

Multiple observations for secret-key binding with SRAM PUFs

Citation for published version (APA):

Kusters, L., & Willems, F. M. J. (2021). Multiple observations for secret-key binding with SRAM PUFs. *Entropy*, 23(5), Article 590. <https://doi.org/10.3390/e23050590>

Document license:

CC BY

DOI:

[10.3390/e23050590](https://doi.org/10.3390/e23050590)

Document status and date:

Published: 11/05/2021

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy



If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

Article

Multiple Observations for Secret-Key Binding with SRAM PUFs

Lieneke Kusters *  and Frans M. J. Willems 

Information and Communication Theory Lab, Signal Processing Systems Group, Department of Electrical Engineering, Eindhoven University of Technology, 5600 MB Eindhoven, The Netherlands; f.m.j.willems@tue.nl

* Correspondence: c.j.kusters@tue.nl

Abstract: We present a new Multiple-Observations (MO) helper data scheme for secret-key binding to an SRAM-PUF. This MO scheme binds a single key to multiple enrollment observations of the SRAM-PUF. Performance is improved in comparison to classic schemes which generate helper data based on a single enrollment observation. The performance increase can be explained by the fact that the reliabilities of the different SRAM cells are modeled (implicitly) in the helper data. We prove that the scheme achieves secret-key capacity for any number of enrollment observations, and, therefore, it is optimal. We evaluate performance of the scheme using Monte Carlo simulations, where an off-the-shelf LDPC code is used to implement the linear error-correcting code. Another scheme that models the reliabilities of the SRAM cells is the so-called Soft-Decision (SD) helper data scheme. The SD scheme considers the one-probabilities of the SRAM cells as an input, which in practice are not observable. We present a new strategy for the SD scheme that considers the binary SRAM-PUF observations as an input instead and show that the new strategy is optimal and achieves the same reconstruction performance as the MO scheme. Finally, we present a variation on the MO helper data scheme that updates the helper data sequentially after each successful reconstruction of the key. As a result, the error-correcting performance of the scheme is improved over time.



Citation: Kusters, L.; Willems, F.M.J. Multiple Observations for Secret-Key Binding with SRAM PUFs. *Entropy* **2021**, *23*, 590. <https://doi.org/10.3390/e23050590>

Academic Editor: Boris Ryabko

Received: 7 April 2021
Accepted: 5 May 2021
Published: 11 May 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: secret-key agreement; Physical Unclonable Functions; helper data scheme; LDPC code

1. Introduction

The The Internet of Things (IoT) makes it possible to connect and share information between many different devices through the Internet. This sharing of information is beneficial for many applications, e.g., in healthcare or consumer electronics. At the same time, the information may be sensitive and should not fall into the wrong hands or be tampered with. Therefore, security is one of the main challenges of the IoT devices. Since the IoT devices are often small and low cost, securing the devices should come at a low price.

Secure communication is often achieved through cryptographic protocols that rely on secret keys. A low-cost alternative for secure storage of the keys is enabled by Static Random-Access Memory Physical Unclonable Functions (SRAM PUFs). A PUF is a physical object or device that responds to a challenge with a response that is unique and unpredictable [1,2]. The SRAM-PUF functionality is based on the uninitialized values of the SRAM. These are the values that appear in the memory cells directly after power up of the SRAM. The corresponding binary vector is unique for each SRAM and it is the result of small variations in the silicon material. It can be considered to be a noisy fingerprint of the device and can be used to generate and bind secret keys [3,4].

Since the SRAM-PUF observations are noisy, additional processing is required to ensure reliable reconstruction of the key. This can be achieved through a so-called key binding scheme, see Figure 1. The scheme considers two phases: an enrollment phase during which a uniformly generated key is bound to a first SRAM-PUF observation; and a reconstruction phase during which the key is reconstructed from an additional observation

of the SRAM-PUF. Please note that enrollment is usually performed only once, whereas reconstruction can be repeated many times. During enrollment, besides the key s , also some helper data w is generated. This helper data w ensures that the key can be reliably reconstructed even though y^n is a noisy version of x^n . The helper data are considered public, and therefore should not reveal information about the key s to an attacker.

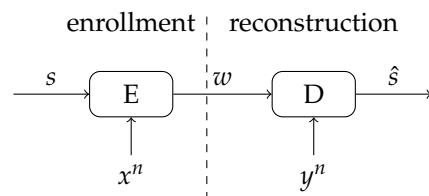


Figure 1. Key binding scheme for reliable secret-key reconstruction from noisy observations.

In classic helper data schemes, a single SRAM-PUF observation is used for enrollment and a single observation is used for reconstruction. However, it has been shown that the mutual information between the encoder and decoder observations increases when more observations are considered [5]. Since the secret-key capacity is equal to the mutual information (see Section 3), it follows that the achievable secret-key rate is increased when multiple SRAM-PUF observations are used instead of a single observation.

We introduce the Multiple-Observations (MO) helper data scheme, which enrolls a single key after processing multiple SRAM-PUF observation vectors. The scheme is based on a linear error-correcting code and can be seen as an extension of the fuzzy commitment scheme [6]. Any number of enrollment observations can be used. Furthermore, the performance of the scheme increases when more observations are used.

1.1. Related Work

A first implementation of a key binding scheme for generating and reconstructing a cryptographic key from SRAM PUFs was presented by Guajardo et al. in [4]. There, the fuzzy commitment scheme [6] was used to construct the helper data and later to reproduce the key. It is known that within one SRAM-PUF, some cells are more reliable (smaller error probability) than other cells [3]. The reliability information of the SRAM cells can be used to improve the performance of the helper data schemes. For example, a Soft-Decision (SD) helper data scheme [7,8] publicly shares the error probability of each SRAM cell to improve the decoder performance. Furthermore, a Selection-based helper data scheme [9–11] selects only the most reliable SRAM cells to reduce the average error probability of the SRAM-PUF observations. Both schemes assume that reliability of each SRAM cell is known during enrollment. However, in general this information is not available. Either, special measurement techniques must be applied, or a sufficient number of observations is required to estimate these values before enrollment. We propose a new scheme that accepts standard SRAM-PUF observation vectors as an input, i.e., the MO helper data scheme. In [12] multiple enrollment observations are used under various environmental conditions. The focus of [12] is on experimental validation of new strategies that consider multiple enrollment temperatures; however, a mathematical analysis of the strategies is missing. Our work focuses instead on finding an optimal multiple observations strategy. In the future, our analysis may be extended to consider temperature dependence as well, see Section 2.

Applying multiple observations for key binding (and generation) has been studied from information-theoretic perspective in [13–15]. It is shown that the secret-key rate can be improved when multiple observations are used by the encoder or the decoder. Achievable rate regions are analyzed for various multiple enrollments and multiple entities scenarios, but no code constructions are proposed or investigated.

Multiple enrollment scenarios are studied from leakage perspective in [16,17]. In these papers, scenarios are considered (e.g., the reverse fuzzy extractor [18]) in which enrollment is repeated multiple times and correspondingly multiple helper data are generated. Please

note that the additional helper data are not generated to increase performance; instead, they are considered to be a security challenge that follows from the repeated enrollments. The decoder performs a classic reconstruction that is based on a single helper data sequence only, whereas an attacker may have stored all previously generated helper data. It is shown in [17] that zero leakage is ensured in these multiple enrollment scenarios, when the SRAM PUFs meet a certain symmetry condition. Inspired by the zero leakage results of [17], we have developed the MO helper data scheme which produces a single helper data sequence based on repeated enrollments. In contrast to the scenarios discussed in the previous paragraph, the decoder now benefits from the additional observations which are embedded in the helper data.

1.2. Contributions and Outline

In Section 3, we define secret-key capacity for multiple enrollment observations and calculate its value for the SRAM-PUF statistical model. We show that secret-key capacity can increase significantly when more enrollment observations are considered. This observation is the main motivation for the results presented in this paper, which are listed as follows.

- We introduce the MO helper data scheme in Section 4. We prove that the helper data does not reveal any information about the key when the SRAM-PUF statistical model meets the symmetry assumption (Section 2). Then, we prove that secret-key capacity can be achieved with the MO helper data scheme for any number of enrollment observations.
- In Section 5, we present a code construction and evaluate performance of the scheme through Monte Carlo simulations.
- We propose a new variation on the Soft-Decision (SD) helper data scheme from [7] in Section 6. In contrast to the original scheme, this scheme considers binary SRAM-PUF observations as an input. We prove that the new SD strategy is optimal (achieves secret-key capacity) and that it can achieve the same reconstruction performance as the MO helper data scheme.
- In Section 7, we present a variation on the MO helper data scheme that can update the helper data sequentially. The error-correcting performance of the scheme improves after each successful key reconstruction, and therefore the performance improves over the lifetime of the device. This enables usage of less observations during the enrollment phase, when allowing worse initial reconstruction performance that is improved over time.

We conclude with a summary of our results. In the following, we first introduce the notation and the statistical model that we use for SRAM PUFs.

2. Notation and SRAM-PUF Statistical Model

In the following, we first introduce the notation that is used. Then, we present the statistical model that we use for SRAM PUFs which is based on the commonly used model introduced in [7]. We introduce a symmetry assumption which is required for the security of the MO helper data scheme. We derive several properties that are needed for the proofs later in this work.

2.1. Notation and Definitions

We use uppercase symbols to denote random variables and lowercase symbols to denote their realizations. We consider t enrollment observations of n SRAM cells, corresponding to t binary observation vectors of length n , i.e., $(x_1^n, x_2^n, \dots, x_t^n)$. The i th observation of the j th SRAM cell is represented by $x_{i,j}$, and assumes a value in $\{0, 1\}$. We often analyze the behavior of a single SRAM cell, in which case we omit the cell index j and we have (x_1, x_2, \dots, x_t) , corresponding to t observations of one SRAM cell.

