# Silicon Physical Unclonable Function resistant to a $10^{25}$-trial brute force attack in 90 nm CMOS

S. Stanzione, G. Iannaccone
Dipartimento di Ingegneria dell'Informazione: Elettronica, Informatica, Telecomunicazioni, Università di Pisa
Via Caruso 16, Pisa, 56122, Italy {stefano.stanzione, g.iannaccone}@iet.unipi.it.

**Abstract**

A CMOS 90 nm physical unclonable function (PUF) based on analog signal processing and process variability has been realized, resistant to a brute force attack of more than $10^{25}$ trials. Experimental measurements show that the circuit exhibits 38 $\mu$W power consumption. Process and temperature monitor and compensator keep the experimental BER below 0.1% at 125°C or with a 10% $V_{DD}$ variation, with excellent accelerated aging behavior.

**Introduction**

The market of automatic identification is steadily increasing, especially due to the diffusion of "Internet of Things" applications. In parallel, the need of low-cost countermeasures to invasive attacks, identity theft, and cloning, is increasing. One of the most promising alternatives to current CPU-intensive digital authentication techniques is the use of Physical Unclonable Functions (PUFs), that are functions based on the physical properties of complex systems, easy to evaluate, but hard to characterize or to invert [1]. Silicon electronic PUFs have been proposed that exploit the random variability of transistor threshold voltages [2], of logic gate delays [3] or of ring oscillator frequencies [4]. Since PUFs in general process analog variables, their stability against variations of the operating conditions and aging is a challenge. Recently, we have proposed a silicon PUF [5] based on threshold voltage variability in a 90 nm CMOS technology, including built-in process and temperature compensation circuits, that achieved a much lower BER compared to the literature in all operating conditions. The circuit in [5] was mainly intended to test the concept (especially against aging) and included very simple analog processing, so that the system was vulnerable to a brute force attack of less than $10^5$ trials. Here, we demonstrate a silicon PUFs resistant to a brute force attack of more than $10^{25}$ trials, with a new analog processing scheme, process and temperature monitor and compensation, improved robustness to aging and to variation of the operating conditions.

**Circuit Description and Results**

The block diagram and the photo of the chip realized in STM 90 nm CMOS are shown in Fig. 1. The "nanokey" system consists of two main components: an array of CMOS inverters and an analog processing unit. The digital challenge is a sequence of $N$ inverter addresses, which are in sequence biased with the input voltage $V_{ref}$. Their analog output $V_{out}$ is sent as input to the analog processing unit, which implements a function of $M$ analog input quantities. Its output $V_{proc}$ is sent to a comparator to provide a single output bit. Every $M/2$ addresses a new response bit is computed so that we obtain a digital response of $2N/M$-1 bits. In order to pre-emptively discard from the response the bits more likely to fail, during the first collection of challenge-response pairs by the authenticating entity an additional string - the response flag string – is also collected. A response flag bit is generated by the analog processor for each response bit and indicates whether the analog output $V_{proc}$ is closer to the threshold than a so-called "decision margin" $V_{DM}$. The first collected response flag string is used as a mask for the subsequent validation of the response.

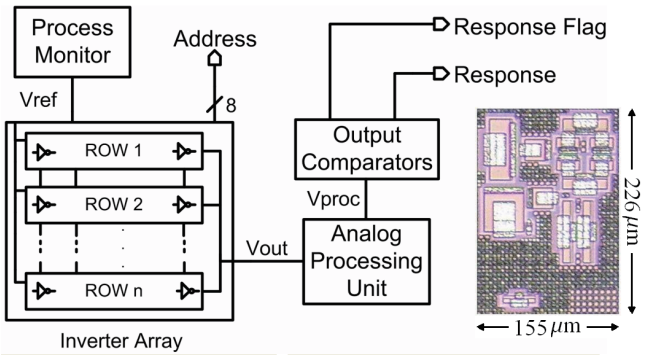


Fig. 1 Block diagram of the proposed PUF and photo of the chip.

This method has the cost of reducing the number of effective bits in the response, but makes the system extremely robust to aging and to variations of the operating conditions. The implementation of [5] can be seen as a particular case of this description with $N$ = 256 and $M$=2. In this case, a brute force attack can be performed, with only 32640 trials. The new implementation corresponds to $N$=256 and $M$=16. In this way the number of required trials becomes about $10^{25}$.

