The Big Picture of Delay-PUF Dependability

Alexander Schaub*, Jean-Luc Danger*†, Olivier Rioul*, and Sylvain Guilley†*‡

*LTCI, Télécom Paris
Institut Polytechnique de Paris
91 120 Palaiseau, FRANCE
firstname.lastname@telecom-paris.fr

†Secure-IC S.A.S.
Think Ahead Business Line
75 015 Paris, FRANCE
firstname.lastname@secure-ic.com

‡École Normale Supérieure, DI ENS, CNRS
PSL Research University
75 005 Paris, FRANCE
firstname.lastname@ens.fr

***Abstract*—Physically Unclonable Functions (PUFs) allow to generate bitstrings for applications such as device identification, authentication, or key management. For real-world deployment, the industry has stringent requirements on reliability. In addition, as it greatly impacts the security of the whole application chain, the randomness produced by the PUF cannot be compromised. These two requirements are captured by the notions of dynamic randomness—to be minimized in order to improve reliability—and static randomness—to be maximized to increase security.**

In this paper, we illustrate the whole methodology on a delay-PUF called the loop-PUF. To meet the above requirements on dynamic and static randomness, the PUF's behavior should be modeled and validated; such activities are described in the international standard ISO/IEC 20897. Modeling consists in establishing a stochastic model of the PUF, to predict bit error rates due to dynamic noise, and entropies of the static noise. The model is then verified, its parameters estimated, based on measures in representative environmental conditions.

***Index Terms*—Physically Unclonable Function, reliability, entropy, stochastic model, ISO/IEC 20897.**

I. Introduction

PUF has become an inevitable technology to enhance security in authentication protocols or cryptographic key generation. Such technology relies on slight and random physical imperfections in the semiconductor manufacturing process, creating a "static" randomness source. Static randomness is exploited using a list of challenge/response pairs (the PUF function) with the highest possible entropy to forge a unique and unclonable "fingerprint" which can be used as a device identifier or cryptographic key.

However, the fingerprint extraction from the PUF is contaminated by measurement noise, creating a "dynamic" randomness source. Dynamic randomness creates measurement errors, which reduce the PUF's reliability and can compromise security. There are two basic strategies to enhance reliability [8]: *Filter* out challenges with unreliable responses; and *fuzzy extraction* using error-correcting codes. A trade-off has to be found between PUF reliability and entropy to ensure security. Correlation between responses to challenges, as well as physical bias in the PUF layout can also decrease entropy.

In this paper, we formalize the notions of reliability and entropy of *delay*-PUFs, whose static randomness is exploited by differential measurements of propagation delays. We address both methods of reliability enhancement to combat dynamic randomness, and study their impact on the PUF entropy. Section II introduces our basic mathematical model for the delay-PUF. Section III then formalizes the impact on reliability of enhancement techniques and of responses' correlation and bias. Sections IV and V validate our theoretical findings based on model parameter estimations and real silicon measurements, respectively. Section VI concludes.

II. Delay-PUF Model

A PUF is modeled as a function that takes a challenge (bit vector) $c \in \{\pm 1\}^n$ as input, and produces one bit $b(c) \in \{\pm 1\}$ of output. For delay-PUFs, the output bit is of the form [12]

$$b_x(c) = \operatorname{sign}(c \cdot x)$$

where $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ represents some internal PUF parameter, usually equal to certain delay differences in the PUF circuit. As shown by simulation over many PUF instances, such delay differences can be modeled as realizations of independent Gaussian $\mathcal{N}(0, \Sigma^2)$ random variables $X = (X_1, \ldots, X_n)$.

A. Entropy

Given a set of challenges $\mathcal{C} \subset \{\pm 1\}^n$, the PUF *entropy* is the entropy of the probability distribution $p_b = \mathbb{P}(b_X(\mathcal{C}) = b)$ of the corresponding random bit vectors $b_X(\mathcal{C}) = \{b_X(c)\}_{c \in \mathcal{C}}$. Different types of entropies can be relevant depending on the PUF use-case [14]: min-entropy H_∞, Shannon entropy $H = H_1$, collision entropy H_2, etc. In general, the *α-Rényi entropy* of distribution $p = \{p_b\}$ is defined as $H_\alpha(p) = \frac{1}{1-\alpha} \log \sum_b p_b^\alpha$.

