Zero secrecy leakage for multiple enrollments of physical unclonable functions

Zero Secrecy Leakage for Multiple Enrollments of Physical Unclonable Functions

Lieneke Kusters* c.j.kusters@tue.nl
Onur Günlü** onur.gunlu@tum.de
Frans M.J. Willems* f.m.j.willems@tue.nl

*Eindhoven University of Technology
Eindhoven, The Netherlands

**Technical University of Munich
Munich, Germany

Abstract

We use physical unclonable functions (PUFs) to generate secret keys. We analyze the performance of the helper data scheme when the enrollment process is repeated multiple times. We show that codes exist such that the scheme remains secure after two enrollments, when all PUF observations are performed over the same channel. Furthermore, we show that a fuzzy commitment scheme remains secure after any number of enrollments, for PUF sources that meet a certain symmetry condition. We show that the temperature dependent model for SRAM-PUF meets this symmetry condition. Furthermore, we argue that many source-channel model pairs exist that meet the symmetry condition, and give some examples. *

1 Introduction

Sensitive data are protected by using secret keys. We use physical unclonable functions (PUFs) to construct such secret keys. A PUF corresponds to a response of a physical device to a challenge. This response is device-specific, reliable, and unpredictable. An attacker may try to guess the key, however, he does not have access to the PUF response. We use the PUF response to generate a random key that is unpredictable for the attacker. Furthermore, we reconstruct the same key at any time by using another response of the same PUF. Two responses of the same PUF device are similar, but not exactly the same due to noise. Therefore, we use an error-correcting code and a helper data scheme to ensure that exactly the same key can be reproduced from a noisy response of the same PUF; see Fig. 1 for a helper data scheme.

1.1 Helper Data Scheme

In a helper data scheme, as depicted in Fig. 1, we distinguish two phases: an enrollment and a reconstruction phase. During the enrollment phase, a key s is generated

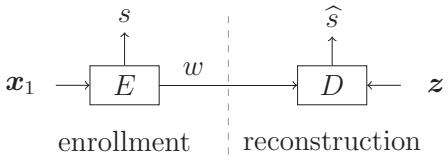

Figure 1: Helper data scheme.

*This work was funded by Eurostars-2 joint programme with co-funding from the EU Horizon 2020 programme under the E! 11897 RESCURE project.

for the first time, based on a response $\boldsymbol{x}$ of the PUF. In addition to the key, a helper message w is generated. The helper message w provides sufficient information to reconstruct the same key s from another response $\boldsymbol{z} \approx \boldsymbol{x}$ of the same PUF during the reconstruction phase. An attacker cannot observe the PUF responses $\boldsymbol{x}$ and $\boldsymbol{z}$, but the helper message is communicated over a public channel, and it may be observed by the attacker. Therefore, the helper message w should not reveal information about the s to an attacker.

The code used in the helper data scheme produces a secret $s \in \mathcal{S} = \{1, 2, \ldots, |\mathcal{S}|\}$ and a helper message w, based on a PUF response $\boldsymbol{x}$ of length $n > 0$, such that the following conditions are satisfied

$$\Pr(\widehat{S} \neq S) \leq \delta, \tag{1}$$

$$\frac{1}{n} H(S) + \delta \geq \frac{1}{n} \log_2 |\mathcal{S}| \geq R_s - \delta, \tag{2}$$

$$\frac{1}{n} I(W; S) \leq \delta \tag{3}$$

for a $\delta > 0$ and n large enough. Here, R_s is an achievable secret-key rate, and the maximum achievable secret-key rate, i.e., secret-key capacity, is known to be $C_s = I(\boldsymbol{X}_1; \boldsymbol{Z})$ [1, 2].