In the case of our implementation the analog processing unit computes the difference between the averages of two groups of $M/2$ analog input voltages. Therefore, we simply need the circuit shown in Fig. 2 (top): a Switched-Capacitor integrator followed by an S/H. After each group of $M/2$ array outputs, the integrator output is sampled and reset. In order to reduce the effects of the leakage currents, the S/H consists of two stages. The leakage currents are a function of the voltage drop between the input and the output of a S/H stage: $I_1=f(V_1-V_2)$ and $I_2=f(V_2-V_3)$. Supposing $I_2 \ll I_1$, during the hold phase the variation of $V_2$ is $\Delta V_2 = t_{HOLD}I_1C_{S1} \ll V_1-V_2$. So, the variation of $V_3$ is $\Delta V_3 = t_{HOLD}I_2C_{S2} = f(\Delta V_2)t_{HOLD}C_{S2} \ll \Delta V_2$. The switches are implemented with high threshold voltage MOS transistors in order to reduce the off currents $I_1$ and $I_2$.

The correlation factor between the responses of different chips to the same challenge, measured on 24 different PUFs, is always smaller than 0.1. The power consumption with $V_{DD}$ = 0.6 V is 38 $\mu$W, for an input bit rate of 768 Kb/s and an output bit rate of 6.25 Kb/s.

To keep the inverters biased in the maximum gain region, and to make the output response reproducible in the presence of temperature, supply voltage, and process variations, the input voltage of the inverters, $V_{ref}$, is provided by the Process Monitor (PM), shown in Fig. 2. The two pairs of very large nMOS and pMOS are perfectly matched and amplify the differential voltage ($V_X-V_{DD}/2$). The circuit labelled with $A$ in Fig. 2 consists of 6 inverters identical to those forming the nanokey array connected in parallel and is equivalent to a single inverter of the array biased in the gain region.

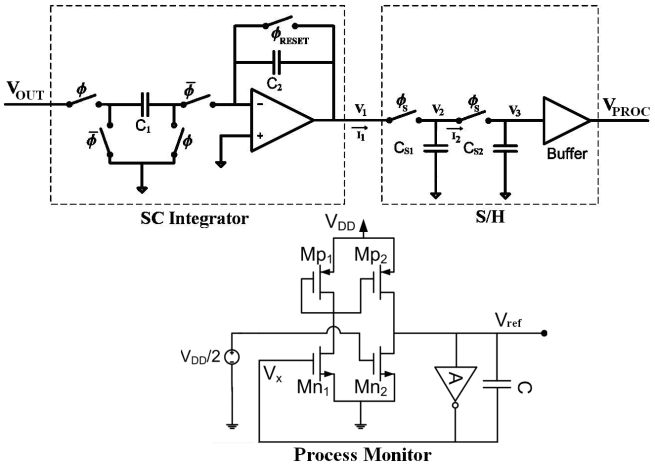


Fig. 2 Analog Processing Unit (above) and Process Monitor (below).

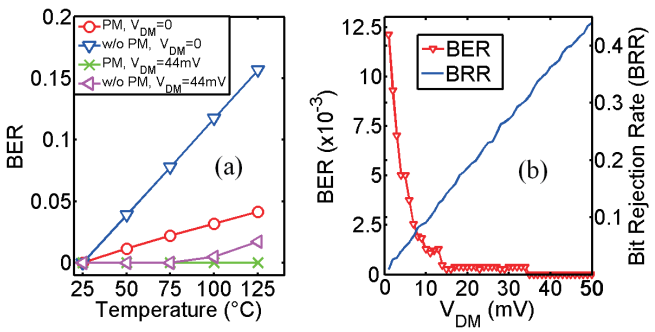


Fig. 3 (a) Simulated BER obtained with and without Process Monitor (PM) and (b) experimental results in standard conditions.

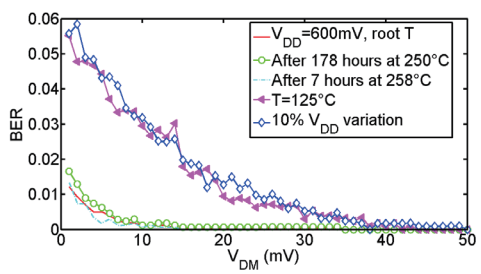


Fig. 4 Experimental BER obtained in different operating conditions and after accelerated aging tests.