B. Reliability

In practice, $b_x(c)$ are evaluated in the presence of measurement noise, which is modeled as additive white Gaussian noise (AWGN) Z. Thus instead of $b_x(c) = \operatorname{sign}(c \cdot x)$ we measure $\operatorname{sign}(c \cdot x + z)$ where z is the realization of an independent Gaussian random variable $Z \sim \mathcal{N}(0, \sigma^2)$. The corresponding signal-to-noise ratio (SNR) is $\frac{n\Sigma^2}{\sigma^2}$, and the bit error rate (BER) is the probability of a bit flip due to the measurement noise [13]

$$\operatorname{BER}(c, x) = \mathbb{P}\{\operatorname{sign}(c \cdot x) \neq \operatorname{sign}(c \cdot x + Z)\}.$$

Reliability enhancing techniques such as filtering and fuzzy extraction are needed to obtain sufficiently low values of the BER for practical applications.

III. Reliability Enhancing Techniques

Two basic strategies are used to enhance reliability in the presence of dynamic randomness. *Filtering* marks certain responses as "unreliable"; they are ignored to generate the PUF identifier. One can either choose to remove a fixed number of the least reliable challenges [15], or to remove all responses that are less reliable than a given threshold [13]. We consider the latter variant as it is easier to analyze.

Fuzzy extraction, e.g., used by PUFKY [9], applies error correcting codes. It is described by Bösch et al. [1] as follows.

❶ *During enrollment:*

1) generate PUF string $b = (\text{sign}(c \cdot x_1), \ldots, \text{sign}(c \cdot x_n))$ using multiple measurements;
2) generate a random codeword w as a reliable identifier to compute the public helper data $d = w \oplus b$;
3) store the public helper data d in the PUF.

❷ *During bitstring generation:*

1) a PUF (unreliable) measurement is made, yielding b';
2) the measurement is XOR'd to the public helper data to obtain a noisy codeword $w' = d \oplus b'$;
3) the noisy codeword w' is decoded to obtain w.

If w is chosen from a binary $[n, k, d]$ code, then up to $\lfloor \frac{d}{2} \rfloor$ error bits can be corrected from noisy b', and the remaining min-entropy is at least $H_\infty(p) - (n - k)$ [4].

While the filtering method requires that the reliability of a response can be efficiently assessed, the fuzzy extraction method can be used for any PUF (not only delay-PUFs) but involves additional hardware at the decoding step.

A. Independent Responses

In this subsection, we assume that the output responses are independent. As shown in [12], this is the case when all challenges in $\mathcal{C}$ are orthogonal, and the corresponding responses are then uniformly distributed. The theoretical Shannon entropy for n delay elements is then $H(n) = n$ raw bits.

As established in [13], without any reliability enhancing technique, the raw average BER equals $(1/\pi)\arctan(1/\sqrt{\text{SNR}})$. When filtering out challenges for which $|c \cdot x| \leq \Theta\sigma$ where Θ is some relative threshold and σ^2 is the measurement noise variance, the resulting BER equals

$$\frac{2}{\text{erfc}(\frac{\Theta}{\sqrt{2}\sqrt{\text{SNR}}})} \left(T(\Theta, \tfrac{1}{\sqrt{\text{SNR}}}) + \tfrac{1}{4}\,\text{erf}(\tfrac{\Theta}{\sqrt{2}\sqrt{\text{SNR}}})(\text{erf}(\tfrac{\Theta}{\sqrt{2}}) - 1) \right)$$

where T is Owen's T-function [11]. Since the remaining responses are independent, the mean remaining entropy equals

$$H(n, \Theta)_{\text{SNR}} = n \cdot \text{erfc}(\frac{\Theta}{\sqrt{2 \cdot \text{SNR}}}).$$