1.2 Literature Review and Main Contributions

In the key agreement literature, only a single enrollment is assumed to be performed for each PUF device. We are interested in a situation that the enrollment procedure is repeated multiple times. This may happen in practice, when, for example, the key is replaced with a new one or the overlying protocol that includes the first enrollment is repeated for some reason. Note that the generated keys will not (necessarily) be independent. We assume that during each PUF enrollment, the previous key is replaced with a new key and a corresponding helper message is published. The decoder uses the most recent helper message to reconstruct the corresponding key. The previous helper messages may all be used by an attacker to derive information about the key.

We have discussed multiple enrollment of an SRAM-PUF with the fuzzy commitment scheme [3] in [4], and showed that for a given model of the SRAM-PUF, the fuzzy commitment scheme remained secure, i.e., (3) is satisfied, also when the multiple enrollments were performed. We extended the proof to the syndrome method in [5].

In the current work, we generalize our results. We show that in the case of two enrollments when all PUF measurements are done via the same channel, there exists a code that satisfies (1)-(3) and achieves the secret-key capacity. Furthermore, we show that the fuzzy commitment scheme remains secure for any number of enrollments given that the PUF response meets a certain symmetry condition. Finally, we extend the model that we used in [4, 5] to a temperature-dependent SRAM-PUF model, similar to ring oscillator PUF models we had in [6], and show that it meets the symmetry condition.

1.3 Notation and PUF Response Assumptions

We use upper case letters to denote random variables and lower case letters to denote their realizations. The symbol $\boldsymbol{x}$ refers to a PUF response used for enrollment and $\boldsymbol{z}$ a PUF response used for reconstruction. We use different symbols to make it easier to follow our reasoning in equations; however, the statistical properties of both responses are the same. Assume that the PUF responses are binary vectors of length n; thus, $\boldsymbol{x} \in \{0, 1\}^n$ and $\boldsymbol{z} \in \{0, 1\}^n$. Furthermore, suppose the values in the vector are independent

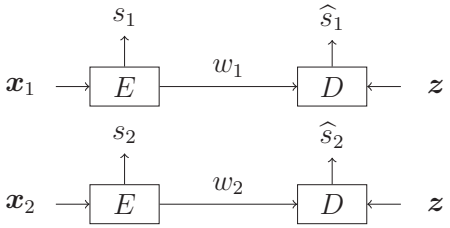

Figure 2: Two enrollments scheme.

identically distributed (i.i.d.), i.e. $\Pr(\boldsymbol{X} = \boldsymbol{x}) = \prod_{i=1}^{n} \Pr(X(i) = x(i))$. Assume that multiple responses $(\boldsymbol{x}_1, \boldsymbol{x}_2, \dots)$ are observed, and the probability distributions are time and permutation invariant, e.g., $\Pr(\boldsymbol{X}_1 = \boldsymbol{x}_1, \boldsymbol{X}_2 = \boldsymbol{x}_2) = \Pr(\boldsymbol{X}_1 = \boldsymbol{x}_2, \boldsymbol{X}_2 = \boldsymbol{x}_1)$. The function $H(X)$ is the entropy function for a random variable. It follows from our assumptions above that

$$H(\boldsymbol{X}_j) = H(\boldsymbol{Z}) = nH(X_1) \qquad \forall j \in \{1, 2, \dots\}, \tag{4}$$

$$H(\boldsymbol{X}_i \boldsymbol{X}_j) = nH(X_1 X_2) \qquad i \neq j,\ \forall i, j \in \{1, 2, \dots\}, \tag{5}$$

$$H(\boldsymbol{X}_i \boldsymbol{X}_j \boldsymbol{X}_k) = nH(X_1 X_2 X_3) \qquad i \neq j \neq k,\ \forall i, j, k \in \{1, 2, \dots\}. \tag{6}$$

2 Multiple Enrollments

We are interested in the scenario where multiple keys and helper messages are generated independently from different measurements of the same PUF. As an example, we show a two-enrollment scenario in Fig. 2. During each enrollment $j \in \{1, 2\}$, a key s_j and corresponding helper message w_j are generated based on an observation $\boldsymbol{x}_j$ of the PUF. The helper message w_j should contain sufficient information such that a decoder can reconstruct the secret s_j when an additional observation $\boldsymbol{z}$ of the PUF is available. An attacker given all helper messages $(w_1, w_2, \dots)$; however, should not learn any information about any of the secrets s_j. We assume that the same code is used by all encoders and decoders. It is required that each key is uniformly distributed. Note that it is not required that the keys are independent. It is straightforward to show that secrecy is leaked about all secret keys when a single key is compromised.

