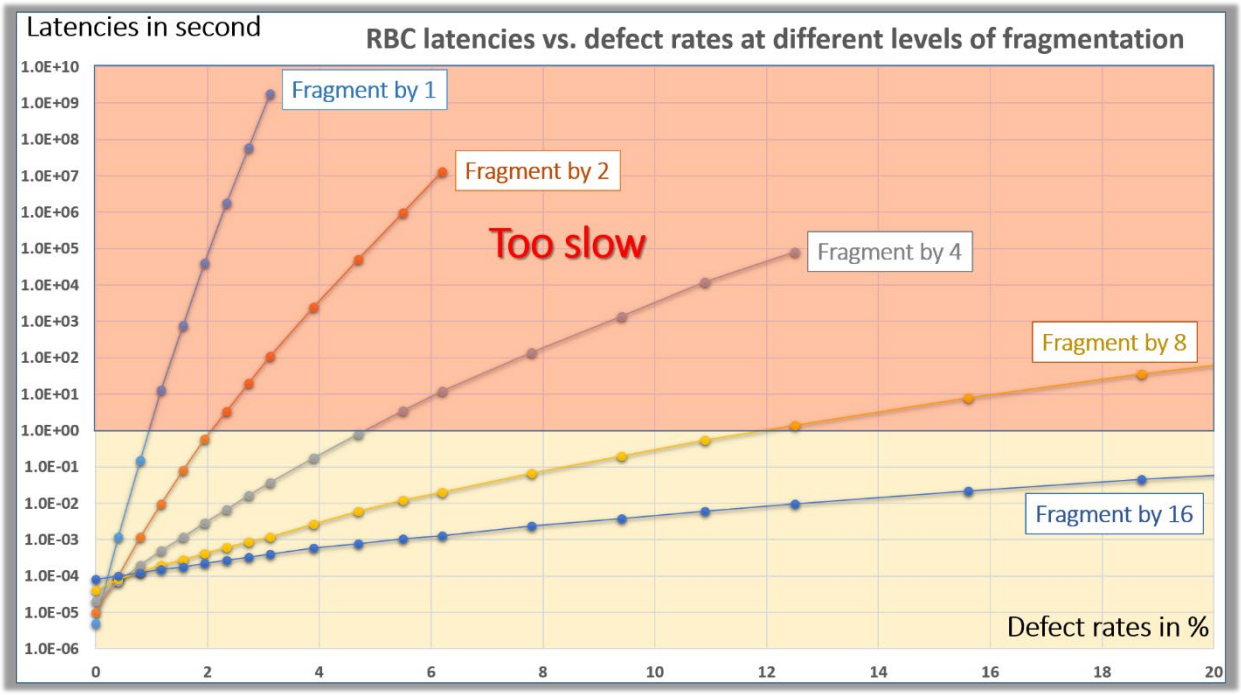
Replacing error correction by key fragmentation and search engines To generate error-free cryptographic keys from PUFs

Bertrand Cambou; Christopher Philabaum; Duane Booher
Northern Arizona University, Flagstaff, Arizona, USA
Bertrand.cambou@nau.edu; cp723@nau.edu; Duane.booher@nau.edu

Physical Unclonable Functions (PUFs) [1-6], the fingerprints of microelectronic components, are subject to aging, temperature drifts, electromagnetic interactions, and various environmental effects. Typically, this results in 2-10% error rates between the initial readings of the PUFs that are stored as references, and the responses generated from these PUFs. Error correcting (ECC) algorithms need to correct all errors, i.e. 100%, to generate usable cryptographic keys from PUFs, single-bit mismatches being unacceptable [7-11]. ECC algorithms use helper data from the transmitting party, and iterative methods such as fuzzy extractors at the receiving party, which consume computing power, and could thereby leak information to the opponents. The response based cryptographic method (RBC) eliminates the need to use error correction at the client level, as it generates cryptographic keys directly from the un-corrected responses of the PUFs [12-13]. This technology relies on the implementation of an efficient search engine, driven by the secure server, interacting with the network of client devices, which finds the uncorrected PUF responses, rather than correcting them. The matching algorithms start from the original PUF challenges, and exploit the knowledge of the cipher texts generated by the transmitting client devices, which have access to uncorrected PUF responses as cryptographic keys.

