Physical Unclonable Function (PUF) based on 0.18 um Sub-threshold SRAM

H.-R. Graf, M. Pons Solé, T.-C. Le, S. Emery

Physical unclonable functions (PUFs) have been proposed as central building blocks in a variety of cryptographic protocols and security architectures. In this study, the suitability to implement PUFs with existing sub-threshold 0.18 um SRAMs was evaluated. Operating PUFs in the sub-threshold region can enable adding security features in ultra-low power applications within a limited power budget.

Physical unclonable functions (PUFs) are increasingly proposed as central building blocks in cryptographic protocols and security architectures. Among other uses, PUFs enable device identification and authentication, binding software to hardware platforms and secure storage of cryptographic secrets.

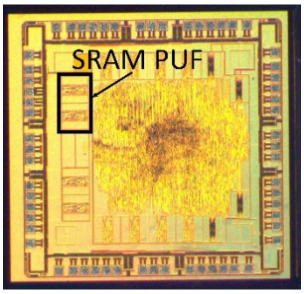

Figure 1: Chip photograph of sub-threshold 0.18 um SRAM PUF.

PUFs typically exhibit a challenge/response behavior: When queried with a challenge, the PUF generates an unpredictable but repeatable response that depends on the physical properties of the underlying PUF hardware. The most vital PUF properties are:

- Robustness
- Uniqueness
- Unpredictability

Robustness requires that, when queried with the same challenge multiple times, the PUF should generate similar responses that differ only by a small error that can be corrected by an appropriate error correction mechanism.

Uniqueness means that the responses for the same challenge on different PUF instances are uncorrelated, based on intrinsically unique and random physical variations of the implementing device.

Unpredictability guarantees that the adversary cannot efficiently compute the response of a PUF to an unknown challenge, even if he can adaptively obtain a certain number of other challenge/response pairs from the same and other PUF instances.

PUFs using intrinsic randomness of ASIC processes are highly attractive because they can be implemented with very small hardware costs, or even be built from existing hardware having the right properties. The most popular electronic PUF types are either delay-based (arbiter and ring oscillator PUFs) or memory-based (SRAM, flip-flop and latch PUFs).

For this study, the suitability of sub-threshold 0.18 um SRAM [1] (Figure 1) to implement PUFs was evaluated. Measurements on a total of 10 devices integrated in EM Microelectronic Marin ALP CMOS 180 nm technology with 2 SRAMs of 256 bytes each were conducted. At 17 different supply voltages (between 0.43 V to 1.2 V), the memory content after power-off-and-on cycles was read-out. The measurements were repeated 100 times for every challenge.

To evaluate robustness and uniqueness, the Hamming distance (in bits) was calculated and analyzed (Figure 2). Good robustness is shown with the intra Hamming distance of 0 bits at 70 % probability. The smooth Gaussian distribution of the inter Hamming distance indicates a good uniqueness as well by having 3-5 bits distance at a probability of 70 %. Further analysis shows that identification is possible and attests a good potential for unpredictability.

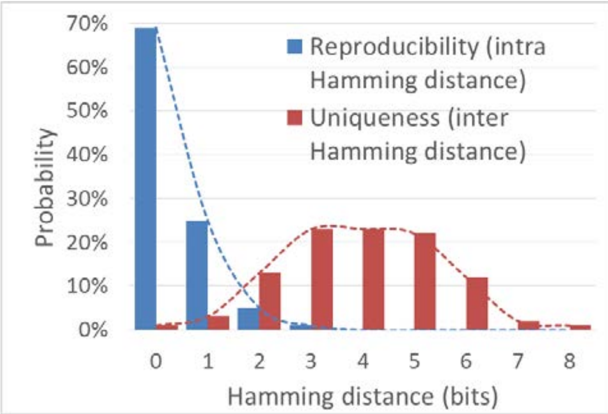

Figure 2: Robustness and uniqueness of SRAM based PUF.

For ultra-low power applications like IoT nodes, adding security features within the limited power budget is key. The presented sub-threshold SRAM PUF, that reaches static consumption in the order of a nW at 0.43 V, is therefore perfectly suitable for this kind of applications.

Next steps will require more measurements with more variations (e.g. impact of temperature and ageing), deeper analysis of the measurements and study of the entropy source (e.g. health check). With digital post-processing, the entropy could get improved. Finally, a system-level design would be required to implement the challenge-response behavior directly on the ASIC, not off-line as in this study.

This research has been funded by a CSEM Creativity Grant.

[1] M. Pons Solé, *et al.*, "Sub-threshold latch-based icyflex2 32-bit processor with wide supply range operation", ESSCIRC (2016).