hardware experiment for investigating the min-entropy over different RO evaluation times in a range of 16 to 524288. The maximum and minimum min-entropy are 0.726 and 0.442.

To investigate the influence of evaluation time on both uniqueness and min-entropy, the RO frequency estimated across increasing evaluation times is calculated. Fig. 8 shows the influence on the min-entropy, for evaluation times of $[16, 32, 64, 4096, 655536, 524288]$ clock cycles. Smaller evaluation times lead to a smaller switching count at the RO output. This leads to a less accurate estimation of the RO frequency, as well as less variation between the actual count values of the different RO instances giving a lower min-entropy estimation. For the 184 devices used in the hardware experiment, the min-entropy estimation is 0.726 for the longest evaluation time of $524,288$ clock cycles, and $0.442$ when the number is 16.

Fig. 9 shows the influence of different RO evaluation times on the uniqueness result. The box plot is derived by evaluating the uniqueness over all $184$ devices, for each of the evaluation times. It can be seen that the lower the evaluation time, the lower the uniqueness obtained as it is harder to distinguish between the PUF instances for the same reasons as outlined in the min-entropy case. The longer the RO evaluation time, the smaller the box in Fig. 9 and the less outliers.

Fig. 10 exhibits the relationship between uniqueness and min-entropy over different RO evaluation times for both the

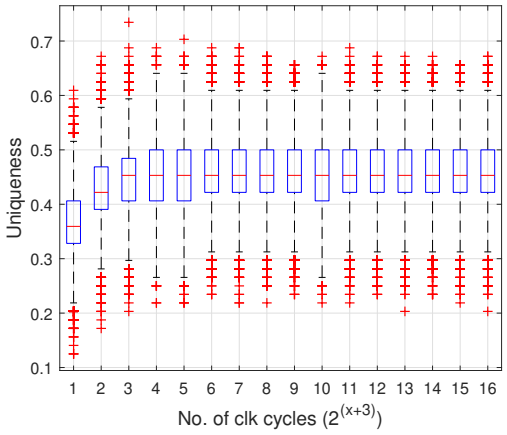


Fig. 9. The hardware experiment for investigating the uniqueness over different RO evaluation times of $2^{(x+3)}$ clock cycles, where $x \in (1, 16)$. On each box, the central mark indicates the median, and the bottom and top edges of the box indicate the $25^{\text{th}}$ and $75^{\text{th}}$ percentiles, respectively. The outliers are plotted individually using the '+' symbol.

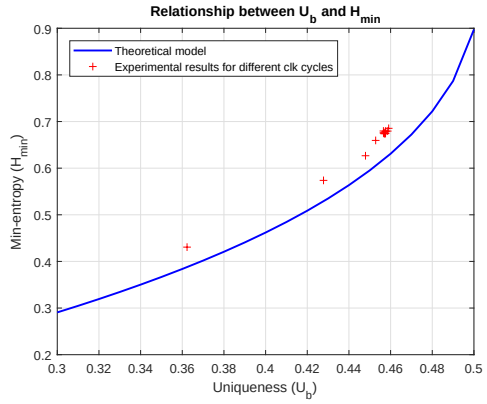


Fig. 10. The relationship between uniqueness and min-entropy over different RO evaluation times. The solid line is derived from the proposed theoretical model and the hardware experimental results are shown using the '+' symbol.

hardware experiment and the proposed theoretical model. The minimum RO evaluation time results in uniqueness and min-entropy values of 0.362 and 0.431, respectively. The maximum RO evaluation time leads to uniqueness and min-entropy values of 0.457 and 0.674, respectively. The longer the RO evaluation time, the higher the uniqueness and the min-entropy. Moreover, it can be seen that the empirical results closely follow that expected from the theoretical model.

## 6 Conclusion and Future Work

In this paper, a novel theoretical model is developed to investigate the relationship between the uniqueness and min-entropy of a PUF response. A software simulation demonstrates that the proposed model can accurately estimate either uniqueness or min-entropy given the other. We have analysed the effect of the number of devices on both uniqueness and min-entropy in practice. For the ideal case, the larger the number of devices, the closer the min-entropy can get to the ideal value of 1, and the closer the uniqueness is to the ideal value of 0.5. In practice the larger number of devices leads a more accurate estimation as for a given value of uniqueness, the min-entropy value is bounded when calculated over a small number of devices. A hardware experiment based on a RO PUF design is presented to evaluate the proposed model and it is implemented on a large scale testbed of 184 Xilinx Artix-7 FPGA based Basys3 boards. The min-entropy and uniqueness experimental results are 0.73 and 0.48, respectively, which match both the theoretical analysis and software simulation. Hence, the proposed model can accurately estimate the trend and the lower bound of the relationship between uniqueness and min-entropy. Moreover, for the RO PUF, the longer the RO evaluation time, the higher the uniqueness and min-entropy.

The RO PUF is utilised to verify the feasibility and accuracy of the proposed model. In future work, an analysis of using the proposed model with other PUF architectures will be performed, as well as investigating the relationship between the process variation and entropy.