The reconstruction observation vector is represented as y^n , with y_j the reconstruction observation of the j th SRAM cell. We use a distinct symbol for the reconstruction observation to emphasize its different functionality in the helper data scheme. Note, however,

that the reconstruction observations have the same statistical behavior as the enrollment observations, and they may as well have been represented as x_{t+1}^n , the $(t + 1)$ th observation of the SRAM cells.

Calligraphic letters are used for finite sets and $|\mathcal{S}|$ denotes the cardinality of the set \mathcal{S} . Finally, (conditional) entropy and mutual information are defined as in [19,20], with the base of the log equal to 2 and the units are bits. We define the binary entropy function as

$$h_2(p) \triangleq -p \log_2(p) - (1 - p) \log_2(1 - p). \tag{1}$$

2.2. Sram-Puf Statistical Model

2.2.1. One-Probability of a Cell

Each SRAM cell has a one-probability $\theta \in [0, 1]$ that defines the probability that a one is observed for this cell, i.e.,

$$\Pr(X = 1 | \Theta = \theta) = \theta. \tag{2}$$

In practice, we do not know the one-probability θ of each SRAM cell. Instead, the one-probability is a random variable, independent and identically distributed over the cells according to some known distribution $p_\Theta(\theta)$. And we can calculate the average one-probability

$$\Pr(X = 1) = \int_0^1 \theta p_\Theta(\theta) d\theta. \tag{3}$$

The currently most used model for PUFs [7] adopts the following Θ -distribution

$$p_\Theta(\theta) = \frac{\lambda_1 \phi(\lambda_2 - \lambda_1 \Phi^{-1}(\theta))}{\phi(\Phi^{-1}(\theta))}. \tag{4}$$

Here $\phi(x)$ and $\Phi^{-1}(x)$ are the probability density function and the inverse of the cumulative distribution function of the normal distribution. Furthermore, λ_1 and λ_2 are parameters that determine the average reliability and average one-probability of the SRAM cells, respectively.

It has been observed on several occasions [3,4,21] that the SRAM PUFs are *unbiased*, i.e.,

$$\Pr(X = 1) = \Pr(X = 0) = 1/2, \tag{5}$$

the average probability of observing a one is equal to the probability of observing a zero. This is a desirable property for PUFs as it ensures that the observations are completely unpredictable for an attacker. In [7], Maes et al. showed that the model (4) well represents their empirical data for $\lambda_1 = 0.065, \lambda_2 = 0.000$, which indeed corresponds to unbiased SRAM PUFs. In this paper, we assume an unbiased SRAM-PUF and set $\lambda_2 = 0$. It follows that the distribution of the one-probabilities is *symmetric*, i.e.,

$$p_\Theta(\theta) = p_\Theta(1 - \theta). \tag{6}$$

This symmetry of the one-probability distribution is a property of the SRAM-PUF model that is key for the zero-secrecy leakage of the multiple observation schemes discussed in this paper.

2.2.2. Multiple Observations

First, we consider multiple observations of a single SRAM cell. The probability of observing t observations (x_1, x_2, \dots, x_t) of an SRAM cell with Hamming weight $k = w_H(x_1, x_2, \dots, x_t)$ (where the Hamming weight is defined as the number of non-zero symbols in the sequence), is defined as

$$\begin{aligned} \pi_t(k) &\triangleq \Pr(X_1 = x_1, \dots, X_t = x_t) = \int_0^1 \Pr(X_1 = x_1, \dots, X_t = x_t | \Theta = \theta) p_\Theta(\theta) d\theta \\ &= \int_0^1 \theta^k (1 - \theta)^{t-k} p_\Theta(\theta) d\theta \stackrel{(a)}{=} \int_0^1 (1 - \theta')^k (\theta')^{t-k} p_\Theta(\theta') d\theta' = \pi_t(t - k), \end{aligned} \tag{7}$$

where in (a) we substituted with $\theta' = (1 - \theta)$ and applied the symmetry property (6). Please note that the probability only depends on the number of observed ones k , and the order of the observations is irrelevant. Furthermore, the probability of observing a length t sequence containing k ones is equal to the probability of observing a length t sequence containing k zeros. Similarly, the conditional probability of observing a value y given a previously observed sequence (x_1, x_2, \dots, x_t) , only depends on the number of previously observed ones k , i.e.,

$$\begin{aligned} \Pr(Y = y | X_1 = x_1, \dots, X_t = x_t) &\stackrel{(a)}{=} \frac{\Pr(Y=y, X_1=x_1, \dots, X_t=x_t)}{\Pr(X_1=x_1, \dots, X_t=x_t)} = \frac{\pi_{t+1}(k+y)}{\pi_t(k)} \\ &= \Pr(Y = y | w_H(X_1, \dots, X_t) = k) \stackrel{(b)}{=} \frac{\pi_{t+1}(t+1-(k+y))}{\pi_t(t-k)} \quad (8) \\ &= \Pr(Y = y \oplus 1 | w_H(X_1, \dots, X_t) = t - k), \end{aligned}$$

where in (a) we used Bayes' theorem and in (b) we used (7). Finally, the last step follows from the fact that $(1 - y) \equiv (y \oplus 1)$ for $y \in \{0, 1\}$.

2.2.3. Multiple SRAM Cells

All the equations that were derived for a single SRAM cell can be easily generalized to multiple SRAM cells. Since the one-probabilities are independent and identically distributed over the SRAM cells, the observations of different cells are also independent and the joint probability of t observations for n cells is

$$\Pr(X_1^n = x_1^n, X_2^n = x_2^n, \dots, X_t^n = x_t^n) = \prod_{j=1}^n \Pr(X_1 = x_{1,j}, \dots, X_t = x_{t,j}) = \prod_{j=1}^n \pi_t(k_j), \quad (9)$$

with $k_j = w_H(x_{1,j}, \dots, x_{t,j})$ the number of observed ones after t observations of the j th cell.

2.2.4. Θ -Distribution

Until now, we have assumed that $\lambda_2 = 0$ and thus the SRAM-PUF is unbiased. This assumption is sufficient for the security and achievability proofs in Section 4. However, to predict the performance of our scheme in a practical setting, we also need to set a value for λ_1 . In correspondence with previous works [7,11] we choose $\lambda_1 = 0.51$ for our simulations, which corresponds to average error probability regarding dominant (most likely) value of a cell

$$\bar{\psi} \triangleq \int_0^1 \min(\theta, (1 - \theta)) p_{\Theta}(\theta) d\theta \approx 0.15. \quad (10)$$

In Figure 2, we plot the Θ -distribution that is used for the calculations later in the paper. Please note that stable cells (one-probability close to 0 or 1) are more likely than unstable cells. We will see later that knowledge about the stability (error probability) of specific cells can improve the performance of helper data schemes.

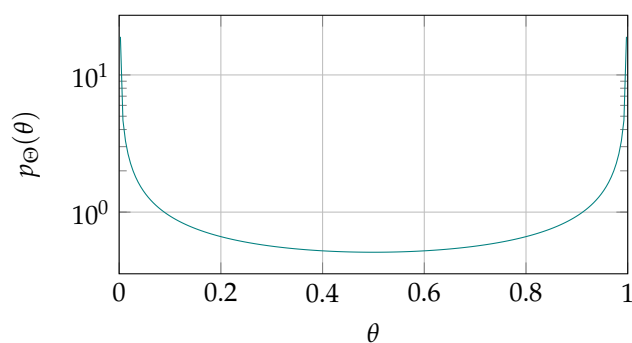


Figure 2. Distribution of the one-probability Θ as used for the simulations in this work. Generated according to the statistical model for SRAM-PUF [7] with $\lambda_1 = 0.51$, and $\lambda_2 = 0$.

Finally, note that temperature and voltage ramp-up time of the power up may influence the behavior of the SRAM PUFs [21]. Here, we do not model this behavior and only assume a worst-case average error probability of 0.15 (see (10)). However, it is worthwhile mentioning that the model (4) can be extended to also model the temperature dependence, see [22]. Knowledge about the temperature behavior can be exploited to improve the performance of the helper data schemes, especially when the temperature is known [23]. Therefore, in the future, it may be beneficial to extend the current work to also consider temperature dependent behavior of the SRAM PUFs.

3. Multiple Enrollment Observations for Increased Secret-Key Capacity

In this section, we describe a secret-key binding scheme with multiple enrollment observations, see Figure 3. We derive the achievable secret-key rate for the used statistical model and show that the rate can improve significantly when more enrollment observations are considered. These results motivate us to design a helper data scheme that can approach such rates in Section 4.

As in the classic (single enrollment) key binding scheme in Figure 1, we distinguish between an enrollment and a reconstruction phase.

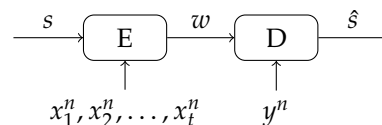


Figure 3. Secret-key binding with t observations by the encoder and a single observation by the decoder.

During enrollment, the secret key $s \in \{1, 2, \dots, |\mathcal{S}|\}$ is generated uniformly at random. An encoder obtains the secret key s and t observation vectors $(x_1^n, x_2^n, \dots, x_t^n)$, and generates corresponding helper data $w \in \mathcal{W}$. The helper data alphabet \mathcal{W} is specified by the encoding function that is used, see Section 4. We assume that the helper data w is stored and/or communicated in the public domain. Therefore, the helper data by itself should not reveal any information about the key. During reconstruction, a decoder observes a reconstruction vector y^n as well as the helper data w and maps this input to an estimate \hat{s} of the secret key. Reconstruction is successful when the estimate is equal to the original key, i.e., when $\hat{s} = s$.