For fuzzy extraction, we consider a concatenation of a $[2r + 1, 1, 2r + 1]$ repetition code and a $[n', k, d]$ outer code as suggested in [1]. Assuming that $n' \cdot (2r + 1)$ divides n, the outer code is repeated $n/(n'(2r + 1))$ times. Letting $\mathcal{B}(n, p)$ represent a (n, p)-binomial random variable, the key error rate after error correction is

$$1 - \mathbb{P}\{\mathcal{B}(n', p_1) \leq d\}^{n/(n'(2r+1))}$$

where $p_1 = \mathbb{P}\{\mathcal{B}(2r + 1, (1/\pi)\arctan(1/\sqrt{\text{SNR}})) > r\}$. The remaining entropy is then

$$H(n) = \frac{nk}{n'(2r + 1)}.$$

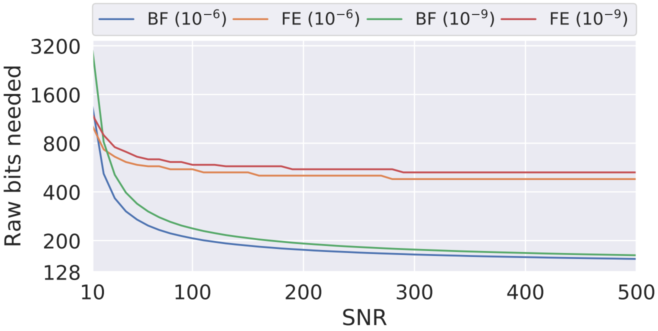

Fig. 1: Raw number of bits to achieve a key error rate of 10^{-6} (resp. 10^{-9}) using bit filtering (BF) or fuzzy extraction (FE). For fuzzy extraction, the outer code has been optimized among a set of binary Golay, Reed-Muller and (shortened) BCH codes, and the inner code among a set of repetition codes of length up to 9.

Fig. 1 compares these two methods in the case of a 128-bit key. It happens that filtering is much more efficient for larger values of SNR, since it allows one to achieve both higher entropy and reliability with lower raw number of bits.

The reliability can also be affected by external parameters, such as temperature. As shown in [13], on average, a temperature difference can be simply modeled as a loss of SNR proportional to the temperature difference.

B. Correlated Responses

For the RO-sum PUF [16], arbiter PUF [6] and loop-PUF [2], one can use up to different 2^n challenges and obtain 2^n output bits. Using more than n challenges does increase the entropy above n bits, which allows the design of PUFs with a lower silicon footprint. However, these output bits will be strongly correlated: The min-entropy H_∞ of the resulting output bit distribution will be only linear in n, not exponential in n [3]. The Shannon entropy $H = H_1$ is upper-bounded by n^2 [14].

Fuzzy extraction provides bounds only on the min-entropy after error correction [4], while one would be more interested on the remaining Shannon entropy in such a setting. As for filtering, the entropy-loss is much more complicated than with uncorrelated responses, because the remaining Shannon entropy is not equal to the entropy of the challenges that are kept. In this section, we will only consider the case of *two* challenges and explain how to compute the conditional entropy of the two responses, under the assumption that both are reliable.

Suppose we consider a PUF with two challenges c_1 and c_2. The responses are distributed as $\text{sign}(c_1 \cdot X)$ and $\text{sign}(c_2 \cdot X)$. The objective is to compute the conditional distribution

$$\text{sign}(c_1 \cdot X), \text{sign}(c_2 \cdot X) \mid |c_1 \cdot X| > \Theta\sigma, |c_2 \cdot X| > \Theta\sigma$$

where Θ is some relative threshold and σ^2 is the measurement noise variance. Let $n_1 = \frac{n + c_1 \cdot c_2}{2}$ and $n_2 = \frac{n - c_1 \cdot c_2}{2}$. This conditional distribution is the same as that of

$$\text{sign}(Y + Z), \text{sign}(Y - Z) \mid |Y + Z| > \Theta\sigma, |Y - Z| > \Theta\sigma$$

where $Y \sim \mathcal{N}(0, n_1\Sigma^2)$ and $Z \sim \mathcal{N}(0, n_2\Sigma^2)$.