## Acknowledgments

This work was partly supported by the Institute for Information & communications Technology Promotion(IITP) grant funded by the Korean government(MSIT) (No. 2016-0-00399, Study on secure key hiding technology for IoT devices [KeyHAS Project]), by the Engineering and Physical Sciences Research Council (EPSRC) (EP/N508664/-CSIT2), by the SPARKS project, funded by EU 7th Framework Programme (FP7/2007-2013, grant agreement no. 608224; www.project-sparks.eu), by National Natural Science Foundation China (61771239) and by Nature Science Foundation of Jiangsu Province (BK20151477).

## References

[1] KrebsonSecurity. DDoS on dyn impacts twitter, spotify, reddit. Accessed: 08-11-2016. [Online]. Available: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

[2] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proc. 9th Int. Conf. on Computational Intelligence and Security (CIS'13)*, 2013, pp. 663–667.

[3] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[4] C. Gu, J. Murphy, and M. O'Neill, "A unique and robust single slice FPGA identification generator," in *Proc. IEEE Int. Symp. on Circuits and Syst. (ISCAS'14)*, Melbourne, Australia, Jun. 2014, pp. 1223–1226.

[5] C. Gu and M. O'Neill, "Ultra-compact and robust FPGA-based PUF identification generator," in *Proc. IEEE Int. Symp. on Circuits and Syst. (ISCAS'15)*, Lisbon, Portugal, May 2015.

[6] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded syst. des. with FPGAs*. Springer, 2013, pp. 245–267.

[7] R. Maes and I. Verbauwhede, *Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 3–37.

[8] S. Katzenbeisser, U. Kocabaş, V. Rožić, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "PUFs: Myth, fact or busted? a security evaluation of physically unclonable functions (PUFs) cast in silicon," in *Proc. 14th Int. Conf. on Cryptographic Hardware and Embedded Syst.*, ser. CHES'12. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 283–301.

[9] M. Claes, V. van der Leest, and A. Braeken, "Comparison of SRAM and FF PUF in 65nm technology," in *Proc. Nordic Conf. on Secure IT Syst.* Springer, 2011, pp. 47–64.

[10] T. Ignatenko, G. j. Schrijen, B. Skoric, P. Tuyls, and F. Willems, "Estimating the secrecy-rate of physical unclonable functions with the context-tree weighting method," in *Proc. IEEE Int. Symp. on Inform. Theory*, July 2006, pp. 499–503.
[11] V. Van der Leest, G.-J. Schrijen, H. Handschuh, and P. Tuyls, "Hardware intrinsic security from D flip-flops," in *Proc. 5th ACM workshop on Scalable trusted comput.*, 2010, pp. 53–62.
[12] W. Liu, Y. Yu, C. Wang, Y. Cui, and M. O'Neill, "RO PUF design in FPGAs with new comparison strategies," in *Proc. IEEE Int. Symp. on Circuits and Syst. (ISCAS'15)*, May 2015, pp. 77–80.
[13] P. Simons, E. van der Sluis, and V. van der Leest, "Buskeeper PUFs, a promising alternative to D flip-flop PUFs," in *Proc. IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST'12)*, Jun. 2012, pp. 7–12.
[14] W. Che, V. K. Kajuluri, M. Martin, F. Saqib, and J. Plusquellic, "Analysis of entropy in a hardware embedded delay PUF," *Cryptography*, vol. 1, no. 1, p. 8, Jun. 2017.
[15] C. Gu, N. Hanley, and M. O'Neill, "FPGA-based strong PUF with increased uniqueness and entropy properties," in *Proc. IEEE Int. Symp. on Circuits and Syst. (ISCAS'17)*, May 2017, pp. 1–4.
[16] E. B. Barker and J. M. Kelsey, *Recommendation for random number generation using deterministic random bit generators (revised)*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, 2007.
[17] R. van den Berg, "Entropy analysis of physical unclonable functions," Ph.D. dissertation, MSc. thesis, Eindhoven University of Technology, 2012.
[18] R. Van Den Berg, B. Skoric, and V. van der Leest, "Bias-based modeling and entropy analysis of PUFs," in *Proc. 3rd Int. Workshop on Trustworthy embedded devices*, 2013, pp. 13–20.
[19] A. Koyily, C. Zhou, C. H. Kim, and K. K. Parhi, "An entropy test for determining whether a MUX PUF is linear or nonlinear," in *Proc. IEEE Int. Symp. on Circuits and Syst. (ISCAS'17)*, May 2017, pp. 1–4.
[20] *Spartan-3E FPGA Family Data Sheet - DS312*, v4.0 ed., Xilinx Inc., 2012, http://www.xilinx.com/support/documentation/data_sheets/ds312.pdf.
[21] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *Proc. 44th ACM/IEEE Des. Automat. Conf. (DAC'07)*, pp. 9–14, 2007.
[22] R. Hesselbarth, F. Wilde, C. Gu, and N. Hanley, "Large scale RO PUF analysis over slice type, evaluation time and temperature on 28nm xilinx FPGAs," in *Proc. IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST'18)*, April 2018, pp. 126–133.