The effect of compensation is dramatic (Fig. 3): it reduces the BER by a factor 4 for $V_{DM}$=0 V, and below 0.06 % with $V_{DM}$=44 mV. In Fig. 3b the BER and the Bit Rejection Rate (BRR), i.e. the ratio of bits preemptively eliminated from response validation, in standard operating conditions ($V_{DD}$=600mV and room temperature) are plotted as a function of the decision margin $V_{DM}$.

After accelerated aging tests no observable degradation in the response has been measured. As a hint of some possible aging going on, we evaluated the standard deviation of the difference between the S/H outputs and those of the first reference measurement. Such value slowly increases in time and is 4.9 mV after 178 hours at 250°C and after 7 hours at 258°C. Assuming an Arrhenius-type process, we obtain a similar aging well in excess of 10 years even at 150°C. As can be seen in Fig. 4, after this time chips still work perfectly. Choosing a $V_{DM}$=44 mV, BER in standard conditions is lower than 0.009%, BER in the worst case (between $V_{DD}$ variation of 10% and T = 125 C) is lower than 0.1% and Bit Rejection Rate is about 39.7%.

The *false rejection rate* (FRR), i.e. the probability that an original PUF is not authenticated, and the *false acceptance rate* (FAR), i.e. the probability that a false PUF is authenticated as the original one, are a function of the total number of response bits $k$ and of the maximum number $t$ of wrong response bits tolerated in the authentication. They are shown in Fig. 5 for $k$=256. Note that for $V_{DM}$=44 mV, both FRR and FAR are lower than $10^{-25}$.

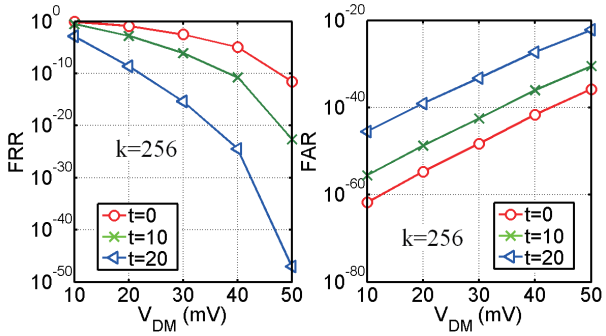


Fig. 5 Experimental FRR (left) and FAR (right) as a function of $V_{DM}$.

In Table I we compare the performance of our presented PUFs with other results presented in the literature: The number of trials required for a brute force attack is larger and the BER is lower than all comparison circuits. Accelerated aging experiments are missing in most comparison devices.

TABLE I

| | Ref. [3] | Ref. [4] | Ref. [5] | This work |
|---|---|---|---|---|
| standard BER (%) | < 0.7 | - | < 0.07 | < 0.009 |
| worst case BER(%) | < 4.8 | < 0.48 | < 0.4 | < 0.1 |
| Trials for brute force attack | $1.4\times10^{20}$ | 523776 | 32640 | $10^{25}$ |
| Technology | TSMC 0.18 $\mu$m | FPGAs 90 nm | CMOS 90nm | CMOS 90 nm |
| Power ($\mu$W) | - | - | 30 | 38 |
| Area (mm$^2$) | 1.47 | - | 0.018 | 0.035 |

In conclusion, we exploit the random process variability of nanoscale CMOS technologies to demonstrate a mixed-signal silicon PUF for secure authentication realized in CMOS 90 nm extremely resistant to a brute force attack and with excellent robustness to process and temperature variations, and to accelerated aging. This work has been supported by Fondazione Cassa di Risparmio di Pisa.

## References

[1] R. Pappu, et al, "Physical one-way functions", *Science*, vol. 297, pp. 2026-2030, 2002.

[2] K. Lofstrom, W. R. Daasch, D. Taylor, "IC identification circuit using device mismatch", *IEEE-ISSCC 2000*, Digest Tech. Papers, pp. 372-373, 2000.

[3] J. W. Lee, et al, "A technique to build a secret key in integrated circuits for identification and authentication application", *2004 Symposium On VLSI Circuits*, pp. 176-179, 2004.

[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation", *Proc. DAC 2007*, pp. 9-14, June 4-8, 2007.

[5] D. Puntin, S. Stanzione, G. Iannaccone, "CMOS unclonable system for secure authentication based on device variability", Proc. ESSCIRC 2008, pp. 130-133, Edinburgh, 2008.