CMOS Silicon Physical Unclonable Functions Based on Intrinsic Process Variability

Stefano Stanzione, Daniele Puntin, and Giuseppe Iannaccone, *Senior Member, IEEE*

***Abstract*—This paper presents an extreme-low-power mixed-signal CMOS integrated circuit for product identification and anti-counterfeiting, which implements a physical unclonable function operating with a challenge-response scheme. We devise a series of circuits and algorithmic solutions based on the use of a process monitor and on the prediction of the erratic response bits which allow to suppress the effects of temperature, voltage supply and process variations in order to obtain a robust and reliable behavior.**

The prototype ICs are implemented in a 90 nm CMOS process. Measurements show that the circuit exhibits 38 μW power consumption, a bit error rate in the response to a challenge smaller than 0.1% at 125°C or with a 10% voltage supply variation, which is a factor 4 lower than the best result obtained in the literature. The circuit is resistant to a brute force attack of more than 10^{25} trials and exhibits false acceptance rate and false rejection rate both lower than 10^{-25}. Accelerated aging tests provide a lifetime estimate much in excess of the conventional ten-year requirement even at 150°C.

***Index Terms*—Physical unclonable functions, process monitor, process variability, RFID, secure authentication.**

I. Introduction

COUNTERFEITING severely affects different industrial sectors, including the pharmaceutical, the aircraft, the automotive, and the luxury goods Industry [1]. For example, counterfeiting of pharmaceutical defrauds consumers and poses ill patients at severe health risks. Recently, radio frequency identification (RFID) technology has been considered in the United States by the Food and Drug Administration (FDA) with the aim of combating counterfeit pharmaceuticals. For this kind of applications it is crucial to be able to authenticate the object as the one originally issued by a given institution, bank or company. From this point of view, low-cost unforgeable authentication hardware would greatly broaden the range of applications of automatic authentication and identification.

In typical high-end RFID systems, authentication is enabled by the shared storage of a secret key in the transponder and in the reader [2]. Such solution entails several security issues, because it is crucial to ensure that a malicious user cannot hack the transponder and then clone it.

The possible attacks to an identification system can be classified in two broad categories: invasive (or physical) attacks and non-invasive attacks [3]. The non-invasive attacks [4], [5] do not modify the system, and can be prevented through the use of more robust authentication algorithms [6]. Another way to prevent non-invasive attacks in a system with a challenge-response authentication protocol, consists in increasing the number of Challenge-Response Pairs (CRPs), that is enlarging the space of possible responses to a stimulus applied to the system. In this way, characterizing the system can become prohibitively time-consuming.

An invasive attack, on the other hand, is an attack where the enemy physically breaks into the device by modifying its structure. For example, the *optical fault induction analysis*, based on the use of a laser light to change the state of a single SRAM cell, can be adopted to reverse engineer a memory address map [7].

An emerging option, resistant to invasive attacks, is represented by Physical Unclonable Functions (PUFs). A PUF is a function mapping challenges to responses that is easy to evaluate but hard (in practice impossible) to characterize, model or reproduce. Its unclonability stems from the fact that the function depends in a complex way upon several physical quantities that the manufacturing process cannot control.

The first PUFs were introduced by R. Pappu *et al.* [8], [9] and were based on an optical principle of operation. A transparent material, containing randomly distributed scattering particles, is illuminated by a laser light with a given angle, distance and wavelength. The speckle patterns that result from multiple scattering of laser light in a disordered optical medium are unique and unpredictable. Using this configuration as an authentication system, the challenge can be the angle of incidence, the focal distance, the wavelength of the laser beam or any other change in the wave front, whereas the response is a digital string obtained by applying a hash function to the digitized image of the speckle pattern.

One of the most important parameters of a PUF is the number of independent CRPs. For an optical PUF like the one proposed by Pappu, this number is lower than 10^6 [10]. So, a non-invasive attack like the brute force technique can be easily performed, in order to fully characterize the system. Another problem of optical PUFs is that a response is not “exactly” reproducible, because of the inherent noise of analog systems.

