Capacity of a dual enrollment system with two keys based on an SRAM-PUF

Citation for published version (APA):

DOI:
10.3929/ethz-b-000245066

Document status and date:
Published: 01/01/2018

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.
Capacity of a Dual Enrollment System with Two Keys Based on an SRAM-PUF

Lieneke Kusters and Frans M.J. Willems
Eindhoven University of Technology, Eindhoven, The Netherlands. Contact: c.j.kusters@tue.nl

Abstract—We investigate the capacity of an SRAM-PUF based secrecy system that produces two secret keys during two consecutive enrollments. We determined the region of secret-key rates that are achievable and show that the total secret-key capacity is larger than for a single enrollment system. In our achievability proofs we focussed on linear codes.

I. INTRODUCTION

An SRAM-PUF has a binary response that is unpredictable but reliable, and that is unique to the specific SRAM. Therefore, SRAM-PUF observation vectors are considered as a digital fingerprint, and may be used to generate and reconstruct secret keys [1]. Such secret keys can be used to authenticate a device or to secure data. It is important that the secret key is hard to guess by an attacker, and at the same time perfectly reconstructible by the user who can observe the SRAM-PUF.

The problem of (re-)generating a secret key from SRAM-PUF observations can be directly mapped to the problem of secret-key agreement [2]. In this case, an encoder and a decoder observe dependent sequences with some known joint distribution and need to agree on a secret key. It is known that the maximum achievable secret-key rate for this scenario is equal to the mutual information between the observed random variables by the encoder and decoder respectively [3], [4]. This rate can be achieved by one-way communication between the encoder and the decoder. The encoder generates a secret key and corresponding helper message, based on its input. We refer to this process as enrollment. The helper message is send over a public channel to the decoder. The decoder uses the helper message and his own observation to reconstruct the same key.

Clearly, the mutual information and thus the achievable secret-key rate may increase when more observations are considered. However, can we also increase the secret-key rate when additional input is observed by the encoder after an enrollment has already been completed? In [5], we have studied the case when enrollment of the same SRAM-PUF is repeated multiple times. The encoder regenerates the secret key and a corresponding helper message after observing an additional input from the SRAM-PUF. We have shown that given certain symmetry properties of the SRAM-PUF no leakage results from the additional helper messages. However, all previous keys are considered invalid and the secret-key rate remains the same. In the current work, we allow the encoder to generate a second key and corresponding helper message after observing an additional response from the SRAM-PUF.

We show that the secret-key rate can be sequentially increased in this case while ensuring no leakage about any of the keys.

In the following, we first introduce the SRAM-PUF model and the notation that is used in the paper. Then, we analyze the 1-enrollment scheme, where a single key and helper message are generated by the encoder. We give the converse and show achievability of the secret-key rates with linear codes for the 1-enrollment scheme. Then, we continue to the 2-enrollment scheme, where a second key and helper message are generated, and we derive the achievable rates for this scheme.

II. NOTATION AND SRAM-PUF STATISTICAL MODEL

We use capitals to refer to random variables and lowercase symbols for realizations of random variables. All vectors in this paper are printed in bold and are binary. The SRAM-PUF observation vector has length $n$ and corresponds to the values of the $n$ cells in an SRAM cell array. We assume that the values of the SRAM-PUF cells are independent of each other and identically distributed. Moreover the observations of an SRAM cell are permutation invariant, hence for three consecutive observations $x$, $y$, and $z$ of an SRAM cell, $p(x,y,z) = p(x,z,y) = \cdots = p(z,y,x)$. This leads to $H(X) = H(Y) = H(Z)$ and $H(X,Y) = H(X,Z) = H(Y,Z)$. We focus here on three subsequent observation vectors $x$, $y$, and $z$, of the same SRAM-PUF. Then e.g. $H(X) = nH(X)$ etc. by the fact that observation vectors are i.i.d. Given that the SRAM-PUF is permutation invariant we obtain

$$H(X) = H(Y) = H(Z),$$
$$H(XY) = H(XZ) = H(YZ).$$

III. 1-ENROLLMENT SETTING

In the 1-enrollment setting shown in Figure 1, an encoder constructs a secret key $k$ and helper message $m$ after observing observation vector $x$. A decoder observing observation vector $z$, should be able to reconstruct $k$ when given helper message $m$. Furthermore, the helper message $m$ should not reveal any information about $k$ to an attacker who can not observe $x$ nor $z$. The secret key assumes values in $\{1, 2, \cdots, |K|\}$ where $|K| \leq 2^n$ since $x \in \{0, 1\}^n$.