Each encoder generates a key $s_j \in \mathcal{S} = \{1, 2, \dots, |\mathcal{S}|\}$, and a corresponding helper message $w_j \in \mathcal{W} = \{1, 2, \dots, |\mathcal{W}|\}$ by using the same code. We are interested in finding codes that achieve the following conditions for $l \geq 1$ enrollments:

$$\Pr(\widehat{S}_1 \neq S_1 \cup \widehat{S}_2 \neq S_2 \cup \dots \cup \widehat{S}_l \neq S_l) \leq \delta, \tag{7}$$

$$\frac{1}{n} H(S_t) + \delta \geq \frac{1}{n} \log_2 |\mathcal{S}| \geq R_s - \delta \qquad \forall t \in \{1, 2, \dots, l\}, \tag{8}$$

$$\frac{1}{n} I(W_1 W_2 \dots W_l; S_t) \leq \delta \qquad \forall t \in \{1, 2, \dots, l\} \tag{9}$$

for a $\delta > 0$ and n large enough. Here, R_s is an achievable secret-key rate, and we are interested in finding the set of achievable secret-key rates that satisfies (7)-(9) for any number of enrollments.

We can find a straightforward upper bound on the achievable rates. Since any enrollment follows exactly the same procedure and is also based on a response with the same statistical properties as the first enrollment, it should be clear that we cannot achieve a higher rate than the rate achieved for a single enrollment. We prove this upper bound in Appendix A.

2.1 Two Enrollments

For the two enrollments scenario shown in Fig. 2, we have the following result.

Theorem 1. *The secret-key capacity for each secret key in a two-enrollment setup defined above is $I(X_1;Z) = I(X_2;Z)$, which is equal to the secret-key capacity for a single enrollment setup.*

Proof. First, we define a random labeling $G : \{0,1\}^n \to (\mathcal{S}, \mathcal{W})$, with $\mathcal{S} = \{1, 2, \ldots, 2^{nR_S}\}$ and $\mathcal{W} = \{1, 2, \ldots, 2^{nR_W}\}$. An encoder uses the labeling G to map an observation vector $\boldsymbol{x}$ to a corresponding secret key and helper message pair (s, w). We distinguish two types of decoders: a regular decoder and a virtual decoder. The regular decoder performs the reconstruction of the secret on the decoding side of the helper data scheme. The virtual decoder is an imaginary decoder which we define to help us prove that the uniformity and leakage conditions are satisfied. Both decoders are based on joint typicality decoding, where we define the set of weakly typical sequences $\mathcal{A}_\epsilon^n(X)$ with respect to P_X as in [7].

The regular decoder reconstructs an observation vector $\boldsymbol{x}_i$ by using his observation $\boldsymbol{z}$ and the helper message w_i. That is, it decodes $\widehat{\boldsymbol{x}}_i$ when the labeling $G(\widehat{\boldsymbol{x}}_i) = (*, w_i)$, where $*$ corresponds to any value that is in $\mathcal{S}$, and $(\widehat{\boldsymbol{x}}_i, \boldsymbol{z}) \in \mathcal{A}_\epsilon^n(X_i Z)$. When the decoder has successfully decoded $\boldsymbol{x}$, it can also reconstruct the secret s by using the labeling G.