Let p_1 (resp. p_2) be the conditional probability that $Y+Z > 0, Y-Z > 0$ (resp. $Y+Z > 0, Y-Z < 0$). One has

$$\begin{aligned}\frac{p_1}{p_2} &= \frac{\mathbb{P}\{Y > -Z \cap Y > Z \cap |Y+Z| > \Theta, |Y-Z| > \Theta\sigma\}}{\mathbb{P}\{Y > -Z \cap Y < Z \cap |Y+Z| > \Theta, |Y-Z| > \Theta\sigma\}} \\ &= \frac{\mathbb{P}\{Y > |Z| + \Theta\sigma\}}{\mathbb{P}\{Z > |Y| + \Theta\sigma\}} \\ &= \frac{\frac{1}{2} - \operatorname{erf}\left(\frac{\Theta}{\sqrt{2}\cdot\sqrt{\mathrm{SNR}}}\right)/2 - 2T\left(\frac{\Theta}{\sqrt{\mathrm{SNR}}}, \sqrt{\frac{n_2}{n_1}}\right)}{\frac{1}{2} - \operatorname{erf}\left(\frac{\Theta}{\sqrt{2}\cdot\sqrt{\mathrm{SNR}}}\right)/2 - 2T\left(\frac{\Theta}{\sqrt{\mathrm{SNR}}}, \sqrt{\frac{n_1}{n_2}}\right)}\end{aligned}$$

where T is Owen's T-function. From this formula, the conditional Shannon entropy can be computed. Results for $n = 8$ are presented in Fig. 2, which shows the tradeoff between the resulting entropy vs. the choice of Θ for different values of n_1, n_2, for $\frac{\Sigma^2}{\sigma^2} = 4$, a ratio consistent with the findings of [13]. As expected, when the responses are not independent, the remaining entropy decreases with the filtering threshold. When the challenges are very correlated, ($n_1 = 1$), then the second challenge hardly increases the total entropy at all when choosing a filtering threshold $\Theta = 4$ or more, which is typically needed in order to achieve PUF reliability. For less correlated challenges ($n_1 = 3$), the entropy loss is much smaller, even for strong filtering up to $\Theta = 6$.

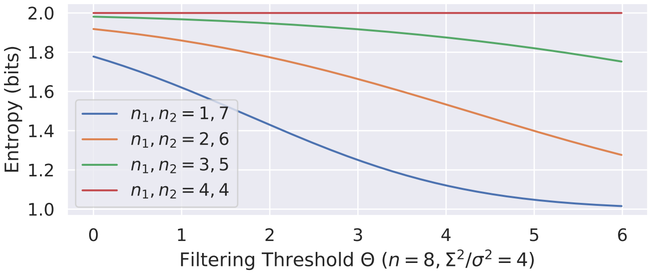

Fig. 2: Conditional entropy after filtering

IV. Model Validation

A. Gaussian Noise and Delays

The average delay differences have been recorded over several PUFs of size $n = 64$ and orthogonal challenges. The distribution of the corresponding delay differences is represented in Fig. 3, and that of the noise in Fig. 4. As can be seen, the delay differences as well as the noise do seem to follow a Gaussian distribution, with an SNR of about 300.

B. PUF Response Independence

Under the hypothesis of independent delay differences $X = (X_1, \ldots, X_n)$, the inner products corresponding to orthogonal challenges $(c_1 \cdot X_1, \ldots, c_n \cdot X_n)$ should also be independent [12]. While true independence is hard to prove, it is possible to show *linear* independence or decorrelation. We used 49 PUFs to compute $n \times n = 64 \times 64$ correlation coefficients $\rho_{i,j}$ between $c_i \cdot X$ and $c_j \cdot X$. The result is shown in Fig. 5.

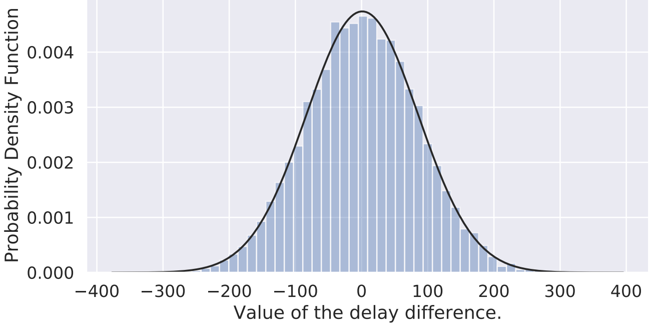

Fig. 3: Empiric delay-difference distribution ($n \cdot \Sigma^2 = 7086$)