We are now interested in the achievable secret-key rate of the scheme when enrollment is performed using t observation vectors of the SRAM-PUF, and where achievable rate is defined as follows.

Definition 1. A secret-key rate R_t is called achievable after t enrollment observations, if for all $\delta > 0$ and for all n large enough, there exist encoders and decoders such that

$$\Pr(\hat{S} \neq S) \leq \delta, \tag{11}$$

$$\frac{1}{n}H(S) = \frac{1}{n} \log_2 |\mathcal{S}| \geq R_t - \delta, \tag{12}$$

$$\frac{1}{n}I(S; W) \leq \delta. \tag{13}$$

The secret-key capacity C_t is the maximum achievable secret-key rate with t enrollment observations.

Here (11) requires that the key reconstruction is reliable, (12) that the key is uniformly distributed, and (13) limits the information leakage by the helper data about the key. Theorem 1 gives the fundamental limit on achievable secret-key rate for key binding schemes with t enrollment observations, and it follows from the results presented in [24,25].

Theorem 1. A secret-key rate R_t is achievable after t enrollment observations if and only if

$$R_t \leq I(Y; X_1, X_2, \dots, X_t). \tag{14}$$

The secret-key capacity $C_t = I(Y; X_1, X_2, \dots, X_t)$.

In Figure 4, we plot the secret-key capacity for an example SRAM-PUF. Here, we have assumed a symmetric distribution of the one-probabilities, and average error probability $\bar{\psi} \approx 0.15$, see Figure 2 for the Θ -distribution. The mutual information increases from 0.26 for a single enrollment observation, to 0.50 after 20 enrollment observations. This corresponds to almost doubling the secret-key rate regarding single enrollment.

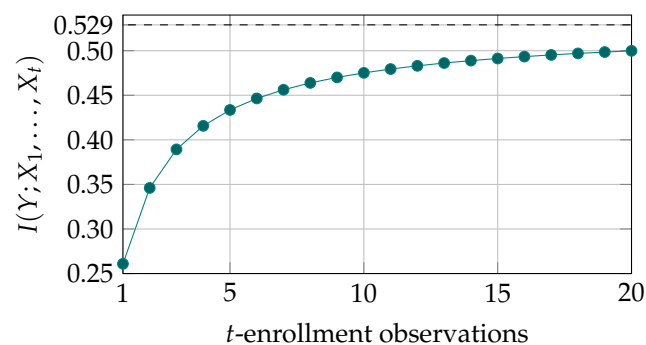


Figure 4. Secret-key capacity in bits per SRAM cell for the secret-key binding scheme with t enrollment observations, evaluated for SRAM PUFs given the Θ -distribution shown in Figure 2. The curve is approaching a limit that is represented by the dashed horizontal line.

In the plot, we also visualize an upper bound to the secret-key capacity, given by

$$\begin{aligned} I(Y; X_1, X_2, \dots, X_t) &\leq I(Y; X_1, X_2, \dots, X_t, \Theta) = I(Y; \Theta) + I(Y; X_1, X_2, \dots, X_t | \Theta) \\ &\stackrel{(a)}{=} I(Y; \Theta) = H(Y) - \int_0^1 H(Y | \Theta = \theta) p_{\Theta}(\theta) d\theta, \end{aligned} \tag{15}$$

where (a) follows from the Markov chain $Y \leftrightarrow \Theta \leftrightarrow (X_1, X_2, \dots, X_t)$. From the weak law of large numbers, i.e., $\lim_{t \rightarrow \infty} \Pr\left(\left|\frac{1}{t} \sum_{i=1}^t x_i - E[X_i]\right| > \epsilon\right) = 0$ for any $\epsilon > 0$, it follows that $\frac{1}{t} \sum_{i=1}^t x_i$ converges (in probability) to θ for $t \rightarrow \infty$. Therefore, the upper bound (15) can be achieved and we say

$$C_{\infty} = I(Y; \Theta) = H(Y) - \int_0^1 h_2(\theta) p_{\Theta}(\theta) d\theta. \tag{16}$$

4. Multiple-Observations Helper Data Scheme

We introduce the Multiple-Observations (MO) helper data scheme for binding a secret key to multiple observations of an SRAM-PUF, see Figure 5. First, we give a step-by-step description of the scheme. Then, we prove that it is secure. Finally, we prove that the scheme achieves the secret-key capacity C_t (see Theorem 1) for t enrollment observations and, therefore, that the MO helper data scheme is optimal. Please note that all derivations are under the symmetric Θ -distribution assumption (6).

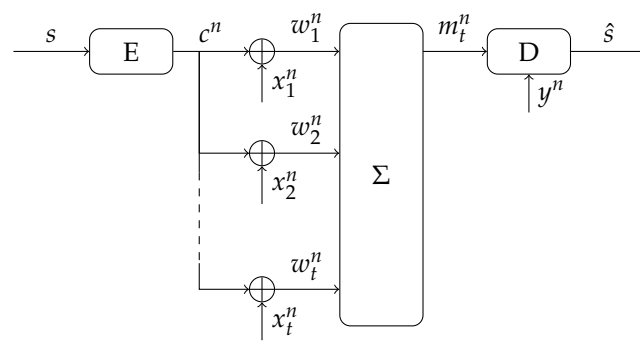


Figure 5. MO helper data scheme: t observations of the SRAM-PUF are used to generate a helper data m_t^n that is published and that can be used by the decoder (together with an additional SRAM-PUF observation) to reconstruct the key.

4.1. Description of the Scheme

First, a binary secret key $s \in \{0, 1\}^{\log_2 |\mathcal{S}|}$ is generated uniformly at random, such that $H(S) = \log_2 |\mathcal{S}|$, with $\log_2 |\mathcal{S}|$ an integer. The key s is then encoded using a linear error-correcting code into a codeword c^n . The codeword is XORed with all t enrollment vectors $(x_1^n, x_2^n, \dots, x_t^n)$, resulting in t sequences $(w_1^n, w_2^n, \dots, w_t^n)$, with

$$w_i^n = c^n \oplus x_i^n, \quad \text{for } i = 1, 2, \dots, t. \tag{17}$$

Please note that w_i^n corresponds to a helper data sequence of the classic fuzzy commitment scheme [6]. The helper data of the MO helper data scheme is constructed by adding all these sequences together, i.e., the helper data are

$$m_t^n \triangleq w_1^n + w_2^n + \dots + w_t^n = \sum_{i=1}^t (c^n \oplus x_i^n). \tag{18}$$

The helper data are stored on the device or in a database, and they are considered public information.

When the key must be recovered, the decoder observes the helper data m_t^n and another observation vector y^n of the SRAM-PUF. A decoder function maps each pair (m_t^n, y^n) to a corresponding estimate \hat{s} of the original secret. Ideally, the reconstructed secret \hat{s} is equal to the original secret. Furthermore, an attacker who can observe the helper data m_t^n should not obtain information about the secret.

4.2. Uniformity and Zero Leakage

First, by definition of the MO helper data scheme, the secret key is generated uniformly at random and therefore the uniformity condition of Definition 1, $\frac{1}{n} H(S) = \frac{1}{n} \log_2 |\mathcal{S}|$, is satisfied. Second, it has been shown in [17] that, for symmetric SRAM PUFs, zero leakage occurs by all the helper data after repeated enrollments, i.e., $I(S; W_1^n, \dots, W_t^n) = 0$. It follows that

$$I(S; M_t^n) \stackrel{(a)}{\leq} I(C^n; W_1^n, W_2^n, \dots, W_t^n) = 0, \tag{19}$$

where (a) follows from the data processing inequality (see [19] Chapter 2) for the Markov Chain

$$S \leftrightarrow C^n \leftrightarrow (W_1^n, W_2^n, \dots, W_t^n) \leftrightarrow M_t^n. \tag{20}$$

By (19) the MO helper data scheme achieves *strong secrecy*, i.e., $I(S; M_t^n) \leq \delta$.