The virtual decoder decodes both observations $(\boldsymbol{x}_1, \boldsymbol{x}_2)$ from all helper messages (w_1, w_2) and one of the secrets s_i. First, it decodes $\widetilde{\boldsymbol{x}}_i$, such that the labeling $G(\widetilde{\boldsymbol{x}}_i) = (s_i, w_i)$, and $(\widetilde{\boldsymbol{x}}_i) \in \mathcal{A}_\epsilon^n(X_i)$. Then, it can decode the other observation $\boldsymbol{x}_j$, using the corresponding helper message w_j and the already decoded observation $\boldsymbol{x}_i$, with joint typicality decoding, as with the regular decoder. That is, it decodes $\widetilde{\boldsymbol{x}}_j$ when the labeling $G(\widetilde{\boldsymbol{x}}_j) = (*, w_j)$, and $(\boldsymbol{x}_i, \widetilde{\boldsymbol{x}}_j) \in \mathcal{A}_\epsilon^n(X_1 X_2)$.

Choosing $R_W = H(X_1|Z)$ and $R_W + R_S = H(X_1)$, it follows from the Slepian-Wolf Theorem, see, e.g., [7], that error-probabilities can be made arbitrarily small for both decoders by increasing n. Therefore, a code exists such that $R_S = I(X_1;Z) = H(X_1) - H(X_1|Z)$ and $R_W = H(X_1|Z)$ and both the regular and virtual decoders are successful with high probability. We say that the probability of error by the decoders is at most ϵ_n when a code of length n is used.

Given that there exists such a code, we can find an upper bound on the entropy of the helper messages and the secrets as $H(W_t) \leq nR_W = nH(X_1|Z)$ and $H(S_t) \leq nR_S = nI(X_1;Z)$. Now, the secrecy leakage about the secret key s_t via the two helper messages is:

$$\begin{aligned}
&I(S_t; W_1 W_2) = H(S_t) + H(W_1 W_2) - H(S_t W_1 W_2) \\
&\leq n(I(X_1;Z) + 2H(X_1|Z)) - H(S_t W_1 W_2 \boldsymbol{X}_1 \boldsymbol{X}_2) + H(\boldsymbol{X}_1 \boldsymbol{X}_2 | W_1 W_2 S_t) \\
&\overset{(a)}{\leq} n(H(X_1) - H(X_1|Z) + H(X_1|Z) + H(X_2|Z) - H(X_1 X_2)) + 1 + 2n\epsilon_n \\
&\overset{(b)}{=} 1 + 2n\epsilon_n
\end{aligned} \tag{10}$$

where (a) follows from Fano's inequality for the virtual decoder, i.e. $H(\boldsymbol{X}_1 \boldsymbol{X}_2 | W_1 W_2 S_t) \leq 1 + 2n\epsilon_n$ with error probability $\epsilon_n > 0$ and (b) follows because $P_{X_1 X_2} = P_{X_2 Z}$ for the measurement model we consider. Thus, the security condition in (9) is satisfied.

Finally we obtain from Fano's inequality for the virtual decoder that

$$\begin{aligned}
nH(X_t) &= H(\boldsymbol{X}_t) = H(\boldsymbol{X}_t W_t S_t) \\
&\leq H(S_t) + H(W_t) + H(\boldsymbol{X}_t | W_t S_t) \\
&\leq H(S_t) + nH(X_1|Z) + 1 + n\epsilon_n
\end{aligned} \tag{11}$$

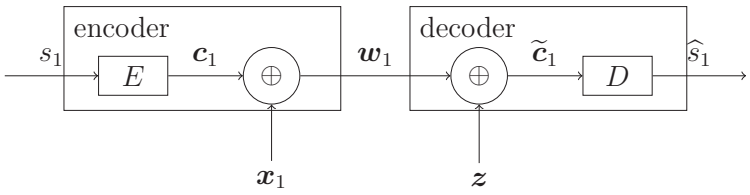

Figure 3: Fuzzy commitment scheme.

and thus $\frac{1}{n}H(S_t) \geq I(X_1;Z) - \epsilon_n - \frac{1}{n}$. Therefore, for any $\delta > 0$ we obtain that $\frac{1}{n}H(S_t) + \delta \geq I(X_1;Z) = \frac{1}{n}\log_2|\mathcal{S}| \geq R_S - \delta = I(X_1;Z) - \delta$, for a large enough n and an ϵ_n that tends to zero as $n \to \infty$. Thus, the uniformity condition for the secret keys holds.

