Selection and balancing for debiasing of SRAM-PUF

Selection and Balancing for Debiasing of SRAM-PUF

Lieneke C. J. Kusters
dept. of Electrical Engineering
Eindhoven University of Technology
c.j.kusters@tue.nl

Frans M. J. Willems
dept. of Electrical Engineering
Eindhoven University of Technology
f.m.j.willems@tue.nl

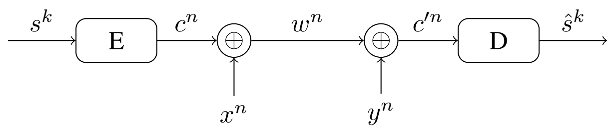

Fig. 1. Fuzzy commitment scheme

The fuzzy commitment scheme (Fig. 1) binds a cryptographic key s^k to an SRAM-PUF observation x^n. Helper data w^n is published, such that the key can be reproduced from another (noisy) observation $y^n = x^n + e^n$ of the SRAM-PUF. Uniformity of the SRAM-PUF observations (i.e. $\Pr(X = 1) = \Pr(X = 0)$) ensures that the key is secure from an attacker who can observe only the helper data w^n.

When the SRAM-PUF observations are not uniformly distributed (i.e. $\Pr(X = 1) \neq \Pr(X = 0)$), the helper data w^n may reveal information about the key, and the fuzzy commitment scheme is not secure. Leakage can be prevented by preprocessing the observation vectors to ensure that the input to the fuzzy commitment scheme is uniformly distributed. This is achieved by so-called debiasing schemes, and several methods have already been proposed in the literature [1]–[4].

Two principal methods for debiasing are selection and balancing. Here, we present both methods and derive the corresponding secret-key capacity. For our analysis we consider a binary PUF source that generates i.i.d. pairs (x, y) s.t.

$$\Pr(X = 1) = \Pr(Y = 1) = p, \tag{1}$$

$$\Pr(X \neq Y) = q. \tag{2}$$

Furthermore, we assume that $0 < p \leq 1/2$ and $0 < q \leq 2p$[1].

The **selection** method (randomly) selects a subset of the bits such that the output sequence has a uniform distribution. The selected bits are used as a regular input (of reduced length) to the fuzzy commitment scheme. The indices of the selected bits are attached to the helper data, such that the decoder can select the corresponding bits from its observation y^n.

We define a new random variable V that is 1 in case of selection and 0 otherwise. Then the selection probabilities are:

$$\Pr(V = 1|X = x) = \begin{cases} 1 & \text{if } x = 1, \\ \frac{p}{1-p} & \text{if } x = 0. \end{cases} \tag{3}$$

This results in $\Pr(X = 1|V = 1) = 1/2$, and thus the selected bits have an unbiased distribution.

The **balancing** method (randomly) flips a subset of the input bits, such that the output sequence has a uniform distribution. Here a bit flip corresponds to changing the value of 0 to 1 and vice-versa. The resulting sequence is used as a regular input to the fuzzy commitment scheme.

We define a new random variable X' that represents a bit X after the balancing method. Then

$$\Pr(X' = 1|X = x) = \begin{cases} 1 & \text{if } x = 1, \\ \frac{1/2-p}{1-p} & \text{if } x = 0. \end{cases} \tag{4}$$

This results in $\Pr(X' = 1) = 1/2$, and thus the output bits have an unbiased distribution.

The secret-key capacity for fuzzy commitment after debiasing is shown for both methods under various conditions in Fig. 2. We conclude that selection results in a higher secret-key capacity than balancing.

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

[1]Note that $q > 2p$ corresponds to $p_{Y|X}(1|1) < 0$.

REFERENCES

[1] R. Maes, V. van der Leest, E. van der Sluis, and F. Willems, "Secure Key Generation from Biased PUFs," in *Cryptographic Hardware and Embedded Systems - CHES 2015*, pp. 517–534, 2015.
[2] A. Schaller, T. Štankó, B. Skoric, and S. Katzenbeisser, "Eliminating Leakage in Reverse Fuzzy Extractors," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 954–964, 2018.
[3] B. Škorić and N. De Vreede, "The spammed code offset method," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 875–884, 2014.
[4] B. Škorić, "A trivial debiasing scheme for Helper Data Systems," *Journal of Cryptographic Engineering*, vol. 8, no. 4, pp. 341–349, 2018.

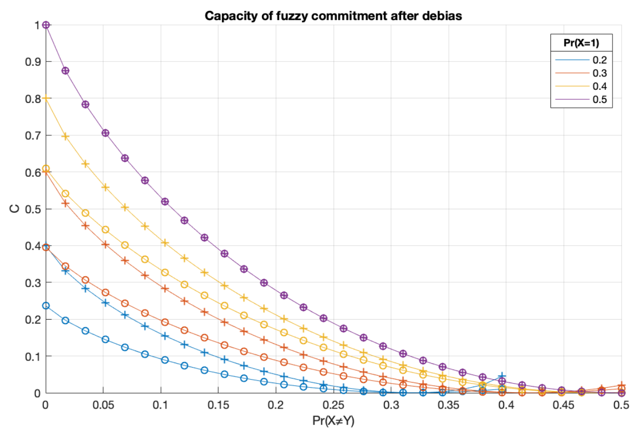

Fig. 2. Capacity of fuzzy commitment after selection + and balancing *o*.