Definition 1: A secret-key rate $R$ is called achievable in the 1-enrollment setting, if for all $\delta > 0$ and for all $n$ large enough, there exist encoders and decoders such that

$$\Pr(\tilde{K} \neq K) \leq \delta,$$
A linear coding strategy $S_k$ is specified by the parity-matrices $H_m$ and $H_k$, with dimensions $(nρ_m × n)$ and $(nρ_k × n)$ respectively. The encoder observes a sequence $x$ of length $n$ and generates a helper message $m = H_m x^T$ and secret key $k = H_k x^T$ and sends the helper message over a public channel to the decoder. The secret key is a binary vector of length $nρ_k$, and $|K| = 2^nρ_k$. The decoder observes a sequence $z$ and reconstructs the unique sequence $\hat{x}$ such that $H_m \hat{x}^T = m$ and $(\hat{x}, z) \in A^{(n)}(XZ)$. If the reconstruction of $x$ is successful the decoder can also reconstruct the secret $k = H_k \hat{x}^T$.

Finally, we introduce a virtual decoder that observes both the secret $k$ and the helper message $m$ and reconstructs $x$ such that $H_m x^T = m$ and $H_k \hat{x}^T = k$ and $\hat{x} \in A^{(n)}(X)$.

We measure the reliability of a linear coding strategy $S_n$ in terms of the error probability

$P_e(S_n) = \Pr(\hat{X} \neq X \text{ or } \hat{X} \neq X|S_n)$.\text{.}$

Next we assume that all matrix elements are chosen uniformly from $\{0, 1\}$ and we bound the error probability averaged over all randomly generated linear codes $H_m, H_k$ as $E[P_e(S_n)] \leq \Pr(E_0) + \Pr(E_1) + \Pr(E_2)$, with

$E_0 = \{(X, Z) \notin A^{(n)}(XZ)\}$,

$E_1 = \{\exists \hat{x} \neq X : H_m \hat{x}^T = H_m x^T \text{ and } (\hat{x}, Z) \in A^{(n)}(XZ)\}$,

$E_2 = \{\exists \hat{x} \neq X : H_m \hat{x}^T = H_m x^T \text{ and } H_k \hat{x}^T = H_k X^T \text{ and } \hat{x} \in A^{(n)}(X)\}$.\text{.}$

By the properties of typical sequences $\Pr(E_0) < \epsilon$.

\begin{align*}
\Pr(E_1) &= \sum_{x, \hat{x}, x \neq \hat{x}} \Pr(\exists \hat{x} \neq X : H_m \hat{x}^T = H_m x^T \text{ and } (\hat{x}, Z) \in A^{(n)}(XZ)) \\
&\leq \sum_{x, \hat{x}, \hat{x} \neq x} \sum_{\hat{x} \in A^{(n)}(XZ)} \Pr(H_m(\hat{x} \oplus x)^T = 0) \\
&\leq \sum_{x, \hat{x}} \sum_{\hat{x} \neq x} \Pr(H_m(\hat{x} \oplus x)^T = 0) \\
&\leq 2^n(H(X|Z) + 2\epsilon) 2^{-nρ_m}.
\end{align*}