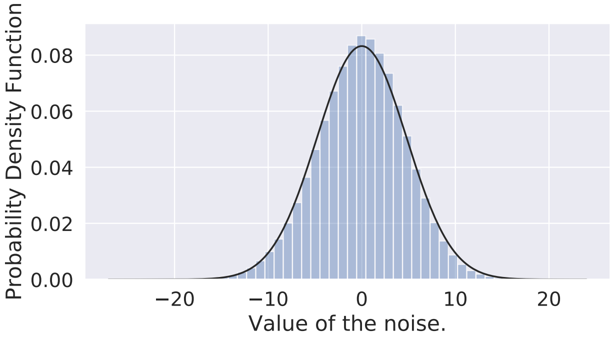

Fig. 4: Empiric noise distribution ($\sigma^2 = 23$)

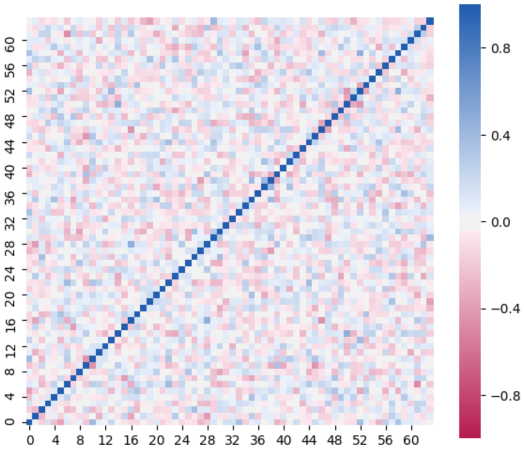

Fig. 5: Correlation matrix $\rho_{i,j}$ $(1 \leq i, j \leq n)$ on 49 loop-PUFs of $n = 64$ delay elements.

Under the independence hypothesis, the Fisher transformation, that is, the hyperbolic arctangent, of the measured correlation coefficients approximately follows a normal distribution around the mean, with a variance of $\sqrt{n-3}$, where n is the number of samples (here, $n = 49$). Thus, we can compute a p-value $p_{i,j}$ for each correlation coefficient $\rho_{i,j}$ by inverting this distribution, and then verify that those p-values are uniformly distributed. This can be done, for instance, using a χ^2 test of goodness of fit. This yields a p-value of 0.158—when using 50 categories for the 2016 computed p-values—with respect to the independence hypothesis. Thus, the independence hypothesis can *not* be rejected with high confidence ($p > 0.05$).

Uniformity can also be assessed. The 49 PUFs generate 3136 bits, of which 1579 are ones. The corresponding binomial distribution $\mathcal{B}(3136, \frac{1}{2})$ has standard-deviation $\sigma = \sqrt{3136\frac{1}{4}} = 28$ and mean $\mu = \frac{3136}{2} = 1568$. Therefore, the number of ones generated by the circuit is less than half a standard-deviation away from the expected mean. These results strongly suggest that the loop-PUF, when considering orthogonal challenges, does have full entropy.

V. Real-world post-silicon validation

In an industrial context, PUF should remain dependable under a wide range of conditions. For instance, in EVITA [5] profile "high", PUF delivers the master key. The most stringent automotive environment conditions are referred to as "grade 0", where the system shall behave nominally in a range of temperature equal to $[-40, 150]$°C. Thus physical validation is a strong requirement and can be carried out using climate chambers.

The tests ideally adhere to some standardized method, such as that presented in ISO/IEC 20897 standard [7], [10] This standard explains how responses shall be collected and metrics such as "steadiness" (called *reliability* in this paper) and "randomness" (called *entropy* in this paper) shall be evaluated.

We present hereafter some experimental measurements which go beyond the strict application of ISO/IEC 20897, in that we analyze the entropy source of the loop-PUF and not simply statistics on the response bits. Validations have been carried out on an actual test-chip, namely the TOISE ASIC. This circuit has been fabricated in STMicroelectronics 65 nm process.

For the loop-PUF, the bit is extracted by comparing the time it takes to achieve 2^L (for $L = 15$) rounds in a loop. This number of loops depends on the challenge. However, we can see in the characterization of Fig. 6 that the number of rounds is tracking over the temperature range. This means that for a given PUF, if one challenge has the PUF oscillate faster at a given temperature, then this order holds across the whole range of temperatures.

