A Rapid Reset 8-Transistor Physically Unclonable Function Utilising Power Gating

Yujin Zheng, Alex Bystrov, Alex Yakovlev
Microsystems Research Group, Newcastle University, Newcastle upon Tyne, UK
y.zheng26@newcastle.ac.uk, a.bystrov@newcastle.ac.uk, alex.yakovlev@newcastle.ac.uk

***Abstract*—Physically Unclonable Functions (PUFs) need error correction whilst regenerating *Secret Keys* in cryptography. The proposed 8-Transistor (8T) PUF, which coordinates with the power gating technique, can significantly accelerate a single evaluation cycle 1000 times faster than 6T-SRAM PUF does with a 12.8% area increase. This design enables multiple evaluations even in the key regeneration phase in field, hence greatly reducing the number of errors and the hardware penalty for error correction. The 8T PUF derives from the 6T SRAM. It is built to eliminate data retention swiftly and maximise physical mismatches. And a two-phase power gating module is designed to provide controllable power-on/off cycles rapidly for the chosen PUF clusters in order to facilitate statistical measurements and curb the in-rush current, thereby enhancing PUF entropy and security. An architecture of the power-gated PUF is developed to accommodate fast multiple evaluations. Post-layout Monte Carlo simulations were performed with Cadence, and the extracted PUF Responses were processed with Matlab to evaluate the 8T PUF performance and statistical metrics for subsequent inclusion into PUF *Responses*.**

***Index Terms*—Physically Unclonable Function, PUF, power gating, SRAM, metastability, data remanence, data retention.**

I. Introduction

PUFs are hardware-based functions which map *Challenge* to *Response* through physically unclonable devices [1], and each function is unique. The uniqueness comes from the uncontrollable physical parameter mismatches generated in semiconductor fabrication. These mismatches provide the SRAM-based PUF [2], [3] random power-up readings. Accordingly, these repeatable start-up values are the raw data for creating PUF *Response*, and the address used to read them is the *Challenge*.

The PUF readings are the source which generates *Secret Keys*, so they must be sole and repeatable. However, a small number of cells produce unreliable readings due to negligible physical mismatches. Hence, there are some requisite techniques for identifying those unstable cells during manufacturing, such as Multiple Evaluation [4] and Temporal Majority Voting [5]. Nevertheless, the SRAM-PUF cells are sensitive to environmental changes and ambient noise in field, and these factors cause bit errors. Meanwhile, the time for key regeneration in field is brief. However, the hardware penalty of the online bit error correction increases exponentially with the error numbers growing [6]. This is unsuitable for lightweight IoT applications. Above all, time is a crucial factor that has been overlooked in many PUF-related papers. Our power-gated 8T PUF is designed to target these issues. The architecture is illustrated in Fig. 1. The main contributions are listed below:

a) Custom 8T PUF facilitates fast statistical measurements and improves security: The 8T PUF maximises physical mismatches and eliminates data remanence swiftly for high-speed evaluations and countering security attacks [7]. It does not require a special process for high-density SRAM manufacturing and can be fabricated in the same process as MCUs.

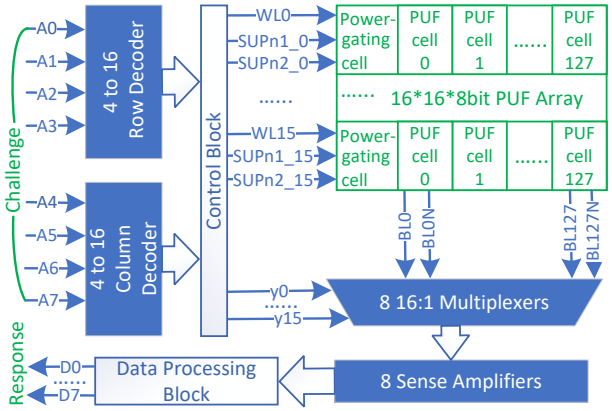

Fig. 1. *A 2kb Power-gated PUF Array Architecture*

b) Two-phase power gating improves security whilst saving energy: This method powers on and off the chosen PUF clusters in three stages: reset, phase I power-up and phase II power-up. The reset stage quickly cut off the virtual power supply. Phase I slowly powers up the chosen PUFs and curbs the in-rush current in the hope of reducing EMI, crosstalk and hiding from Differential Power Analysis (DPA). Then phase II speeds up the voltage ramp-up process. Meanwhile, without the power supply and data remanence, no secret information or energy will leak out from the unchosen PUFs.