We conclude that a code exists such that all conditions for the two enrollment scenario are met and that achieves secret-key rates

$$R_S = I(X_1;Z) = I(X_2;Z). \tag{12}$$

□

3 Zero Secrecy Leakage for Symmetric PUFs

In the following, we show that zero secrecy leakage occurs for any number of enrollments, when a linear code is used in the fuzzy commitment scheme and the PUF source has a certain type of symmetry.

3.1 Fuzzy Commitment Scheme

First, we introduce the fuzzy commitment scheme for secret-key binding, see Fig. 3. On the encoder side, a secret-key is encoded into a binary codeword that is bound to the PUF output. The helper message $\boldsymbol{w}_1$ is the modulo-2 sum of the codeword $\boldsymbol{c}_1$ and the PUF output $\boldsymbol{x}_1$. A decoder can now reconstruct a noisy version of the codeword $\widetilde{\boldsymbol{c}}_1 = \boldsymbol{w}_1 \oplus \boldsymbol{z} = \boldsymbol{c}_1 \oplus (\boldsymbol{x}_1 \oplus \boldsymbol{z})$ by summing his observation of the PUF and the received helper message modulo-2. As long as there are not too many errors between the two observations $\boldsymbol{x}_1$, and $\boldsymbol{z}$, the decoder can reconstruct the secret from $\widetilde{\boldsymbol{c}}_1$. This procedure is repeated for each PUF enrollment. Furthermore, we use a linear code $E : \{0,1\}^n \to \mathcal{C}$ to encode each secret into a binary codeword as $E(s) = \boldsymbol{c}$. Since the code is linear, it follows that the modulo-2 sum of two codewords is also a codeword $(\boldsymbol{c} \oplus \boldsymbol{c}') \in \mathcal{C}$.

3.2 Symmetry Property for Zero Secrecy Leakage

We list our results from [5] that show that the fuzzy commitment scheme does not leak any information about the secret key, when the PUF observations have the following symmetry property for all $x_1, x_2, \ldots$:

$$\Pr(X_1 = x_1, X_2 = x_2, \ldots) = \Pr(X_1 = \overline{x_1}, X_2 = \overline{x_2}, \ldots) \tag{13}$$

where $\bar{x}$ is the one's complement of x. Firstly, we have

$$\begin{aligned}\Pr(\boldsymbol{X}_1 = \boldsymbol{x}_1, \boldsymbol{X}_2 = \boldsymbol{x}_2, \ldots) &= \Pr(\boldsymbol{X}_1 = \overline{\boldsymbol{x}_1}, X_2 = \overline{\boldsymbol{x}_2}, \ldots) \\ &= \Pr(\boldsymbol{X}_1 = \boldsymbol{x}_1 \oplus \boldsymbol{x}_j, \boldsymbol{X}_2 = \boldsymbol{x}_2 \oplus \boldsymbol{x}_j, \ldots)\end{aligned} \tag{14}$$

where $\boldsymbol{x}_j$ is an observed vector. Then, we can derive that the probability distribution for any set of generated helper messages and given the l^{th} secret s_l and its corresponding codeword $\boldsymbol{c}_l$,