4.3. Achievable Secret-Key Rate

Third, we derive the achievable rate over the channel from the encoder to the decoder. The channel is described by the conditional distribution $\Pr(M_t = m_t, Y = y | C = c)$, and

it follows from the channel coding theorem (see, e.g., [20], Chapter 3) that the maximum achievable rate is given by the mutual information maximized over the input distribution. Furthermore, C is uniform here, since we are using a linear code. We therefore evaluate this mutual information next

$$\begin{aligned}
 R_{MO,t}^* &\stackrel{\Delta}{=} I(C; M_t, Y) = I(C; M_t) + I(C; Y|M_t) \\
 &\stackrel{(a)}{=} H(Y|M_t) - H(Y|M_t, C) \\
 &\stackrel{(b)}{=} H(Y|M_t) - H(Y|w_H(X_1, X_2, \dots, X_t), C) \\
 &\stackrel{(c)}{=} 1 - H(Y|w_H(X_1, X_2, \dots, X_t)) \\
 &\stackrel{(d)}{=} H(Y) - H(Y|X_1, X_2, \dots, X_t) \\
 &= I(Y; X_1, X_2, \dots, X_t).
 \end{aligned} \tag{21}$$

Please note that (a) follows from zero leakage (see (24)), and (b) holds since (by (18)) the Hamming weight $w_H(x_1, x_2, \dots, x_t)$ is uniquely determined by m_t given c and vice-versa. Furthermore, (c) follows from (22) below and since the key and thus codebit c are generated independently from the SRAM-PUF observations. Finally, (d) follows from the fact that the symmetric SRAM-PUF is unbiased (5), and by the fact that the conditional probability of the next observation given t previous observations (x_1, x_2, \dots, x_t) only depends on the number of observed ones (7). The following derivation shows that the helper data integer m_t by itself does not reveal any information about the reconstruction observation y , and thus $H(Y|M_t) = 1$.

$$\begin{aligned}
 \Pr(Y = 1|M_t = m_t) &\stackrel{(a)}{=} \sum_{c \in \{0,1\}} \Pr(C = c) \Pr(Y = 1|M_t = m_t, C = c) \\
 &\stackrel{(b)}{=} \frac{1}{2} \Pr(Y = 1|w_H(X_1, \dots, X_t) = m_t, C = 0) \\
 &\quad + \frac{1}{2} \Pr(Y = 1|w_H(X_1, \dots, X_t) = t - m_t, C = 1) \\
 &\stackrel{(c)}{=} \frac{1}{2} \Pr(Y = 1|w_H(X_1, \dots, X_t) = m_t) \\
 &\quad + \frac{1}{2} \Pr(Y = 0|w_H(X_1, \dots, X_t) = m_t) = \frac{1}{2},
 \end{aligned} \tag{22}$$

where (a) follows from (23), (b) follows from the definition of the helper data (18), and in (c) we use the fact that the key and codebit c is generated independently from the SRAM-PUF observations, and furthermore we use the symmetry property for the conditional distribution (8) that we have derived for symmetric SRAM-PUF in Section 2. In the above derivation we use that

$$\Pr(C = c|M_t = m_t) = \Pr(C = c), \tag{23}$$

which can be derived from (19) by observing that

$$I(C; M_t) \stackrel{(a)}{\leq} I(S; M_t^n) = 0, \tag{24}$$

where (a) follows from the data processing inequality (see [19], Chapter 2) for the Markov Chain

$$C \leftrightarrow C^n \leftrightarrow S \leftrightarrow M_t^n \leftrightarrow M_t. \tag{25}$$

It follows from the derivations in Sections 4.2 and 4.3 that the MO helper data scheme achieves secret-key rate $R_{MO,t}^*$, where achievable secret-key rate is defined in Definition 1. Furthermore, $R_{MO,t}^* = C_t$ is equal to the secret-key capacity for t enrollment observations as given by Theorem 1, which shows that the MO helper data scheme is optimal.

5. Code Construction and Simulation Results

In the previous section, we have proved that secret-key capacity for t enrollment observations is achievable with the MO helper data scheme. However, the performance that is achieved in practice depends on the error-correcting code that is implemented by the encoder and decoder function. Here, performance is evaluated in terms of secret-key

rate (R) and reconstruction error probability (FER). Until now, we have not specified an error-correcting code. Please note that a Soft-Decision decoder should be used that can benefit from the reliability information of the SRAM cells. Furthermore, we are looking for codes that have a low rate and that perform well for relatively short blocklengths (128 key bits). Here, we use an off-the-shelf LDPC code to evaluate the expected performance of the scheme in a practical setting.

5.1. Encoder

First, a key s of 128 bits length is generated uniformly at random. The secret-key is then encoded using an error-correcting code, resulting in codeword c^n . As the error-correcting code we use a CRC (cyclic-redundancy check) code concatenated with an LDPC code as defined in the 5G NR (fifth generation new radio) standard [26]. For our simulations, we use the LDPC coding-chain implementation from the MATLAB 5G Toolbox [27]. The codeword c^n is XORed with t SRAM-PUF observation vectors of length n and the results are added together, resulting in helper data m_t^n . This concludes the encoder part of the scheme, where the helper data m_t^n is stored for later usage and all other variables are discarded.

The secret-key rate of our implementation is

$$R = \frac{128}{n} \quad \text{key bits per SRAM cell.} \quad (26)$$

Furthermore, for t enrollment observations of n SRAM cells the required number of bits for storage of the helper data are $n \lceil \log_2(t+1) \rceil$, and thus the helper data rate is

$$R^{\text{hd}} = \frac{\lceil \log_2(t+1) \rceil}{R} \quad \text{helper data bits per key bit.} \quad (27)$$

5.2. Decoder

The decoder uses an SRAM-PUF observation y^n and the previously stored helper data m_t^n to reconstruct the key \hat{s} . First, the log-likelihood ratios (LLR) of the received code bits are calculated. Since the SRAM cells are independently distributed, we can calculate the LLR of each bit separately. The LLR of a code bit c , after observing the corresponding helper data m_t and SRAM-PUF observation y , is

$$\text{LLR}(y, m_t) = \log \frac{\pi_{t+1}(y + m_t)}{\pi_{t+1}(y + t - m_t)}. \quad (28)$$

See the Appendix A.1 for a derivation of the above equation. Please note that there are $2(t+1)$ possible combinations of (y, m_t) . However, due to the symmetry properties of the LLR function (see Appendix A.1), we only need to store $\frac{(t+2)}{2}$ LLRs in a look-up table. Finally, the LDPC decoder uses an iterative Soft-Decision decoder (belief propagation algorithm), combined with CRC for error detection, to reconstruct the 128 bit secret \hat{s} from the received LLRs.

5.3. Simulation Results

We have simulated the MO helper data scheme using Monte Carlo simulations and the statistical model for SRAM PUFs that was presented in Section 2, with $\lambda_1 = 0.51$ and $\lambda_2 = 0$ and average error probability $\bar{\psi} \approx 0.15$. We plot the resulting error probability of the key reconstruction (FER) for various key rates R and number of enrollment observations t in Figure 6.

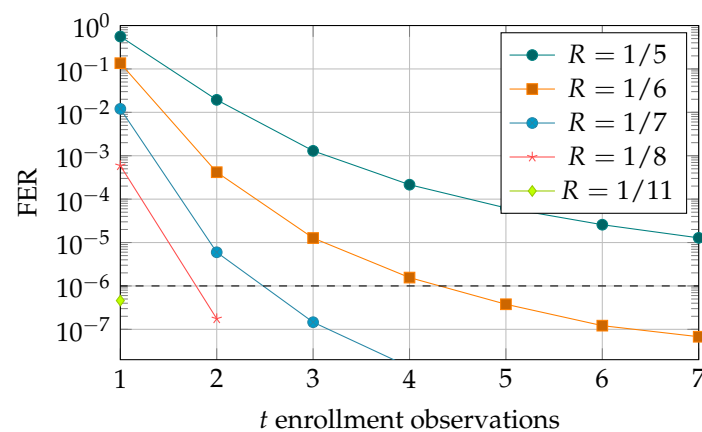


Figure 6. Reconstruction error probability FER for the MO helper data scheme, with 128 bit key and $128/R$ SRAM cells.

Observe that the error probability can be reduced by decreasing the secret-key rate R and by increasing the number of enrollment observations t . We choose $\text{FER} \leq 10^{-6}$ as the target error probability and find that $R = 1/6$ is the best (highest) achievable secret-key rate that achieves the target FER. Furthermore, at least 5 enrollment observations are required to achieve the target FER with this key rate, and the corresponding helper data rate is $R^{\text{hd}} \approx 15.5$. Another rate-enrollment pair that achieves the target FER is $R = 1/7$ for $t = 3$ enrollment observations, with corresponding helper data rate $R^{\text{hd}} \approx 14$. Please note that the classic single enrollment scheme (corresponding to MO scheme for $t = 1$) achieves the target FER for $R = 1/11$ or worse key rates. Furthermore, the helper data rate $R^{\text{hd}} = 11$ bits per key bit in this case. Therefore, the MO helper data scheme achieves a secret-key rate that is $11/6 \approx 1.8$ times higher than the single enrollment scheme. However, the improved secret-key rate comes at a cost since the helper data rate is $\frac{15.5}{11} \approx 1.4$ times as high in comparison to the classic scheme.

We conclude that a trade-off must be considered between the required enrollment time, helper data storage, and the number of SRAM cells, when selecting the parameters (enrollment observations and secret-key rate) for a given setting.

6. The Soft-Decision Helper Data Scheme

The performance increase of the MO helper data scheme, regarding the traditional single enrollment scheme, is mostly due to the fact that it can distinguish between reliable and unreliable SRAM cells. A well-known helper data scheme that also considers the reliability information of the SRAM cells is the Soft-Decision scheme introduced by Maes et al. [7]. In this section, we first describe the SD scheme and derive its achievable performance. We note that the SD scheme assumes that the one-probabilities of the SRAM cells are observable which in practice is often not the case. Therefore, a pre-processing step is required that estimates the one-probabilities of the SRAM cells. Based on this observation, we propose a variation on the SD scheme that instead directly considers the binary SRAM-PUF observations as an input. We show that the newly proposed strategy results in the same decoder LLRs as the MO scheme (for equal key and SRAM observations). This implies that both schemes achieve the same reconstruction performance, and thus, since the MO scheme is provably optimal, the newly proposed strategy for the binary SD scheme is optimal as well.

To the best of our knowledge, we are the first to propose an optimal strategy for the SD scheme with binary enrollment observations. Furthermore, we show that very few observations (less than 10) are sufficient to achieve an acceptable performance, whereas in the literature 64 observations are used [8] for the same statistical model and parameter settings that are used in the current work.