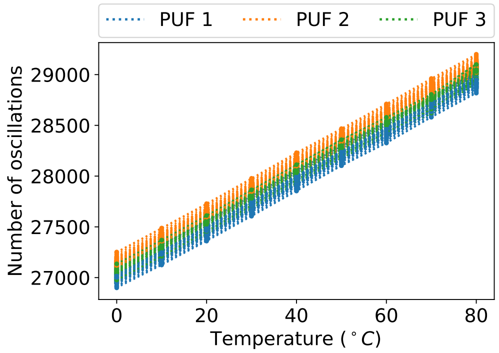

Fig. 6: Number of oscillations in a loop-PUF as a function of the challenge c and of the temperature, for different PUFs.

VI. Conclusion

This paper has shown that stochastic models can actually provide a thorough understanding of the behavior of delay-PUFs in terms of reliability and entropy. We show in particular that for representative SNR values, filtering is more efficient than fuzzy extraction for PUF reliability improvement. However, the theoretical assumptions have to be validated using real world "post-silicon" measurements. Our experiments show that it is possible to assess that the model parameters are of the appropriate order of magnitude. Overall, strong PUFs like delay-PUFs provide definitive advantages in terms of dependability on the reliability-entropy tradeoff.

Acknowledgments

This research has been partially supported by the European Commission under H2020 SPARTA (Grant Agreement 830892).

References

[1] Christoph Bösch, Jorge Guajardo, Ahmad-Reza Sadeghi, Jamshid Shokrollahi, and Pim Tuyls. Efficient helper data key extractor on FPGAs. In *CHES*, volume 5154, pages 181–197. Springer LNCS, 2008.

[2] Zouha Cherif, Jean-Luc Danger, Sylvain Guilley, and Lilian Bossuet. An Easy-to-Design PUF Based on a Single Oscillator: The Loop PUF. In *2012 15th Euromicro Conference on Digital System Design*, pages 156–162, Sep. 2012.

[3] Jeroen Delvaux, Dawu Gu, and Ingrid Verbauwhede. Upper bounds on the min-entropy of RO sum, arbiter, feed-forward arbiter, and S-ArbRO PUFs. In *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, pages 1–6. IEEE, 2016.

[4] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *EUROCRYPT*, volume 3027, pages 523–540. Springer LNCS, 2004.

[5] EVITA. E-safety vehicle intrusion protected applications. European Project https://www.evita-project.org/.

[6] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Delay-based circuit authentication and applications. In *Proceedings of the 2003 ACM Symposium on Applied Computing*, pages 294–301, 2003.

[7] ISO/IEC 20897. Information technology – security techniques – security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters.

[8] Stefan Katzenbeisser, Ünal Kocabaş, Vladimir Rožić, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, and Christian Wachsmann. PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon. *CHES 2012*, pages 283–301, 2012.

[9] Roel Maes, Anthony Van Herrewege, and Ingrid Verbauwhede. PUFKY: A fully functional PUF-based cryptographic key generator. In *CHES 2012*, pages 302–319. Springer-Verlag, 2012.

[10] Nicolas Bruneau et al. Development of the unified security requirements of PUFs during the standardization process. In *SecITC 2018, Bucharest, Romania, November 8-9, 2018*, volume 11359 of *LNCS*, pages 314–330.

[11] Donald B Owen. Tables for computing bivariate normal probabilities. *The Annals of Mathematical Statistics*, 27(4):1075–1090, 1956.

[12] Olivier Rioul, Patrick Solé, Sylvain Guilley, and Jean-Luc Danger. On the entropy of physically unclonable functions. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2928–2932. IEEE, 2016.

[13] Alexander Schaub, Jean-Luc Danger, Sylvain Guilley, and Olivier Rioul. An improved analysis of reliability and entropy for delay PUFs. In *DSD*, pages 553–560. IEEE, 2018.

[14] Alexander Schaub, Olivier Rioul, and Joseph J Boutros. Entropy estimation of physically unclonable functions via Chow parameters. In *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 698–704. IEEE, 2019.

[15] Boris Škoric, Pim Tuyls, and Wil Ophey. Robust key extraction from physical uncloneable functions. In *Applied Cryptography and Network Security*, volume 3531, pages 407–422. Springer, 2005.

[16] Meng-Day Mandel Yu and Srinivas Devadas. Recombination of physical unclonable functions. *35th Annual GOMACTech Conference*, March 2010. Reno, NV, USA.