$$\begin{aligned}
&\Pr(\boldsymbol{W}_1 = \boldsymbol{w}_1, \ldots, \boldsymbol{W}_l = \boldsymbol{w}_l | \boldsymbol{C}_l = \boldsymbol{c}_l) \\
&= \sum_{\boldsymbol{c}_1 \in \mathcal{C}} \cdots \sum_{\boldsymbol{c}_{l-1} \in \mathcal{C}} \Pr(\boldsymbol{X}_1 = \boldsymbol{w}_1 \oplus \boldsymbol{c}_1, \ldots, \boldsymbol{X}_l = \boldsymbol{w}_l \oplus \boldsymbol{c}_l) \\
&\overset{(a)}{=} \sum_{\boldsymbol{c}'_1 \in \mathcal{C}} \cdots \sum_{\boldsymbol{c}'_{l-1} \in \mathcal{C}} \Pr(\boldsymbol{X}_1 = \boldsymbol{w}_1 \oplus \boldsymbol{c}'_1, \ldots, \boldsymbol{X}_l = \boldsymbol{w}_l \oplus \boldsymbol{0}) \\
&\overset{(b)}{=} \Pr(\boldsymbol{W}_1 = \boldsymbol{w}_1, \ldots, \boldsymbol{W}_l = \boldsymbol{w}_l), \qquad (15)
\end{aligned}$$

where (a) follows from the linearity of the code, and (b) follows because there is no longer a dependency on the value of c_l. The above derivation can be repeated for any of the secrets s_j, so we have

$$H(\boldsymbol{W}_1, \boldsymbol{W}_2, \ldots, \boldsymbol{W}_l | S_j) = H(\boldsymbol{W}_1, \boldsymbol{W}_2, \ldots, \boldsymbol{W}_l). \qquad (16)$$

We conclude that the leakage about any secret S_j, by all the observation vectors

$$I(\boldsymbol{W}_1, \boldsymbol{W}_2, \ldots, \boldsymbol{W}_l; S_j) = H(\boldsymbol{W}_1, \boldsymbol{W}_2, \ldots, \boldsymbol{W}_l) - H(\boldsymbol{W}_1, \boldsymbol{W}_2, \ldots, \boldsymbol{W}_l | S_j) = 0. \qquad (17)$$

3.3 SRAM-PUF Model Under Varying Ambient Temperature

Suppose the power-on value of an SRAM is used to generate the PUF response used in the fuzzy commitment scheme. We use the statistical model presented in [8] that models the temperature dependent behavior of the SRAM values. Each SRAM cell has two hidden model variables that define the probability that a bit one is observed at an ambient temperature T. The first hidden variable m defines the bias of the cell. The second hidden variable d defines how the one-probability changes with temperature. For an SRAM cell with given hidden variables m and d, the j^{th} observation at temperature $T^{(j)}$ is modeled as

$$r^{(j)}(T^{(j)}) = \begin{cases} 0 & \text{if } m + n^{(j)} + d \cdot T^{(j)} \leq \tau, \\ 1 & \text{if } m + n^{(j)} + d \cdot T^{(j)} > \tau \end{cases} \qquad (18)$$

where $n^{(j)}$ represents the realization of noise sampled in each measurement according to a Gaussian distribution $\mathcal{N}(0, 1)$. The probability that a one is observed at temperature T for this cell, is given by $Q(-m - d \cdot T + \tau)$, where $Q(\cdot)$ is the Q-function. The hidden variables m and d are assumed to be unknown. These cell properties are a result of random variations in the production process and are modeled as independent samples of the random variables, respectively, $M \sim \mathcal{N}(\mu_M, \sigma_M)$ and $D \sim \mathcal{N}(0, \sigma_D)$ for each SRAM cell. Therefore, for a cell with unknown values for the hidden variables, the one-probability at temperature $T^{(j)}$ is

$$\Pr(R^{(j)} = 1) = \int \int Q(-m - d \cdot T^{(j)} + \tau) p_M(m) p_D(d) \, \mathrm{d}m \, \mathrm{d}d. \qquad (19)$$