6.1. Description of (Regular) SD Helper Data Scheme

The SD helper data scheme, see Figure 7, observes the one-probability vector θ^n of all the cells, and derives the dominant values u^n , defined as

$$u \triangleq \begin{cases} 0 & \text{if } 0 \leq \theta \leq 1/2, \\ 1 & \text{if } 1/2 < \theta \leq 1, \end{cases} \quad (29)$$

and the error probability ψ^n (regarding the dominant value of the cell), defined as

$$\psi \triangleq \min(\theta, (1 - \theta)) = \begin{cases} \theta & \text{if } 0 \leq \theta \leq 1/2, \\ 1 - \theta & \text{if } 1/2 < \theta \leq 1, \end{cases} \quad (30)$$

with $\psi \in [0, 1/2]$. As in the MO helper data scheme, a key is generated uniformly at random, and encoded using a linear error-correcting code into a codeword c^n . Then the codeword is XORed with the dominant values u^n to create the helper data sequence

$$w^n = c^n \oplus u^n. \quad (31)$$

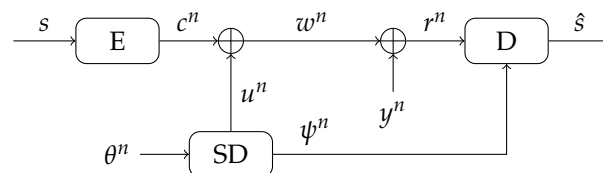


Figure 7. The Soft-Decision helper data scheme, with public information the helper data sequence w^n and error probabilities ψ^n .

Besides the helper data sequence w^n , also the reliability values ψ^n of the SRAM cells are stored publicly. For reconstruction, another observation y^n of the SRAM-PUF is XORed with the helper data, resulting in a noisy codeword

$$r^n = w^n \oplus y^n = c^n \oplus (u^n \oplus y^n), \quad (32)$$

where $(u^n \oplus y^n)$ is an error vector, and an error ($r_j = c_j \oplus 1$) occurs when the reconstruction observation y_j is flipped regarding the dominant value u_j of a cell. The decoder reconstructs the key \hat{s} based on the received noisy codeword r^n and the error probabilities of the cells ψ^n .

6.2. Achievable Performance

We are interested in the maximum achievable secret-key rate of the SD scheme. As for the MO scheme (Section 4.2) we should first show that the SD scheme is secure, i.e., the uniformity condition of Definition 1 is satisfied since the key is generated uniformly at random. Furthermore, the leakage condition is satisfied as $I(S; W^n, \Psi^n) = 0$ as is shown in Appendix A.2. Now, we can derive the achievable rate over the channel from the encoder to the decoder. The channel is described by the conditional distribution $\Pr(R = r, \Psi = \psi | C = c)$, and it follows from the channel coding theorem (see, e.g., [20], Chapter 3) that the maximum achievable rate is given by the mutual information maximized over the input distribution. Furthermore, C is uniform here, since we are using a linear code. We therefore evaluate this mutual information next

$$R_{SD,\infty}^* \triangleq I(C; R, \Psi) \stackrel{(a)}{=} I(C; R | \Psi) \stackrel{(b)}{=} 1 - \int_0^{1/2} h_2(\psi) p_\Psi(\psi) d\psi. \quad (33)$$

In (a) we used the fact that the key is generated independently from the SRAM-PUF observations and thus $I(C; \Psi) = 0$. In (b) we used the fact that $r = c \oplus (u \oplus y)$ so the channel from encoder to decoder can be modeled as a binary symmetric channel with cross-over probability ψ (the probability that $u \neq y$). Please note that $R_{SD,\infty}^* = C_\infty$ (for

symmetric SRAM-PUF) this rate is equal to the limit (for t to infinity) of the secret-key capacity for multiple enrollment observations, see (16). Therefore, the SD helper data scheme is optimal, and furthermore the MO helper data scheme approaches the same key rate as the SD helper data scheme when sufficient enrollment observations are used.

6.3. New SD Strategy for Binary Enrollment Observations

In practice, the one-probabilities θ^n are non-observable and therefore, they must be estimated based on the binary observation vectors $(x_1^n, x_2^n, \dots, x_t^n)$ before the SD scheme can be applied. Instead of applying a pre-processing step for estimation, we propose to adjust the SD scheme s.t. the dominant values and error probabilities are directly estimated based on t binary observations. The dominant value of an SRAM cell is then estimated as

$$\hat{u}_t \triangleq \begin{cases} 0 & \text{if } w_H(x_1, \dots, x_t) \leq t/2, \\ 1 & \text{otherwise.} \end{cases} \tag{34}$$

And furthermore, the error probability (regarding the dominant value) is

$$\hat{\psi}_t \triangleq \frac{\pi_{t+1}(1 + m_t^{\text{SD}})}{\pi_t(m_t^{\text{SD}})}, \tag{35}$$

with

$$\begin{aligned} m_t^{\text{SD}} &\triangleq \min(w_H(x_1, \dots, x_t), t - w_H(x_1, \dots, x_t)) \\ &= \begin{cases} w_H(x_1, \dots, x_t) & \text{if } w_H(x_1, \dots, x_t) \leq t/2, \\ t - w_H(x_1, \dots, x_t) & \text{otherwise.} \end{cases} \end{aligned} \tag{36}$$

In Appendix A.3 we show that (36) indeed is equal to the error probability (regarding the dominant value) of a cell given the t binary enrollment observations.

The helper data and noisy codeword are constructed as before, so $w^n = c^n \oplus \hat{u}_t^n$ and $r^n = c^n \oplus (\hat{u}_t^n \oplus y^n)$. The decoder reconstructs the key \hat{s} based on the received noisy codeword r^n and the error probabilities of the cells $\hat{\psi}_t^n$.

6.4. Achievable Performance

We are interested in the maximum achievable secret-key rate of the binary SD scheme. As before we should first show that the scheme is secure, i.e., the uniformity condition of Definition 1 is satisfied since the key is generated uniformly at random. Furthermore, the leakage condition is satisfied as $I(S; W^n, \hat{\Psi}_t^n) = 0$ as is shown in Appendix A.4. Now, we can derive the achievable rate over the channel from the encoder to the decoder. The channel is described by the conditional distribution $\Pr(R = r, \hat{\Psi}_t = \hat{\psi}_t | C = c)$, and it follows from the channel coding theorem (see, e.g., [20], Chapter 3) that the maximum achievable rate is given by the mutual information maximized over the input distribution. Furthermore, C is uniform here, since we are using a linear code. We therefore evaluate this mutual information next

$$\begin{aligned} R_{\text{SD},t}^* &\stackrel{(a)}{\triangleq} I(C; R, \hat{\Psi}_t) \stackrel{(a)}{=} I(C; R | \hat{\Psi}_t) = H(R | \hat{\Psi}_t) - H(R | \hat{\Psi}_t, C) \\ &\stackrel{(b)}{=} 1 - H(\hat{U}_t \oplus Y | \hat{\Psi}_t) \stackrel{(c)}{=} 1 - H(\hat{U}_t \oplus Y | M_t^{\text{SD}}, \hat{U}_t) = 1 - H(Y | M_t^{\text{SD}}, \hat{U}_t) \\ &\stackrel{(d)}{=} 1 - H(Y | w_H(X_1, X_2, \dots, X_t)) \stackrel{(e)}{=} H(Y) - H(Y | X_1, X_2, \dots, X_t) \\ &= I(Y; X_1, X_2, \dots, X_t). \end{aligned} \tag{37}$$

In (a) we used the fact that the key is generated independently from the SRAM-PUF observations and thus $I(C; \hat{\Psi}_t) = 0$. In (b) we used that $r = c \oplus (\hat{u}_t \oplus y)$ and furthermore the key (and codebit) is generated uniformly and independently from the SRAM-PUF

observations (and thus also independently from $\hat{\psi}_t$). Furthermore, (c) follows by the Markov Chain

$$Y \oplus \hat{U}_t \leftrightarrow \hat{\Psi}_t \leftrightarrow (M_t^{\text{SD}}, \hat{U}_t), \quad (38)$$

and (d) holds since (by (18)) $w_H(x_1, x_2, \dots, x_t)$ is uniquely determined by the tuple $(m_t^{\text{SD}}, \hat{u}_t)$ and vice-versa. Finally, (e) follows from the fact that the symmetric SRAM-PUF is unbiased (5), and by the fact that the conditional probability of the next observation given t previous observations (x_1, x_2, \dots, x_t) only depends on the number of observed ones (7).

It follows from the derivations above that the binary SD scheme achieves secret-key rate $R_{\text{SD},t}^*$, where achievable secret-key rate is defined in Definition 1. Furthermore, $R_{\text{SD},t}^* = C_t$ is equal to the secret-key capacity for t enrollment observations as given by Theorem 1, which shows that the binary SD scheme is optimal.

6.5. Code Construction and Simulations

As with the MO scheme we can now define a code construction, with a uniformly generated secret s , an encoder based on an off-the-shelf LDPC code, and where the helper data w^n and reliability information $\hat{\psi}_t^n$ are constructed as explained in Section 6.3.

The decoder observes r^n and the error probabilities $\hat{\psi}_t$ which can be used to calculate the log-likelihood ratios needed for reconstruction of the secret. Since the SRAM cells are independently distributed, we can calculate the LLR of each bit separately. The LLR for a codebit c , after observing the noisy codebit r and the error probability $\hat{\psi}_t$ for t enrollment observations, is

$$\text{LLR}^{\text{SD}}(r, \hat{\psi}_t) = \begin{cases} \log \frac{\hat{\psi}_t}{1-\hat{\psi}_t} & \text{if } r = 1, \\ \log \frac{1-\hat{\psi}_t}{\hat{\psi}_t} & \text{otherwise.} \end{cases} \quad (39)$$

See Appendix A.5 for a derivation.