In this paper, we are presenting an optimization of the RBC algorithm by fragmenting the keys generated from the uncorrected responses. The experimental work is based on window 10 PCs powered by Intel I7 quad core processors, able to process the Advanced Encryption Standard (AES) in five microseconds. The client devices are the WiFire development boards from Microchip with 200Mhz 32-bit RISCs from ARM. The PUFs are generated from commercial 32Kbyte SRAMs produced by Cypress Semiconductor. Below 1% challenge-response-pair (CRP) error rates, the RBC algorithm is fast enough to be able to handle 256-bit long keys, and find in a few seconds the uncorrected keys generated by the client device, and its SRAM PUF. In order to enhance effectiveness at higher error rates, we propose the fragmentation of the keys generated by the PUF into sub-keys, also 256-bit long, which are padded with known random numbers. In a fragmentation by two, the first sub-key is generated by keeping the first 128 bits of the key generated by the PUF, filled with 128 bits that do not contain errors. The second sub-key is generated from the last 128 bits of the PUF. Statistically, the two sub-keys are showing error rates that are half of those of the full keys, and they are faster to find by the RBC engine. The figure enclosed below shows the efficiency of fragmentation as a function of the CRP error rates, in percent, for 256-bit long keys, and the RBC based on AES cipher texts.

Both modelling and experimental data demonstrate that the RBC with fragmentation can be effective on any PUFs, regardless of the CRP error rates. It is always desirable to minimize the level of fragmentation to reduce computing power at the client level. The suggested method has the potential of eliminating the need to use error correcting methods, as well as helper data, and thereby simplifies PUF-based cryptographic protocols, and enhances security.



References:

1) Holcomb, D. E., W. P. Burleson, and K. Fu. 2008. "Power-up SRAM state as an Identifying Fingerprint and Source of TRN". *IEEE Transaction on Computing, vol 57, No 11.*

2) Chen, T. I. B., F. M. Willems, R. Maes, E. v. d. Sluis, and G. Selimis. 2017. "A Robust SRAM-PUF Key Generation Scheme Based on Polar Codes". *In arXiv:1701.07320 [cs.IT].*

3) Prabhu, P., A. Akel, L. M. Grupp, W-K S. Yu, G. E. Suh, E. Kan, and S. Swanson. 2011. "Extracting Device Fingerprints from Flash Memory by Exploiting Physical Variations". *In 4th international conference on Trust and trustworthy computing.*

4) Cambou, B., and M. Orlowski. 2016. "Design of Physical Unclonable Functions with ReRAM and ternary states". *Cyber and Information Security Research Conference, CISR-2016, Oak Ridge, TN, USA.*

5) Korenda, A., F. Afghah and B. Cambou. 2018. "A Secret Key Generation Scheme for Internet of Things using Ternary-States ReRAM-based Physical Unclonable Functions". *In International Wireless Communications and Mobile Computing Conference (IWCMC 2018).*

6) Gao, Y., D. Ranasinghe, S. Al-Sarawi, O. Kavehei, and D. Abbott. 2016. "Emerging Physical Unclonable Functions with nanotechnologies". *IEEE, DOI:10.1109/ACCESS.2015.2503432.*

7) Maes, R., P. Tuyls and I. Verbauwhede. 2009. "A Soft Decision Helper Data Algorithm for SRAM PUFs". *In 2009 IEEE International Symposium on Information Theory.*

8) Boehm, H. M. 2010. "Error correction coding for physical unclonable functions". *In Austrochip-2010, Workshop in Microelectronics.*

9) Taniguchi, M., M. Shiozaki, H. Kubo and T. Fujino. 2013. "A stable key generation from PUF responses with a Fuzzy Extractor for cryptographic authentications". *In IEEE 2nd Global Conference on Consumer Electronics (GCCE), Tokyo, Japan.*

10) Delvaux, J., D. Gu, D. Schellekens and I. Verbauwhede. 2015. "Helper Data Algorithms for PUF- Kang, H., Y. Hori, T. Katashita, M. Hagiwara and K. Iwamura. 2014. "Cryptographie key generation from PUF data using efficient fuzzy extractors". *In 16th International Conference on Advanced Communication Technology, Pyeongchang, Korea.*

11) Becker, G. T., A. Wild and T. Güneysu. 2015. "Security analysis of index-based syndrome coding for PUF-based key generation". *In 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC.*

12) Cambou, B., C. Philabaum, D. Duane Booher, and D. Telesca. "Response-based Cryptography Methods with Physical Unclonable Functions". *Future of Information and Communication Conference, FICC-2019.*

13) Cambou, B., "Unequally Powered Cryptography with PUFs for network of IoT", Spring Simulation Conference, SpringSim2019.