At about the same time, more convenient silicon PUFs have been introduced. They use the manufacturing process variations in ICs with identical masks to uniquely characterize each chip. The first idea was to exploit the mismatch of MOSFET threshold voltages implemented with a standard 0.35 μm CMOS process [11]. The core of the circuit is an addressable array of MOS-

Manuscript received March 15, 2010; revised November 20, 2010; accepted February 04, 2011. Date of publication April 29, 2011; date of current version May 25, 2011. This paper was approved by Associate Editor Kari Halonen. This work was supported in part by Fondazione Cassa di Risparmio di Pisa and by Cassa di Risparmio di Pisa, Lucca e Livorno.

The authors are with the Dipartimento di Ingegneria dell’Informazione: Elettronica, Informatica, Telecomunicazioni, Università di Pisa, Pisa 56122, Italy (e-mail: g.iannaccone@iet.unipi.it)

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSSC.2011.2120650

FETs sequentially biased according to an order defined by the challenge. The response is obtained by converting the sequence of analog voltage samples into a binary string. The obtained bit error rate (BER) was slightly lower than 5%, so very close to the results of optical PUFs.

Other silicon PUFs exploit the statistical delay variation of circuits and interconnects to identify individual ICs [12], [13]. A chain of switches, driven by the bits of the challenge, determines the path of the input digital signal. The signal propagates in parallel through two different but nominally identical paths and finally an arbiter circuit produces a digital response bit, effectively measuring which of the two paths is faster. Experiments on a test chip fabricated with TSMC 0.18-μm CMOS process have shown a BER of about 0.7%, that rises to 4.8% at a temperature of 67°C or to 3.7% for a $\pm 2\%$ voltage supply variation [12].

Subsequently, a different type of silicon PUFs has been proposed [14]. N ring oscillators have been implemented in the same chip. Due to manufacturing variations, each ring oscillator generates a signal with a slightly different frequency. Using the challenge bits, two of the N oscillators are selected and their frequencies are compared, in order to generate the response. Experimental measurements have shown a BER lower than 0.48% in the temperature range from 20°C to 120°C and with a $\pm 10\%$ voltage supply variation.

A low-power PUF has been proposed by Su *et al.* [15]. The circuit is an SRAM, implemented in a 0.13 μm CMOS process, and exploits the dependence of the initial state of the cells on the threshold-voltage mismatch of the latch transistors. When the circuit is powered on, the transient time is less than 10 ns and, during the reading phase, the power consumption is essentially due to static leakage currents. However, the BER is about 3.04% and the circuit is fundamentally digital, therefore it has a smaller CRP space and then it is easier to characterize than a circuit based on analog processing.

In this work we propose a silicon PUF (the "nanokey") to be used in a challenge-response authentication scheme. The circuit exploits the variability of minimum size MOSFET threshold voltages in a standard CMOS 90 nm process, in order to generate a unique unclonable and reliable digital response to challenges provided as input to the system. This solution is also robust to invasive attacks because removing passivation layers would dramatically alter small differences between transistor threshold voltages.

We propose and use a series of circuits and algorithmic solutions that strongly suppress the dependence of circuit behavior and of the authentication operation upon process, temperature, supply voltage variations, and ageing. In this way we are able to obtain a lower BER and more robust operation, compared to the other solutions proposed in the literature. This first prototype (P_1) has been used to verify the concept and the effects of aging on its performance [16]. A second prototype (P_2) has been implemented [17], to verify the operations of an authentication circuit with a much larger CRP space, and therefore much more resistant to brute force attacks.

Since the response of the PUF to any challenge is unknown even to the manufacturer, we envisage a scheme in which an authenticating entity tests each PUF before release, collects and stores a large number of valid challenge-response pairs. When one wants to authenticate the PUF, she has first to ask to the authenticating entity a challenge, and then has to send the response back to the authenticating entity which matches the response to the stored one. Maximum security is obtained if each CRP is used only once and new CRPs are periodically generated.