It is shown in Appendix A.5 that the LLRs for the SD scheme are equal to the LLRs for the MO scheme when the same enrollment observations (x_1, \dots, x_t) and reconstruction observation y are generated by the SRAM-PUF. Therefore, simulations for the SD scheme would give the same FER results as for the MO scheme, and we can use the plots in Figure 6 to predict the performance of the SD scheme.

7. Sequential MO Helper Data Scheme

We have seen in Section 5 that a better performance (smaller reconstruction error probability) is often achieved when the number of enrollment observations is increased. However, each enrollment observation requires a full reset (power off and power up) of the SRAM-PUF. Therefore, considering more enrollment observations results in an increased duration of the enrollment phase of the MO helper data scheme. This may be undesirable in practice as the enrollment phase must be completed in a secure environment and limited time is available.

In this section, we present a variation on the MO helper data scheme that we call the Sequential Multiple-Observations (SMO) helper data scheme. We exploit the fact that a new SRAM-PUF observation is required for each key reconstruction, and, after the reconstruction, we use this additional observation to update the helper data. As a result, the helper data are updated (sequentially) after each reconstruction, and thus the reconstruction error rate is reduced over time. The SMO scheme improves the efficiency regarding the MO scheme, since observations are used both for reconstruction and enrollment. Furthermore, the SMO scheme enables the usage of a reduced number of observations during the enrollment phase. The reduced number of enrollment observations comes at an initial cost of larger reconstruction error probability (FER); however, this is quickly reduced (see Figure 8) during the lifetime of the device.

7.1. Description

The enrollment phase of the Sequential MO helper data scheme is the same as for the MO helper data scheme, i.e., a key s is generated uniformly at random, and the helper data are constructed according to (18), with $t = t_0$ enrollment observations. Therefore, after the initial enrollment, a helper data $m_{t_0}^n$ is stored that is based on t_0 enrollment observations. The reconstruction phase, however, is different than before and it is visualized in Figure 8.

In the reconstruction phase of the SMO scheme, the helper data m_t^n (corresponding to t SRAM-PUF observations) and an SRAM-PUF observation y^n are used to reconstruct the key \hat{s} . If reconstruction is successful (We assume that correctness of the key can be verified, for example, by feedback from other protocols that apply the key for decryption, or by a failed authentication.), the SRAM-PUF observation is XORed with the encoded secret and is added to the existing helper data, which results in a new (improved) helper data corresponding to $t + 1$ SRAM-PUF observations. If, on the other hand, reconstruction has failed, it is not possible to reconstruct the original codeword c^n which is required for the helper data update. Therefore, the helper data remains the same as before in this case.

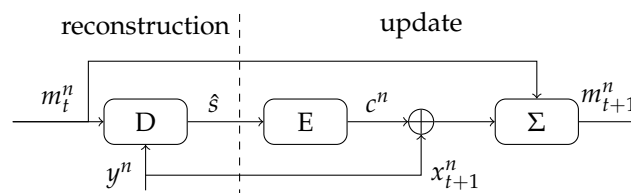


Figure 8. Reconstruction phase of the Iterative MO helper data scheme: the helper data m_t^n is updated to m_{t+1}^n after each successful reconstruction.

7.2. Security and Achievable Rate

The main difference between the Sequential MO helper data scheme and the original MO helper data scheme is that the helper data are now updated sequentially in the field. Therefore, an attacker may have access to multiple helper data $(m_1^n, m_2^n, \dots, m_t^n)$, instead of only the final helper data m_t^n . However, despite the reveal of multiple helper data, we can show that zero-secrecy leakage is still guaranteed. In particular, a similar Markov Chain as defined in (20) holds in this case

$$S \leftrightarrow C^n \leftrightarrow (W_1^n, W_2^n, \dots, W_t^n) \leftrightarrow (M_1^n, M_2^n, \dots, M_t^n). \tag{40}$$

Therefore, we can repeat the same derivations as in Section 4.2 to show that

$$I(S; M_1^n, M_2^n, \dots, M_t^n) \leq I(C^n; W_1^n, W_2^n, \dots, W_t^n) = 0, \tag{41}$$

and thus, there is no information leakage about the key by all the revealed helper data.

Please note that only the helper data are updated, whereas the key that has been generated during the enrollment phase remains the same. Since the key should be reconstructable already after the initial enrollment (since successful reconstruction is required for each update), the maximum achievable rate of the Sequential MO scheme is limited by the number of observations t_0 that is used for the initial enrollment, i.e.,

$$R_{SMO,t_0}^* = R_{MO,t_0}^* = I(Y; X_1, X_2, \dots, X_{t_0}). \tag{42}$$

Nevertheless, as we show in the next subsection, the main advantage of the SMO scheme is that the reconstruction observations are exploited to improve the reconstruction error probability over time.

7.3. Simulation Results

We evaluate the performance of the Sequential MO helper data scheme through Monte Carlo simulations. The encoder and decoder constructions and LLR calculations are similar

to the construction presented in Section 5. We evaluate two key rates, $R = 1/6$ and $R = 1/7$ with $t_0 = 4$ and $t_0 = 2$ enrollment observations, respectively. We have chosen the number of enrollment observations s.t. the achieved initial error probability is larger than, but close to, the target $\text{FER} < 10^{-6}$ (based on the previous results in Figure 6). We simulate 4 consecutive reconstruction attempts of the SMO scheme and plot the FER as function of the number of reconstruction attempts (time) in Figure 9. Please note that the helper data are only updated when the reconstruction attempt is successful. Therefore, the ‘reconstructions’ in the current simulation are different from ‘ t enrollment observations’ plotted on the x-axis in Figure 9.

First, we can directly observe that the FER reduces with each reconstruction attempt. Therefore, indeed the SMO scheme supports an improved reconstruction performance over the lifetime of the devices. More specifically, for the simulated rates and selected number of enrollment observations, we see that the average error probability already reduces below the required threshold $\text{FER} < 10^{-6}$ after the first reconstruction attempt. Therefore, in both cases, the initial cost (larger FER) of reducing the number of enrollment observations by one, was already nullified after one reconstruction.

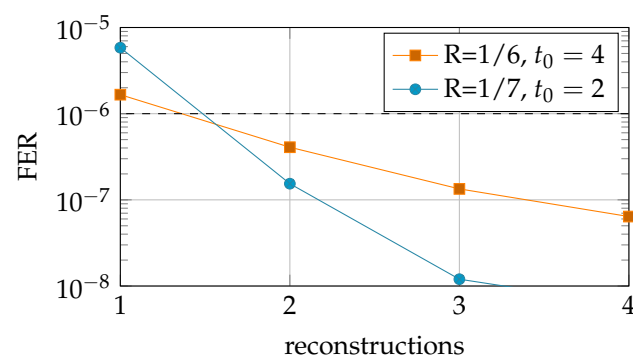


Figure 9. Reconstruction error probability FER for consecutive reconstructions for the Sequential MO helper data scheme, with 128 bit key.

8. Conclusions

We have presented the Multiple-Observations (MO) helper data scheme for binding a secret key to multiple observations of an SRAM-PUF. We have shown that the MO helper data scheme can achieve secret-key capacity corresponding to t enrollment observations, and therefore the scheme is optimal in information-theoretic sense. Furthermore, we have evaluated performance of the scheme with Monte Carlo simulations for a standard statistical model for SRAM PUFs with average error probability $\bar{\psi} \approx 0.15$. Secret-key rate $R = 1/6$ is sufficient to achieve $\text{FER} \leq 10^{-6}$ after $t = 5$ enrollment observations. This is a key rate that is $11/6 \approx 1.8$ times higher (better) than for the single enrollment scheme with comparable FER.

The MO helper data scheme is very similar to the Soft-Decision (SD) helper data scheme; however, the SD scheme assumes one-probabilities as an input, which in practice are non-observable. Therefore, we proposed a new strategy that considers binary observations instead. We have shown that this new strategy is optimal and achieves the same reconstruction performance as the MO scheme.

We have introduced a variation on the MO scheme, which we call the Sequential Multiple-Observations helper data scheme. The scheme supports a sequential update of the helper data after each successful reconstruction of the key, resulting in a reduced FER over the lifetime of the device. The SMO scheme enables the usage of less enrollment observations, by accepting a (slightly) worse initial FER that is quickly improved upon.

Author Contributions: Conceptualization, L.K. and F.M.J.W.; Formal analysis, L.K. and F.M.J.W.; Software, L.K.; Writing—original draft, L.K.; Writing—review & editing, F.M.J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Eurostars-2 joint program with co-funding from the EU Horizon 2020 program under the E! 11897 RESCURE project.

Data Availability Statement: The plots in Figures 2, 4 6 and 9 are based on calculations and simulations performed in MATLAB. The scripts can be found at <https://github.com/TUE-ICTLab/Multiple-Observations-for-Secret-Key-Binding-with-SRAM-PUFs> (accessed on 7 April 2021).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SRAM	Static Random-Access Memory
PUF	Physical Unclonable Function
MO	Multiple Observations
SMO	Sequential Multiple Observations
SD	Soft Decision
LDPC	Low-density Parity-check
LLR	Log-likelihood ratio
CRC	cyclic-redundancy check

Appendix A.