c) Enabling data processing in field: The high-speed measurements not only reduce the time of the key enrolment phase but also enable multiple evaluations in the key regeneration phase. Combining with data processing, Bit Error Rate (BER) drops greatly. Thus, the hardware penalty for error correction reduces. The raw PUF readings are processed and marked onto a bitmap to identify the stability level of each PUF. Those unstable readings can be used for *True Random Number* generation or as part of the PUF *Response*.

II. Power-gated PUF Design

The architecture of a power-gated PUF array is illustrated in Fig. 1. The Data Processing block is to evaluate and mark the raw read-out bits for improving PUF entropy. There are two building blocks, i.e. the custom 8T PUF in Fig. 2(a) and the two-phase power gating cells in Fig. 2(c). A single-phase power

978-3-9819263-7-8/DATE23/© 2023 EDAA

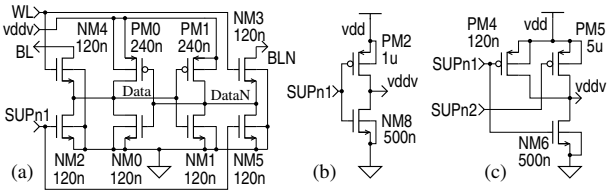

Fig. 2. Schematics of (a) 8T PUF cell, (b)Single-phase Power Gating Cell, (c)Two-phase Power Gating Cell

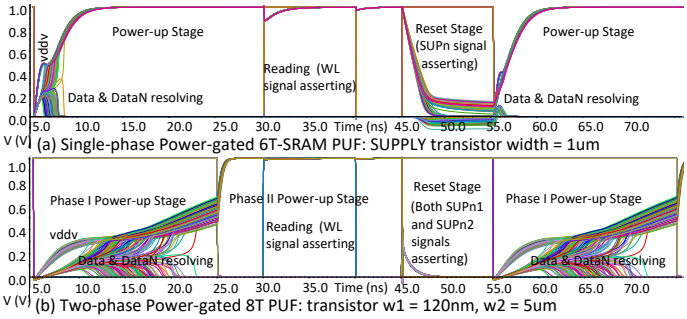

Fig. 3. *Waveforms of a 100-Run Post-layout Monte Carlo Simulation*

gating cell for comparison is shown in Fig. 2(b). Test circuits were implemented in UMC90nm technology with Cadence.

a) 8T PUF Design: The 8T PUF stems from conventional 6T SRAM but abandons the write function and keeps only the read process. The smallest transistors were chosen to maximise the physical mismatches. Moreover, two NMOS (*NM2* and *NM5*) were added for rapidly discharging the internal nodes *Data* and *DataN* during the reset stage. Thus, the reset time can be shortened from $5\mu s$ to *5ns*, and no retention data can be exploited by attackers. The 8T PUF layout was implemented symmetrically with a 12.8% area increase to 6T SRAM.

b) Two-phase Power Gating Method and Design: Two PMOS (*PM4* and *PM5*) are the *SUPPLY* transistors for two-stage power switching, and an NMOS (*NM6*) is for fast resetting. The reset stage quickly drops the virtual power supply *vddv* to *0V* and eliminates retained data. Phase I power-up utilises the smallest *SUPPLY* transistor to curb the *vddv* output and prolong the metastability resolving process hoping to minimise the mutual disturbance amongst the PUF cells. Then Phase II power-up employs a larger *SUPPLY* transistor to release the *vddv* quickly for a cluster of 128 PUF cells. The sizes of two *SUPPLY* transistors can be manipulated to support more PUF cells and control the in-rush current.