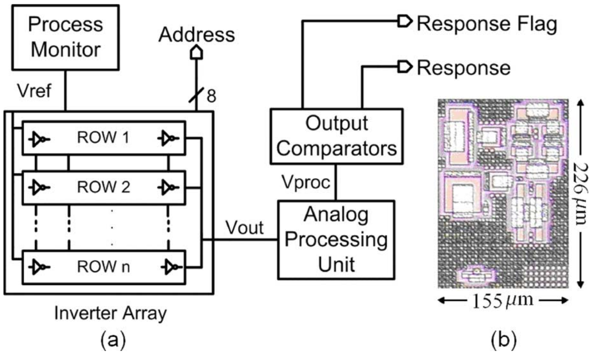


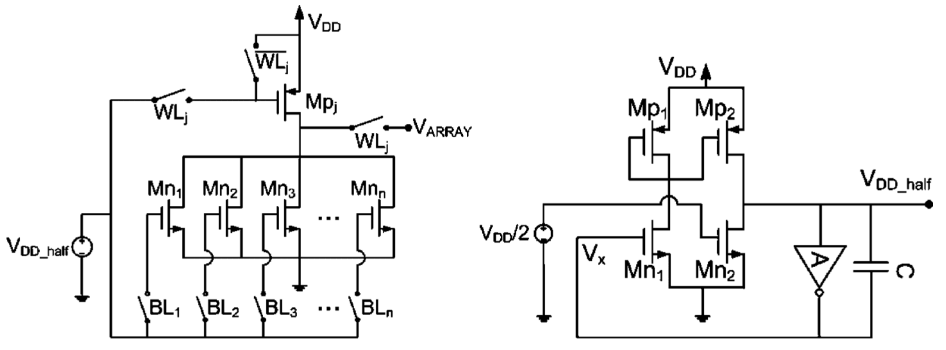
Fig. 1. Block diagram (a) and photo (b) of the nanokey circuit.

II. Circuit

Each bit of the response is obtained as a function of the analog output of a two-dimensional array of inverters biased at the point of maximum gain. The inverters are realized with nMOSFETs of minimum length and width, in order to maximize threshold voltage variability and therefore output voltage dispersion. In order to reduce the power consumption, the inverters are implemented with high threshold voltage MOS transistors. In this way, the inverters of the array work in subthreshold conditions, which does not pose a performance problem because the clock frequency of the circuit is about 1 MHz. In Fig. 1(a) the block diagram of the system is shown. The core of the structure is the two-dimensional array of inverters. The digital challenge is a sequence of N inverter addresses. In general, each response bit is obtained as a function of the analog outputs of M inverters consecutively addressed, implemented by the "Analog Processing Unit" and by the "Output Comparators".

The structure of a single row of the array is shown in Fig. 2(a). Bit lines BL_i are the outputs of the column decoder, wordlines WL_j are the outputs of the row decoder shown in Fig. 1(a). A single pMOSFET is used for each row, in order to reduce the total area occupation on the silicon die. This solution is especially useful if the number N of inverters in the array is large. In fact, in this way, it is possible to obtain N^2 inverters by using only M pMOSFETs. Furthermore, pMOSFETs are large enough to exhibit negligible mismatch in comparison to the minimum sized nMOSFETs, so that they do not introduce a systematic shift of the output voltages on the same row.

In the first and simplest realized prototype [16], we have $\mathrm{M} = 2$ and the Analog Processing Unit is not required, because the response bits are obtained by the difference of consecutive array outputs, performed by the output comparators. This prototype served us to test the concept, the temperature and process compensation circuits, and the ageing properties. However, with $\mathrm{M} = 2$ the nanokey is relatively easy to hack,



(a) (b)

Fig. 2. Structure of a row of the inverter array (a) and schematic view of the process monitor (b).