Note that vector $e = \hat{x} \oplus x$ has at least one non-zero component (since $x \neq \hat{x}$), say at position $j$. Then for a randomly generated $H_m$ of dimension $(nρ_m × n)$

\begin{align*}
\Pr(H_m e^T = 0) &= \Pr\left(\sum_{i=1}^{n} H_m(:, i)e(i) = 0\right) \\
&= \Pr\left(\sum_{i=1,i\neq j}^{n} H_m(:, i)e(i) = H_m(:, j)\right) \\
&= \Pr(H_m(:, j) = e) = 2^{-nρ_m},
\end{align*}

where $H(:, i)$ corresponds to the $i^{th}$ column of the matrix and $e(i)$ corresponds to the value at the $i^{th}$ position of vector $e$ and $e$ corresponds to some column vector. Next

\begin{align*}
\Pr(E_2) &= \sum_{x} \Pr(\exists \hat{x} \neq X : H_m \hat{x}^T = H_m x^T \text{ and } \hat{x} \in A^{(n)}(X)).
\end{align*}
\[ H_{k}(\tilde{x}^{T} = H_{k}x^{T} \text{ and } \tilde{x} \in A_{k}(X)) \leq \sum_{x} p(x) \sum_{\tilde{x} \in A_{k}(X), \tilde{x} \neq x} \Pr(H_{m}(\tilde{x} \oplus x)^{T} = 0, H_{k}(\tilde{x} \oplus x)^{T} = 0) \leq \sum_{x} p(x)|A_{k}(X)|2^{-n(\rho_{m} + \rho_{k})} \leq 2^{n(H(X)+\epsilon)}2^{-n(\rho_{m} + \rho_{k})}. \]

We conclude that \( E[P_{e}(S_{n})] \leq 3e \) as long as

\[ \rho_{m} > H(X|Z) + 2\epsilon, \]

\[ \rho_{m} + \rho_{k} > H(X) + \epsilon. \]

From this it follows that linear codes exist with \( \rho_{m} = H(X|Z) + 3e \) and \( \rho_{k} = I(X;Z) - \epsilon \), such that decoding (both for the helper message decoder and the virtual decoder) has an acceptable error probability, as long as \( n \) is large enough.

C. Leakage, Uniformity of the keys, and Rate

Now, we investigate for the linear codes found before, having dimensions \( n\rho_{m} \) and \( n\rho_{k} \), the resulting leakage about secret \( K \) from syndrome \( m \).

\[ I(K;M) = H(K) + H(M) - H(MK) \leq H(K) + H(M) - H(XMK) + H(X|MK) \leq nI(X;Z) - ne + n(H(X|Z) + 3e) - nH(X) + 1 + nE[P_{e}(S_{n})] \leq 2ne + 1 + nE[P_{e}(S_{n})] \leq 5ne + 1, \]

thus for \( n \) large enough and some appropriate choice for \( \epsilon \) we conclude that \( \frac{1}{n}I(K;M) \leq \delta \) for any \( \delta > 0 \), and the leakage requirement is satisfied.

Next we find that

\[ H(X) = H(XMK) \leq H(K) + H(M) + H(X|MK) \leq H(K) + n(H(X|Z) + 3e) + 1 + nE[P_{e}(S_{n})], \]

\[ \frac{1}{n}H(K) \geq I(X;Z) - 6e - \frac{1}{n}. \]

Therefore, for any \( \delta > 0 \) we obtain that \( \frac{1}{n}H(K) + \delta \geq I(X;Z) - \epsilon = \frac{1}{n} \log_{2}|K| \geq R - \delta = I(X;Z) - \delta \) by suitable choice of \( \epsilon \) and large enough \( n \). Now the uniformity/rate condition of Definition 1 is satisfied. It follows that rate \( R = I(X;Z) \) is achievable, and that the secret-key capacity is \( I(X;Z) \). This concludes the proof.

IV. 2-enrollment setting

In the 2-enrollment setting shown in Figure 2, we assume that a first enrollment is performed by encoder 1. A secret key \( k_{1} \) and helper message \( m_{1} \) are generated based on observation of \( x \). A decoder that observes \( z \) and \( m_{1} \) has sufficient information to form an estimate \( \hat{k}_{1} \) of secret \( k_{1} \).