Appendix A.1. Log-Likelihood Ratio for MO Helper Data Scheme

We give the derivation that leads to (28) the log-likelihood ratio for a codebit c , after observing the current observation y and the helper data m_t for t enrollment observations. We start by deriving the likelihood for $c = 0$,

$$\begin{aligned} \Pr(Y = y, M_t = m_t | C = 0) &\stackrel{(a)}{=} \Pr(Y = y, w_H(X_1, \dots, X_t) = m_t | C = 0) \\ &\stackrel{(b)}{=} \Pr(Y = y, w_H(X_1, \dots, X_t) = m_t) \\ &= \binom{t}{m_t} \pi_{t+1}(y + m_t), \end{aligned} \quad (A1)$$

where (a) follows from the definition of the helper data (18), and in (b) we used the fact that the code bit c is generated independently from the SRAM observations. We can repeat a similar derivation to find the likelihood for $c = 1$,

$$\Pr(Y = y, M_t = m_t | C = 1) = \binom{t}{t - m_t} \pi_{t+1}(y + t - m_t), \quad (A2)$$

and the log-likelihood ratio is then

$$\begin{aligned} \text{LLR}(y, m_t) &\stackrel{\Delta}{=} \log \frac{\Pr(Y=y, M_t=m_t | C=0)}{\Pr(Y=y, M_t=m_t | C=1)} \\ &= \log \frac{\pi_{t+1}(y+m_t)}{\pi_{t+1}(y+t-m_t)}. \end{aligned} \quad (A3)$$

Please note that we can derive the following two symmetry properties for the LLR function

$$\begin{aligned} \text{LLR}(y, m_t) &= -\log \frac{\pi_{t+1}(y+t-m_t)}{\pi_{t+1}(y+m_t)} \\ &= -\text{LLR}(y, t - m_t), \\ \text{LLR}(y, m_t) &\stackrel{(a)}{=} \log \frac{\pi_{t+1}(t+1-y-m_t)}{\pi_{t+1}(t+1-y-t+m_t)} \\ &= \log \frac{\pi_{t+1}((y \oplus 1) + t - m_t)}{\pi_{t+1}((y \oplus 1) + m_t)} \\ &= \text{LLR}(y \oplus 1, t - m_t), \end{aligned} \quad (A4)$$

where (a) follows from (7) which follows from the symmetry assumption for SRAM PUFs.

Appendix A.2. Zero Leakage Proof for Traditional SD Helper Data Scheme

We show that for the SD helper data scheme zero leakage occurs about the secret s , by the helper data w^n and error probability information ψ^n , i.e.,

$$\begin{aligned} I(S; W^n, \Psi^n) &\stackrel{(a)}{\leq} I(C^n; W^n, \Psi^n) = I(C^n; \Psi^n) + I(C^n; W^n | \Psi^n) \\ &\stackrel{(b)}{=} H(W^n | \Psi^n) - H(W^n | \Psi^n, C^n) \\ &\stackrel{(c)}{=} H(W^n | \Psi^n) - H(U^n | \Psi^n) \stackrel{(d)}{\leq} n - n = 0. \end{aligned} \quad (\text{A5})$$

Where (a) follows from the data processing inequality (see [19], Chapter 2) with $C^n = g(S)$ a function of S , and (b) follows since the secret is generated independently from the SRAM-PUF observations. Furthermore, (c) follows since $w^n = u^n \oplus c^n$ (31) and since the secret is generated independently from the SRAM-PUF observations. Finally, (d) follows from the upperbound of entropy, by the fact that the SRAM cells are independently distributed, and by the derivations below.

$$\begin{aligned} \Pr(U = 0 | \Psi = \psi) &= \int_0^{1/2} p_{\Theta | \Psi}(\theta | \psi) d\theta \stackrel{(a)}{=} \frac{1}{2} \int_0^{1/2} \delta(\theta - \psi) + \delta(\theta - (1 - \psi)) d\theta \\ &= \frac{1}{2} = \Pr(U = 1 | \Psi = \psi), \end{aligned} \quad (\text{A6})$$

where $\delta(\cdot)$ is the Dirac delta function, and in (a) we used symmetry of the SRAM-PUF (6) and definition (30).

Appendix A.3. Reliability Estimate for Binary SD Helper Data Scheme

We show that indeed the error probability of the SRAM cells can be estimated as (35), i.e.,

$$\hat{\psi}_t = \Pr(Y \neq \hat{U} | X_1, \dots, X_t) \stackrel{(a)}{=} \frac{\Pr(Y \neq \hat{U}, X_1, \dots, X_t)}{\Pr(X_1, \dots, X_t)} \stackrel{(b)}{=} \frac{\pi_{t+1}(1 + m_t^{\text{SD}})}{\pi_t(m_t^{\text{SD}})} \stackrel{(c)}{=} \frac{\pi_{t+1}(t - m_t^{\text{SD}})}{\pi_t(m_t^{\text{SD}})}. \quad (\text{A7})$$

Here (a) follows from Bayes' theorem and (b) and (c) both follow from (A8) and (A9) below.

$$\begin{aligned} \Pr(Y \neq \hat{U}, X_1, \dots, X_t) &= \begin{cases} \Pr(Y = 1, X_1, \dots, X_t) & \text{if } w_H(x_1, x_2, \dots, x_t) \leq t/2, \\ \Pr(Y = 0, X_1, \dots, X_t) & \text{otherwise,} \end{cases} \\ &= \begin{cases} \pi_{t+1}(1 + w_H(x_1, x_2, \dots, x_t)) & \text{if } w_H(x_1, x_2, \dots, x_t) \leq t/2, \\ \pi_{t+1}(w_H(x_1, x_2, \dots, x_t)) & \text{otherwise,} \end{cases} \\ &\stackrel{(a)}{=} \begin{cases} \pi_{t+1}(1 + m_t^{\text{SD}}) & \text{if } w_H(x_1, x_2, \dots, x_t) \leq t/2, \\ \pi_{t+1}(t - m_t^{\text{SD}}) & \text{otherwise,} \end{cases} \\ &\stackrel{(b)}{=} \pi_{t+1}(1 + m_t^{\text{SD}}) = \pi_{t+1}(t - m_t^{\text{SD}}), \end{aligned} \quad (\text{A8})$$

where (a) follows from definition (36) and (b) follows from (7). Furthermore,

$$\Pr(X_1, \dots, X_t) = \pi_t(w_H(x_1, x_2, \dots, x_t)) \stackrel{(a)}{=} \pi_t(t - w_H(x_1, x_2, \dots, x_t)) \stackrel{(b)}{=} \pi_t(m_t^{\text{SD}}) \quad (\text{A9})$$

where (a) follows from (7) and (b) follows from (36).

Appendix A.4. Zero Leakage Proof for Binary SD Helper Data Scheme

We show that the strategy presented in Section 6.3 ensures zero leakage about the key by the published helper data w^n and error probabilities $\hat{\psi}_t^n$. Since this is a variation

on the standard SD helper data scheme, we can repeat similar derivations to (A5) to show that indeed

$$I(S; W^n, \hat{\Psi}_t^n) \leq H(W^n | \hat{\Psi}_t^n) - H(\hat{U}_t^n | \hat{\Psi}_t^n) \leq n - n = 0. \tag{A10}$$

In the last step we used that

$$H(\hat{U}_t^n | \hat{\Psi}_t^n) \geq H(\hat{U}_t^n | \hat{\Psi}_t^n, M_t^{\text{SD}n}) = n, \tag{A11}$$

which follows from

$$\begin{aligned} \Pr(\hat{U}_t = 0 | \hat{\Psi}_t = \hat{\psi}_t, M_t^{\text{SD}} = m_t^{\text{SD}}) &= \Pr(w_H(X_1, \dots, X_t) \leq t/2 | M_t^{\text{SD}} = m_t^{\text{SD}}) \\ &\stackrel{(a)}{=} \frac{\Pr(w_H(X_1, \dots, X_t) = m_t^{\text{SD}})}{\Pr(w_H(X_1, \dots, X_t) = m_t^{\text{SD}}) + \Pr(w_H(X_1, \dots, X_t) = t - m_t^{\text{SD}})} \\ &= \frac{\pi_t(m_t^{\text{SD}})}{\pi_t(m_t^{\text{SD}}) + \pi_t(t - m_t^{\text{SD}})} = \frac{1}{2} = \Pr(\hat{U}_t = 1 | \hat{\Psi}_t = \hat{\psi}_t, M_t^{\text{SD}} = m_t^{\text{SD}}). \end{aligned} \tag{A12}$$