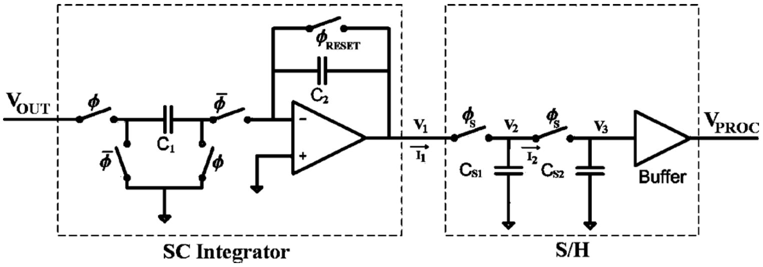


Fig. 3. Analog processing unit.

because the number of trials required for a complete characterization with a brute force attack is $\binom{N}{M}$. Since in the prototype the array consists of $\mathrm{N} = 256$ inverters, in the simplest version ($\mathrm{M} = 2$) the number of uncorrelated CRPs is 32640. There are two ways to increase this number: increasing N or increasing M. Increasing N inevitably causes an increase of the area occupation and power consumption of the circuit. Otherwise, increasing M causes an exponential rise of the number of CRPs increasing the challenge bit-rate and then even the power consumption.

The idea for the second implementation of the nanokey [17] has been to obtain each response bit from the difference between the mean of 8 consecutive array output voltages. In this way $\mathrm{M} = 16$ and the number of uncorrelated CRPs becomes 10^{25}. So, in our case the Analog Processing Unit consists of a Switched-Capacitor integrator followed by a sample and hold circuit (S/H), as shown in Fig. 3. After each group of $\mathrm{M}/2$ array outputs, the integrator output is sampled and reset. With the aim to reduce the effects of the leakage currents, the S/H consists of two stages. Since the leakage currents are a monotonic function of the voltage drop between the input and output of a S/H stage, the undesired variation of V_2 when the switch is off is much smaller than the variation of V_1, and therefore the leakage current I_2 is much smaller than the leakage current I_1, leading to a variation of V_3 much smaller than that of V_2.

Let us describe now the authentication algorithm in the case $\mathrm{M} = 16$: every response bit is obtained by the sign of the difference between consecutive values of the output V_{PROC} of the Analog Processing Unit. So, the response bits can be easily extracted using an autozeroing comparator.

A problem is that a response bit obtained by two almost equal Analog Processing Unit output voltages can easily change, as a result of noise, operating condition variations, or aging. So, a measure to make the response robust and reliable is to identify and exclude from the response validation those bits more likely to change. To this aim a response flag is attached to each response bit upon the first reading, when the challenge-response pair is collected and stored: if the response flag is 1 the bit is marked as unreliable, and is not considered in the validation of the response. The string of response flags is used as a mask to select the valid response bits during an authentication. In the case of $\mathrm{M} = 16$, the response flag is set to one for those bits obtained when the difference ΔV_{PROC} of consecutive Analog Processing Unit outputs is smaller than a quantity that we call V_{DM} or "decision margin". It is important to observe the choice of V_{DM} is a design tradeoff: decreasing V_{DM} results in an increased bit error rate, increasing V_{DM} results in an increased number of bits to be rejected from the response. We will return to this point in Section III-C.

It is important to bias the inverters in the maximum gain region, in order to maximize the inverter output dispersion and to make the output response robust and reproducible in presence of temperature, supply voltage, and process variations. To this aim, the input voltage of the inverters, $\mathrm{V}_{\mathrm{DD\_half}}$, is provided by a Process Monitor (PM) circuit, shown in Fig. 2(b). Exploiting a negative feedback, this circuit guarantees that the mean value of the array output voltages is equal to $V_{\mathrm{DD}}/2$, compensating the effects of process, temperature and voltage supply variations. Instead, the effects of mismatch are unchanged, and that is useful because our circuit exploits local variations for operation. The two pairs of nMOS and pMOS in Fig. 2(b) have a

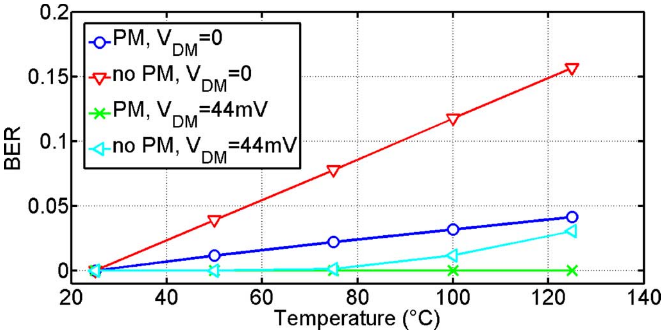


Fig. 4. Effects of the process monitor (PM) and of the decision margin $\mathrm{V_{DM}}$ on the BER.

large size, in order to be mismatch-insensitive, and amplify the differential voltage $(V_X - V_{\mathrm{DD}}/2)$.