Encoder 2 observes observation vector \( y \) and performs a second enrollment, generating a secret key \( k_{2} \) and corresponding helper message \( m_{2} \). A decoder that observes both helper messages \( m_{1} \) and \( m_{2} \), and an observation vector \( z \) should be able to form the estimate \( \hat{k}_{1}\hat{k}_{2} \). Furthermore, both helper messages should not reveal any information about the secret keys to an attacker who can not observe any observation vector \( x \), \( y \) or \( z \). Finally the secret keys \( k_{1} \) and \( k_{2} \) should be uniformly distributed and independent of each other.

Definition 2: A secret-key rate pair \( (R_{1}, R_{2}) \) is called achievable in the 2-enrollment setting, if for all \( \delta > 0 \) and for all \( n \) large enough, there exist encoders and decoders such that

\[ \Pr(\hat{K}_{1} \neq K_{1} \lor \hat{K}_{1}\hat{K}_{2} \neq K_{1}K_{2}) \leq \delta, \]

\[ \frac{1}{n}H(K_{1}K_{2}) + \delta \geq \frac{1}{n} \log_{2}|K_{1}||K_{2}|, \]

\[ \frac{1}{n} \log_{2}|K_{1}| \geq R_{1} - \delta, \]

\[ \frac{1}{n} \log_{2}|K_{2}| \geq R_{2} - \delta, \]

\[ \frac{1}{n}I(K_{1}K_{2};M_{1}M_{2}) \leq \delta. \]

The secret-key capacity is the maximum achievable total rate \( C = R_{1} + R_{2} \).

Theorem 2: The secret-key capacity \( C = I(XY;Z) \) and the achievable secret-key rate pairs \( (R_{1}, R_{2}) \) satisfy

\[ R_{1} \leq I(X;Z) \]

\[ R_{1} + R_{2} \leq I(XY;Z). \]

In the following, we first show the converse of Theorem 2, that is no secret-key rate pairs \( (R_{1}, R_{2}) \) exist for which \( R_{1} > I(X;Z) \) or \( R_{1} + R_{2} > I(XY;Z) \).

A. Converse for 2-enrollment secret-key capacity

The upper bound to the achievable rate for the first key \( R_{1} \) follows from our results for the 1-enrollment scheme. We continue with

\[ H(K_{1}K_{2}ZM_{1}M_{2}) = H(K_{1}K_{2}ZM_{1}M_{2}\hat{K}_{1}\hat{K}_{2}) \leq H(K_{1}K_{2}) \leq 1 + P_{ek} \log_{2}|K_{1}||K_{2}| \leq 1 + 2nP_{ek}, \]

with \( P_{ek} = \Pr(\hat{K}_{1}\hat{K}_{2} \neq K_{1}K_{2}) \). For achievable rates

\[ H(K_{1}K_{2}) = I(K_{1}K_{2};ZM_{1}M_{2}) + H(K_{1}K_{2}|ZM_{1}M_{2}) \]

\[ \leq I(K_{1}K_{2};ZM_{1}M_{2}) + H(K_{1}K_{2}|ZM_{1}M_{2}), \]

\[ \leq I(K_{1}K_{2};ZM_{1}M_{2}) + H(K_{1}K_{2}|ZM_{1}M_{2}), \]

\[ \leq \]
This results in
\[ R_1 - \delta + R_2 - \delta \leq \frac{1}{n} H(K_1K_2) + \delta \]
\[ \leq 3\delta + I(XY; Z) + \frac{1}{n} + \delta. \]
Now with $\delta \downarrow 0$ and $n \to \infty$ we obtain the bound $R_1 + R_2 \leq I(XY; Z)$ for achievable rate pairs.

### B. Linear codes for 2-enrollment setting

Next, we demonstrate that linear codes exist that achieve the rates specified in Theorem 2, for the 2-enrollment scheme.