Appendix A.5. Log-Likelihood Ratio for Binary SD Helper Data Scheme

We give the derivation that leads to (39) the log-likelihood ratio for a codebit c , after observing the noisy codebit r and the error probability $\hat{\psi}_t$ for t enrollment observations. First, we note that

$$1 - \hat{\psi}_t = 1 - \frac{\pi_{t+1}(1 + m_t^{\text{SD}})}{\pi_t(m_t^{\text{SD}})} = \frac{\pi_t(m_t^{\text{SD}}) - \pi_{t+1}(1 + m_t^{\text{SD}})}{\pi_t(m_t^{\text{SD}})} \stackrel{(a)}{=} \frac{\pi_{t+1}(m_t^{\text{SD}})}{\pi_t(m_t^{\text{SD}})} \stackrel{(b)}{=} \frac{\pi_{t+1}(1 + t - m_t^{\text{SD}})}{\pi_t(m_t^{\text{SD}})} \tag{A13}$$

in (a) we used that $\pi_t(m_t^{\text{SD}}) = \pi_{t+1}(m_t^{\text{SD}}) + \pi_{t+1}(1 + m_t^{\text{SD}})$ and (b) follows from (7). The log-likelihood ratio at the encoder, for a received value r and given an estimated error probability $\hat{\psi}_t$, is

$$\begin{aligned} \text{LLR}^{\text{SD}}(r, \hat{\psi}_t) &\triangleq \log \frac{\Pr(R=r, \hat{\Psi}_t=\hat{\psi}_t | C=0)}{\Pr(R=r, \hat{\Psi}_t=\hat{\psi}_t | C=1)} \\ &= \log \frac{\Pr(\hat{U}_t \oplus Y=r | \hat{\Psi}_t=\hat{\psi}_t)}{\Pr(\hat{U}_t \oplus Y=r, \hat{\Psi}_t=\hat{\psi}_t)} \\ &= \begin{cases} \log \frac{\Pr(\hat{U}_t \neq Y | \hat{\Psi}_t=\hat{\psi}_t)}{\Pr(\hat{U}_t=Y, \hat{\Psi}_t=\hat{\psi}_t)} & \text{if } r = 1, \\ \log \frac{\Pr(\hat{U}_t=Y | \hat{\Psi}_t=\hat{\psi}_t)}{\Pr(\hat{U}_t \neq Y, \hat{\Psi}_t=\hat{\psi}_t)} & \text{otherwise,} \end{cases} \\ &= \begin{cases} \log \frac{\hat{\psi}_t}{1-\hat{\psi}_t} & \text{if } r = 1, \\ \log \frac{1-\hat{\psi}_t}{\hat{\psi}_t} & \text{otherwise.} \end{cases} \end{aligned} \tag{A14}$$

In the following, we show that the LLR of the SD scheme is equal to the LLR for the MO scheme when the same enrollment observations (x_1, \dots, x_t) and reconstruction observation y are generated by the SRAM-PUF.

First, we can express the log-likelihood ratio (A14) as a function of m_t^{SD}

$$\begin{aligned} \text{LLR}^{\text{SD}}(r, m_t^{\text{SD}}) &\triangleq \begin{cases} \log \frac{\pi_{t+1}(1+m_t^{\text{SD}})}{\pi_t(1+t-m_t^{\text{SD}})} & \text{if } r = 1, \\ \log \frac{\pi_t(m_t^{\text{SD}})}{\pi_{t+1}(t-m_t^{\text{SD}})} & \text{otherwise.} \end{cases} \\ &= \log \frac{\pi_{t+1}(r+m_t^{\text{SD}})}{\pi_t(r+t-m_t^{\text{SD}})}. \end{aligned} \tag{A15}$$

Furthermore,

$$\begin{aligned}
 m_t^{\text{SD}} &= \begin{cases} m_t & \text{if } c = 0 \text{ and } w_H(x_1, \dots, x_t) \leq t/2, \\ & \text{or if } c = 1 \text{ and } w_H(x_1, \dots, x_t) > t/2, \\ t - m_t & \text{otherwise,} \end{cases} \\
 &= \begin{cases} m_t & \text{if } r = y, \\ t - m_t & r = y \oplus 1, \end{cases} \quad (\text{A16})
 \end{aligned}$$

where in the last step we used the definition of \hat{u}_t (29) and the fact that $r = c \oplus \hat{u}_t \oplus y$.

Combining (A15) and (A16) we find that the log-likelihood ratio for the SD scheme is

$$\begin{aligned}
 \text{LLR}'^{\text{SD}}(r, m_t^{\text{SD}}) &= \begin{cases} \text{LLR}'^{\text{SD}}(y, m_t) & \text{if } r = y, \\ \text{LLR}'^{\text{SD}}(y \oplus 1, t - m_t) & \text{if } r = y \oplus 1, \end{cases} \\
 &= \begin{cases} \log \frac{\pi_{t+1}(y+m_t)}{\pi_t(y+t-m_t)} & \text{if } r = y, \\ \log \frac{\pi_{t+1}((y \oplus 1)+t-m_t)}{\pi_t((y \oplus 1)+m_t)} & \text{if } r = y \oplus 1, \end{cases} \quad (\text{A17}) \\
 &= \log \frac{\pi_{t+1}(y+m_t)}{\pi_t(y+t-m_t)}.
 \end{aligned}$$

In the last step we used (7). Now the last expression in (A17) is equal to the log-likelihood ratio for the MO helper data scheme (28). Therefore, we conclude that the LLRs of both schemes are equal when the same enrollment observations (x_1, \dots, x_t) , codebit c and reconstruction observation y are used.

References

- Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical One-Way Functions. *Science* **2002**, *297*, 2026–2030. [[CrossRef](#)] [[PubMed](#)]
- Gassend, B.; Clarke, D.; van Dijk, M.; Devadas, S. Silicon physical random functions. In Proceedings of the 9th ACM Conference on Computer and Communications Security—CCS, Washington, DC, USA, 18–22 November 2002. [[CrossRef](#)]
- Holcomb, D.E.; Burleson, W.P.; Fu, K. Power-Up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Trans. Comput.* **2009**, *58*, 1198–1210. [[CrossRef](#)]
- Guajardo, J.; Kumar, S.S.; Schrijen, G.J.; Tuyls, P. FPGA Intrinsic PUFs and Their Use for IP Protection. In *Cryptographic Hardware Embedded System—CHES*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 63–80.
- van den Berg, R.; Škorić, B.; van der Leest, V. Bias-based modeling and entropy analysis of PUFs. In Proceedings of the 3rd Int. Workshop Trustworthy Embedded Devices—TrustED, Berlin, Germany, 4 November 2013; pp. 13–20. [[CrossRef](#)]
- Juels, A.; Wattenberg, M. A fuzzy commitment scheme. In Proceedings of the 6th ACM Conference on Computer and Communications Security—CCS, Singapore, 1–4 November 1999; pp. 28–36. [[CrossRef](#)]
- Maes, R.; Tuyls, P.; Verbauwhede, I. A soft decision helper data algorithm for SRAM PUFs. In Proceedings of the 2009 IEEE International Symposium on Information Theory, Seoul, Korea, 28 June–3 July 2009; pp. 2101–2105. [[CrossRef](#)]
- Maes, R.; Tuyls, P.; Verbauwhede, I. Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs. In *Cryptographic Hardware and Embedded System—CHES*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 332–347. [[CrossRef](#)]
- Yu, M.D.; Devadas, S. Secure and robust error correction for physical unclonable functions. *IEEE Des. Test Comput.* **2010**, *27*, 48–65. [[CrossRef](#)]
- Hiller, M.; Merli, D.; Stumpf, F.; Sigl, G. Complementary IBS: Application specific error correction for PUFs. In Proceedings of the 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, San Francisco, CA, USA, 3–4 June 2012; pp. 1–6. [[CrossRef](#)]
- Hiller, M.; Yu, M.D.M.; Sigl, G. Cherry-Picking Reliable PUF Bits with Differential Sequence Coding. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2065–2076. [[CrossRef](#)]
- Gao, Y.; Su, Y.; Xu, L.; Ranasinghe, D.C. Lightweight (Reverse) Fuzzy Extractor With Multiple Reference PUF Responses. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1887–1901. [[CrossRef](#)]
- Günlü, O.; Kramer, G. Privacy, Secrecy, and Storage with Multiple Noisy Measurements of Identifiers. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2872–2883. [[CrossRef](#)]
- Günlü, O. Multi-Entity and Multi-Enrollment Key Agreement With Correlated Noise. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1190–1202. [[CrossRef](#)]
- Kusters, L.; Willems, F.M.J. Secret-Key Capacity Regions for Multiple Enrollments With an SRAM-PUF. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2276–2287. [[CrossRef](#)]
- Boyer, X. Reusable cryptographic fuzzy extractors. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 82–91.

17. Kusters, L.; Ignatenko, T.; Willems, F.M.J.; Maes, R.; van der Sluis, E.; Selimis, G. Security of helper data schemes for SRAM-PUF in multiple enrollment scenarios. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 1803–1807. [\[CrossRef\]](#)
18. Van Herrewege, A.; Katzenbeisser, S.; Maes, R.; Peeters, R.; Sadeghi, A.R.; Verbauwhede, I.; Wachsmann, C. Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kralendijk, Bonaire, 27 February–2 March 2012; Volume 7397 LNCS, pp. 374–389. [\[CrossRef\]](#)
19. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; Wiley-Interscience: Hoboken, NJ, USA, 2006.
20. El Gamal, A.; Kim, Y.H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011. [\[CrossRef\]](#)
21. Katzenbeisser, S.; Kocabaş, Ü.; Rožić, V.; Sadeghi, A.R.; Verbauwhede, I.; Wachsmann, C. PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Leuven, Belgium, 9–12 September 2012; pp. 283–301.
22. Maes, R. An Accurate Probabilistic Reliability Model for Silicon PUFs. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems, Santa Barbara, CA, USA, 19–22 August 2015; pp. 73–89. [\[CrossRef\]](#)
23. Kusters, L.; Rikos, A.; Willems, F.M.J. Modeling Temperature Behavior in the Helper Data for Secret-Key Binding with SRAM PUFs. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020.
24. Ahlswede, R.; Csiszàr, I. Common Randomness in Information Theory & Cryptography. *IEEE Trans. Inf. Theory* **1993**, *39*, 1121–1132.
25. Maurer, U.M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [\[CrossRef\]](#)
26. Hui, D.; Sandberg, S.; Blankenship, Y.; Andersson, M.; Grosjean, L. Channel Coding in 5G New Radio: A Tutorial Overview and Performance Comparison with 4G LTE. *IEEE Veh. Technol. Mag.* **2018**, *13*, 60–69. [\[CrossRef\]](#)
27. *MATLAB and 5G Toolbox Release*; The MathWorks, Inc.: Natick, MA, USA, 2020.