The circuit labelled with A in Fig. 2(b) consists of 6 inverters identical to those in the array and connected in parallel. In this way, they are equivalent to a single inverter of the array biased in the gain region, but less sensitive to mismatch. Note that a larger number of inverters in parallel in the circuit A could reduce its sensitiveness to mismatch. On the other hand, since inverters biased in the maximum gain region require a considerable bias current, the circuit A absorbs a significant portion of the power budget, and therefore the number of inverters in A cannot be increased at will.

The operation of the process monitor is the following: if for any reason a change is induced in the value of V_X, the negative feedback of the circuit will compensate it, changing the input voltage V_{DD_half} of the array inverters. So, the voltage V_{DD_half} is regulated in order to keep A in the gain region even if undesired variations occur. Since A works in the maximum gain region, the gain loop of the circuit is high and V_X is very close to $V_{\mathrm{DD}}/2$. The capacitor C of 250 fF allows Miller compensation to achieve loop stability. Given that A exhibits the same process dependence of the nanokey inverters, their average outputs will be compensated with respect to process, temperature, and voltage supply variations.

With the aim to demonstrate the effects of the process monitor and of the decision margin on the BER of the described authentication system, the array output distribution has been simulated at different temperatures. The results have been analyzed for two different values of the decision margin V_{DM} (0 and 44 mV). As shown in Fig. 4, the BER becomes completely negligible if both the process regulator and the described rejection mechanism are used.

In Fig. 1(b) a photo of the nanokey circuit is shown [17]. The area occupation of this circuit is 0.035 mm^2. To keep constant the output bit rate to 6.25 Kb/s, the input bit rate has been increased 8 times with respect to the first implementation and then it is 768 Kb/s.

III. Experimental Results

Two prototype chips have been realized in a standard 90 nm CMOS process. In order to verify the validity of the concept, the performance of the process monitors and of the algorithm based on the decision margin, we have implemented an array with $\mathrm{N} = 256$ inverters using $\mathrm{M} = 2$ (chip P_1) and $\mathrm{M} = 16$ (chip P_2) voltage outputs for the determination of each response bit.

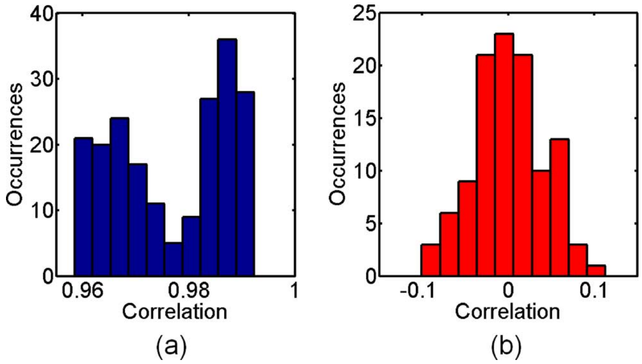


Fig. 5. Experimental distribution of the correlation coefficient between response strings produced by the same chip (a) and by different chips (b) without taking into account the effect of the decision margin.

At room temperature and with supply voltage of 600 mV P_1 and P_2 absorb 30 μW and 38 μW, respectively. Therefore, the increase of power consumption is negligible with respect to the advantages of the second version in terms of security. In this section, the measurements performed in order to show the correct operations of the chip will be described. Moreover, describing the experimental tests, our attention will be focused to highlight the effects due to temperature, voltage supply variations and aging. The purpose of this section will be also to show how the decision margin V_{DM} improves the performance of the chip.