Assume that the SRAM cells are unbiased (i.e., on average the probability that a one is observed for any SRAM cell, is equal to the probability that a zero is observed),

so $\mu_M = \tau$. For l observations of an SRAM cell, at various *given* temperatures $T^l = (T^{(1)}, T^{(2)}, \ldots, T^{(l)})$, we have

$$\begin{aligned}
&\Pr(R^l = r^l) \\
&= \int\int \prod_{j=1}^{l} Q(-m - d\cdot T^{(j)})^{r^{(j)}} Q(m + d\cdot T^{(j)})^{\overline{r^{(j)}}} p_M(m) p_D(d)\ \mathrm{d}m\ \mathrm{d}d \\
&= \int\int \prod_{j=1}^{l} Q(m + d\cdot T^{(j)})^{r^{(j)}} Q(-m - d\cdot T^{(j)})^{\overline{r^{(j)}}} p_M(-m) p_D(-d)\ \mathrm{d}m\ \mathrm{d}d \\
&\overset{(a)}{=} \int\int \prod_{j=1}^{l} Q(-m - d\cdot T^{(j)})^{\overline{r^{(j)}}} Q(m + d\cdot T^{(j)})^{r^{(j)}} p_M(m) p_D(d)\ \mathrm{d}m\ \mathrm{d}d \\
&= \Pr(R^l = \overline{r^l}) \qquad (20)
\end{aligned}$$

where (a) follows from the symmetry properties $p_M(m) = p_M(-m)$ and $p_D(d) = p_D(-d)$.

Since the hidden model variables are i.i.d. over all SRAM cells, we have for observation vectors $\boldsymbol{r}^l = (r_1^l, r_2^l, \ldots, r_n^l)$ corresponding to l observations of n SRAM cells at temperatures T^l that

$$\begin{aligned}
\Pr(\boldsymbol{R}^l = \boldsymbol{r}^l) &= \Pr\left((R_1^l, R_2^l, \ldots, R_n^l) = (r_1^l, r_2^l, \ldots, r_n^l)\right) \\
&\overset{(a)}{=} \prod_{i=1}^{n} \Pr(R_i^l = r_i^l) \overset{(b)}{=} \prod_{i=1}^{n} \Pr(R_i^l = \overline{r_i^l}) \\
&= \Pr(\boldsymbol{R}^l = \overline{\boldsymbol{r}^l}) \qquad (21)
\end{aligned}$$

where (a) follows from independence of the SRAM cells, and (b) follows by (20). Therefore, we conclude that the temperature dependent SRAM-PUF model given in [8] meets the symmetry condition in (13) that results in zero secrecy leakage when the fuzzy commitment scheme is used.

3.4 Other PUF Models with the Symmetry Property

We remark that a PUF response $\boldsymbol{x}$ is a noisy observation of a hidden source through a measurement channel. We can show that there is a big set of source-channel model pairs that satisfy the symmetry property in (13) in addition to the SRAM-PUF model under varying temperature conditions, as discussed in Section 3.3. For instance, any binary-input symmetric memoryless measurement channel (see, e.g., [9] for its definition) such as dependent binary symmetric PUF measurement channels [10] satisfies this equality if the hidden source is symmetric.

We also give an example source-channel model pair where both the source and channel are asymmetric but the outputs are symmetric to further illustrate that the symmetry property in (13) is not limited to a small set of models. Consider an asymmetric hidden source with one-probability $\Pr(Y = 1) = 4/5$, and an asymmetric measurement channel that is given by the Z-channel with parameter $z = 3/8$, see Fig. 4. Now single channel observations are symmetric, that is $\Pr(X = 1) = \Pr(X = 0) = 1/2$. Furthermore, for two observations $P_{X_1X_2}(11) = P_{X_1X_2}(00) = 5/16$ and $P_{X_1X_2}(01) = P_{X_1X_2}(10) = 3/16$. Therefore, the symmetry condition (13) is satisfied, which is a sufficient condition for zero secrecy leakage for two enrollments with the fuzzy commitment scheme. Also note that for this source-channel model, the secret-key capacity for each key is approximately $R_s = 0.0456$ bits/source-bit.

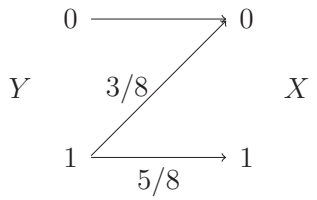

Figure 4: Z-channel with $z = 3/8$.