Fix an $\epsilon > 0$. Now $A^{(n)}(XYZ)$ is the set of jointly typical sequences as defined in Cover and Thomas [7], based on the joint distribution of the XYZ-source.

We specify a linear coding strategy $S_n$ by four parity check matrices. Two parity-check matrices $H_{m1}$ and $H_{k1}$ for the first encoder, with dimensions $(n\rho_{m1} \times n)$ and $(n\rho_{k1} \times n)$ respectively, and two further parity-check matrices $H_{m2}$ and $H_{k2}$ for the second encoder, with dimensions $(n\rho_{m2} \times n)$ and $(n\rho_{k2} \times n)$ respectively.

Encoder 1 observes a sequence $x$ of length $n$, generates a helper message $m_1 = H_{m1}x^T$ of length $n\rho_{m1}$ and a secret key $k_1 = H_{k1}x^T$ of length $n\rho_{k1}$, and sends this helper message over a public channel to the decoders. A one-step decoder that has received $m_1$ and did observe a sequence $z$, reconstructs the unique sequence $\tilde{x}$ such that $m_1 = H_{m1}\tilde{x}^T$ and $(\tilde{x}, z) \in A^{(n)}(XZ)$. If the reconstruction of $x$ is successful, this one-step decoder can reconstruct the secret $k = H_{k1}\tilde{x}^T$.

Encoder 2 observes a sequence $y$ of length $n$, generates a helper message $m_2 = H_{m2}y^T$ of length $n\rho_{m2}$ and a secret key $k_2 = H_{k2}y^T$ of length $n\rho_{k2}$, and sends the helper message over a public channel to the two-step decoder. This decoder has already processed the first step, see above. In addition, since it has obtained $m_2$ this two-step decoder reconstructs the unique $\tilde{y}$ such that $m_2 = H_{m2}\tilde{y}^T$ and $(\tilde{x}, \tilde{y}, z) \in A^{(n)}(XYZ)$, where $\tilde{x}$ was determined in the first step. Note that the secrets are binary vectors with $|K_1| = 2^{n\rho_{k1}}$ and $|K_2| = 2^{n\rho_{k2}}$.

Finally, we define a virtual decoder that observes both secrets $k_1$, $k_2$ and the helper messages $m_1$, $m_2$ and reconstructs $\tilde{x}$ and $\tilde{y}$ such that $k_1 = H_{k1}\tilde{x}^T$, $m_1 = H_{m1}\tilde{x}^T$ and $k_2 = H_{k2}\tilde{y}^T$ and $m_2 = H_{m2}\tilde{y}^T$ and $(\tilde{x}, \tilde{y}) \in A^{(n)}(XY)$.

We measure the reliability of a linear coding strategy $S_n$ in terms of the average error probability
\[ P_e(S_n) = \Pr(\hat{X} \neq X \text{ or } \hat{Y} \neq Y \text{ or } \hat{X}\hat{Y} \neq XY|S_n). \]
\[ \Pr(E_4) = \sum_{x,y} p(x,y) \Pr(\exists \tilde{y} \neq y : H_{k_2 \tilde{y} T} = H_{k_2 y T} \text{ and } H_{m_2 \tilde{y} T} = H_{m_2 y T} \text{ and } (x, \tilde{y}) \notin A^{(n)}(X|Y)) ) \]

\[ \leq 2^{n(H(X|Y) + 2\epsilon)} 2^{-n(\rho_{m_1} + \rho_{k_1})}. \]

\[ \Pr(E_5) = \sum_{x,y} p(x,y) \Pr(\exists \tilde{x} \neq x : H_{k_1 \tilde{x} T} = H_{k_1 x T} \text{ and } H_{m_2 \tilde{x} T} = H_{m_2 x T} \text{ and } (\tilde{x}, y) \notin A^{(n)}(X|Y)) ) \]

\[ \leq 2^{n(H(X|Y) + 2\epsilon)} 2^{-n(\rho_{m_1} + \rho_{k_2})}. \]