III. Simulations and Results

a) Power Gating Parameter Evaluation: The DC sweep and transient simulations were performed to evaluate the size of *SUPPLY* transistors and the corresponding behaviour of the PUF cells. By decreasing the size of the *SUPPLY* transistor, the metastability resolving time is prolonged, and the current peak is flattened. These effects can be utilised to reduce EMI, crosstalk and against side-channel attacks.

b) Power-gated PUF Behaviour: The post-layout Monte Carlo simulations with threshold voltage mismatches were conducted to observe the different power-up and reset behaviour between 8T PUFs and 6T-SRAM PUFs. The test circuit includes a row of two-phase power-gated 128 8T PUFs and a row of single-phase power-gated 128 6T-SRAM PUFs for comparison. In Fig. 3 (a), single-gated *vddv* reaches *1V* in roughly *7ns* whilst quickly resolving metastability of *Data* and *DataN*. By contrast, Fig. 3 (b) shows that in phase I, *Data* and *DataN* start wrestling while *vddv* ramping up slowly, then escape metastability and tend to their distinct logical status in various resolving times. These opposite tendencies demonstrate the PUF randomness in real circuits. Following this, phase II swiftly raises *vddv* to *1V* in around *1ns*. The major evolution of 8T PUF can be seen in the reset stage. *Data* and *DataN* of the 8T PUFs can be reset within *5ns*. In contrast, the 6T-SRAM PUFs still have data remanence which keeps the following cycles of data readings unchanged and is the target of attackers.

c) Reset Time and Effect: Without resetting thoroughly, the assessment of the PUF characteristics can be misguiding. The readings of the under-reset 6T-SRAM PUFs have never changed during our more than 200,000 runs of simulations in nominal condition. This creates a deceptive deduction that the 6T-SRAM PUFs are 100% stable. However, by prolonging the reset time duration from *5ns* to $5\mu s$, the simulation results show that the 6T-SRAM PUFs are as unstable as the 8T PUFs.

d) 8T PUF property measurements: Twenty clusters of 2048 8T PUFs were read out for 100 on/off power cycles. These PUF clusters imitate different PUF devices. The simulations resemble the same 100 times *Challenge* through different PUF devices. And the 2048-bit strings are the raw *Responses*. The readings were processed with Matlab to assess the PUF properties. For the 8T PUF robustness, the average BER is 0.65% in nominal condition and 0.92% in the worst corners. However, the worst corner BER drops to 0.26% after data processing which combines Multiple Evaluation with Majority Voting etc. Meanwhile, the average intra-distance is 1.4% which is close to the ideal value of 0%. For the 8T PUF uniqueness, the average inter-distance of our 8T PUF clusters is 51.5% which is close to the ideal value of 50%.

References

[1] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 148–160.

[2] J. Guajardo, S.S. Kumar, G.J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," in *International workshop on cryptographic hardware and embedded systems*, 2007, pp. 63–80.

[3] D.E. Holcomb, W.P. Burleson, and K. Fu, "Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID tags," in *Conference on RFID Security, vol. 7, no. 2,* 2007, pp. 01.

[4] M. Bhargava, C. Cakir, and K. Mai, "Reliability enhancement of bi-stable PUFs in 65nm bulk CMOS," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, 2012, pp. 25-30.

[5] S.K. Mathew, et al., "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," in *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, 2014, pp. 278–279.

[6] C. Bösch, J. Guajardo, A.R. Sadeghi, J. Shokrollahi, and P. Tuyls, "Efficient helper data key extractor on FPGAs," in *International workshop on cryptographic hardware and embedded systems,* Springer, Berlin, Heidelberg, 2008, pp. 181-197.

[7] N.A. Anagnostopoulos, et al., "Attacking SRAM PUFs using very-low-temperature data remanence," *Microprocessors and Microsystems, 71,* 2019, pp.102864.