4 Conclusion

We have studied security of the helper data scheme in case of multiple enrollments. We proved that codes exist for any PUF source that is time and permutation invariant, such that the key remains secure when enrollment is repeated for a second time. Furthermore, we have shown that the fuzzy commitment scheme remains secure for any number of repeated enrollments when the PUF source meets a symmetry condition. The temperature-dependent model for SRAM-PUF meets the symmetry condition. We argued that many source-channel models exist that meet the symmetry condition and have shown examples.

Appendix A. Proof of Converse for Theorem 1

We show that for any number of enrollments, the secret-key rate cannot exceed $I(X_1; Z)$ for each secret key generated for the two-enrollment case. First, we have

$$\begin{aligned} H(S_t|\boldsymbol{Z}W_t) &= H(S_t|\boldsymbol{Z}W_t\widehat{S}_t) \\ &\leq H(S_t|\widehat{S}_t) \\ &\leq 1 + P_e \log_2 |\mathcal{S}_t| \leq 1 + \delta n \end{aligned} \tag{22}$$

where $P_e = \Pr(\widehat{S}_t \neq S_t) \leq \delta$ with $\delta > 0$. Then, the entropy of the key is

$$\begin{aligned} H(S_t) &= I(S_t; \boldsymbol{Z}W_t) + H(S_t|\boldsymbol{Z}W_t) \\ &\leq I(S_t; W_t) + I(S_t; \boldsymbol{Z}|W_t) + 1 + n\delta \\ &\leq H(\boldsymbol{Z}) - H(\boldsymbol{Z}|W_t S_t \boldsymbol{X}_t) + 1 + 2n\delta \\ &= nI(X_t; Z) + 1 + 2n\delta. \end{aligned} \tag{23}$$

This results in

$$R_t - \delta \leq \frac{1}{n} H(S_t) + \delta \leq I(X_t; Z) + \frac{1}{n} + 2\delta. \tag{24}$$

Now with $n \to \infty$ and $\delta \downarrow 0$ we obtain the proof of converse.

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 2733–742, May 1993.

[3] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM Conf. Comp. Commun. Security*, New York, NY, Nov. 1999, pp. 28–36.

[4] L. Kusters, T. Ignatenko, and F. M. J. Willems, "Zero-leakage multiple key-binding scenarios for SRAM-PUF systems based on the XOR-method," in *6th Joint WIC/IEEE Symp. on Inf. Theory and Signal Proc. in the Benelux, May 19-20, 2016, Louvain, Belgium*, 2016, pp. 120–127.

[5] L. Kusters, T. Ignatenko, F. M. J. Willems, R. Maes, E. van der Sluis, and G. Selimis, "Security of helper data schemes for SRAM-PUF in multiple enrollment scenarios," in *2017 IEEE International Symposium on Information Theory (ISIT)*, June 2017, pp. 1803–1807.

[6] O. Günlü, O. İşcan, and G. Kramer, "Reliable secret key generation from physical unclonable functions under varying environmental conditions," in *IEEE Int. Workshop Inf. Forensics Security*, Rome, Italy, Nov. 2015, pp. 1–6.

[7] T. M. Cover and J. A. Thomas, *Elements of information theory*, 2nd ed. John Wiley & Sons, 2006.

[8] R. Maes, "An Accurate Probabilistic Reliability Model for Silicon PUFs," in *Cryptogr. Hardw. Embed. Systems - CHES 2013 15th Int. Work. St. Barbar. CA, USA*, 2013, pp. 73–89.

[9] N. Chayat and S. Shamai, "Extension of an entropy property for binary input memoryless symmetric channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 5, pp. 1077–1079, Sep. 1989.

[10] O. Günlü and G. Kramer, "Privacy, secrecy, and storage with multiple noisy measurements of identifiers," *IEEE Trans. Inf. Forensics and Security*, 2018, to appear.