We conclude that for \( n \) large enough \( E(P_e(S_n)) \leq 6\epsilon \) as long as

\[ \rho_{m_1} > H(X|Z) + 2\epsilon \]

\[ \rho_{m_2} > H(Y|XZ) + 2\epsilon \]

\[ \rho_{k_1} + \rho_{m_1} > H(Y|X) + 2\epsilon \]

\[ \rho_{k_2} + \rho_{m_2} > H(Y|X) + 2\epsilon \]

\[ \rho_{k_1} + \rho_{m_1} + \rho_{k_2} + \rho_{m_2} > H(X|Y) + \epsilon. \]

Therefore, we have shown that linear codes exist that have \( \rho_{m_1} = H(X|Z) + 3\epsilon \) and \( \rho_{m_2} = H(Y|XZ) + 3\epsilon \), such that the decoders can successfully decode the secrets as long as \( n \) is large enough. Furthermore, we choose \( \rho_{k_1} = \alpha \) and \( \rho_{k_2} = I(X|Y; Z) - \alpha \) with \( 0 \leq \alpha \leq I(X; Z) \). Note that this choice for the matrix dimensions satisfies the above inequalities for SRAM-PUF’s, since \( H(X|Z) = H(X|Y) \) in this case.

C. Zero-leakage and uniformity of the keys

Now, we focus on the linear codes with dimensions \( \rho_{m_1}, \rho_{k_1}, \rho_{m_2}, \) and \( \rho_{k_2} \) that we have found before. The resulting leakage about the secrets from syndrome \( m_1 \) and \( m_2 \) is

\[ I(K_1, K_2; M_1, M_2) \]

\[ = H(K_1, K_2) + H(M_1 M_2) - H(M_1 M_2 K_1 K_2) \]

\[ \leq H(K_1 K_2) + H(M_1 M_2) - H(X Y) \]

\[ \leq H(K_1 K_2) + H(M_1 M_2) \]

\[ + \alpha n + 2n H[P_e(S_n)] \]

\[ \leq 6\epsilon + 1 + 2n H[P_e(S_n)] < 6\epsilon + 1 + 12n \epsilon. \]

Now for \( n \) large enough and an appropriate choice for \( \epsilon \) we conclude that \( I(K_1, K_2; M_1, M_2) \leq \delta \) for any \( \delta > 0 \), which satisfies the leakage requirement.

Next we find, from Fano’s inequality for the virtual decoder, that

\[ H(X|Y) = H(X|Y) K_1 M_1 M_2 \]

\[ \leq H(K_1 K_2) + H(M_1) + H(M_2) + H(X|Y) K_1 M_1 M_2 \]

\[ \leq H(K_1 K_2) + n(H(X|Z) | H(Y|X Z) + 6\epsilon) \]

\[ + 1 + 2n H[P_e(S_n)], \]

and thus

\[ \frac{1}{n} H(K_1 K_2) \geq I(X|Y; Z) - 18 \epsilon - 1. \]

Therefore, for any \( \delta > 0 \) we obtain that \( \frac{1}{n} H(K_1 K_2) + \delta \geq I(X|Y; Z) = \frac{1}{n} \log_2 |K_1||K_2| > R_1 - \delta + R_2 - \delta = I(X|Y; Z) - \delta \), by suitable choice of \( \epsilon \) and large enough \( n \). Thus the uniformity and independence conditions of the secret keys in Definition 2 hold. We conclude that the achievable secret-key rates are

\[ R_1 \leq I(X; Z), R_1 + R_2 \leq I(X|Y; Z). \]

V. CONCLUSION

We have shown that an encoder can generate a second key after observing additional input, while ensuring that both helper messages do not reveal information about the keys. The total achievable secret-key rate increases from \( I(X; Z) \) for the first key, to \( I(X|Y; Z) \) for both keys. Therefore, the same rate can be achieved sequentially by the 2-encoder scheme, as would be achievable when the encoder would generate a single key and helper message based on two observations. Finally, we note that the encoder does not require any information about the first enrollment in order to realize the second enrollment.

REFERENCES