A. Circuit Operation

For authentication, when a single chip is repeatedly tested with the same challenge its response must not change, and the responses of different chips to the same challenge must be uncorrelated. These requirements have been verified in experiments by supplying to a set of 50 different chips the same test challenge of 1800 addresses. In Fig. 5 the distributions of the correlation coefficients between the corresponding response strings produced by the same chip (a) and by different chips (b) are shown. Note that in these graphs the effect of the decision margin is not taken into account, and therefore they have to be considered as the worst case. The presence of erratic bits slightly degrades the correlation coefficient in Fig. 5(a). However, when a decision margin is applied of 44 mV, the correlation coefficient goes to 100%, since all erratic bits are removed from the validation procedure. As can be seen in Fig. 5(b), average correlation between different chip responses is zero.

As previously described, each response bit is obtained by the operation $sign[V_{PROC}(h) - V_{PROC}(k)]$, where h and k are integer number from 1 to 10^{25} and identify two combinations of 8 group of array outputs accessed in succession. One a practical basis, we can choose to have a response bit for each 16 challenge bits, or a response bit for each 8 challenge bits (interlaced response). Experiment show that in the first case, correlation between consecutive response bits is 1.5%, in the second case 34%. The first option therefore requires longer challenges for the same nominal CRP space size, but implies a larger *effective* CRP space.

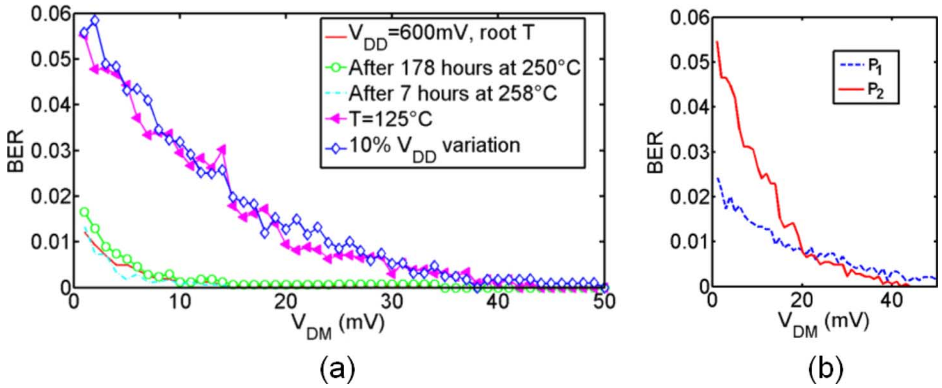


Fig. 6. Experimental BER as a function of the decision margin $V_{\rm DM}$ of the prototype $\rm P_1$ (a) and comparison between prototypes $\rm P_1$ and $\rm P_2$ (b).

Another way to show the correct operation of the chip consists in the estimation of the BER, defined as the error probability of a valid response bit, that is a response bit not discarded in the first reference measurement. By performing measurements for various values of the decision margin $V_{\rm DM}$, the behavior of the BER as a function of $V_{\rm DM}$ has been obtained. As shown in Fig. 6(a), the BER is a decreasing function of $V_{\rm DM}$. Instead, the fraction of non-valid bits in the response increases with $V_{\rm DM}$. Choosing a decision margin of 44 mV, the Bit Rejection Rate is 39.7% and the BER for $V_{\rm DD} = 600$ mV at room temperature is always zero for a challenge of 1800 addresses, i.e., the BER is much lower than 0.009%. As shown in Fig. 6(b), for a decision margin larger than 22 mV, the BER of the second prototype $\rm P_2$ is lower than the BER of the first prototype $\rm P_1$.

B. Aging, Voltage Supply and Temperature Variations

Measurements have been performed also with varying operating conditions. Operating tests have been performed at 125°C or with a 10% voltage supply variation. Although CMOS inverter outputs are strongly dependent on temperature and voltage supply, the process monitor makes the circuit robust to such variations. For $V_{\rm DM} = 44$ mV, in the worst case as far as temperature and voltage supply variations are concerned, the BER is lower than 0.1%, which is a factor 4 lower than the best result presented in literature [14]. For larger $V_{\rm DM}$, the BER can be further suppressed.

Finally, accelerated aging tests have been performed. Circuits with no power supply have been put in an oven and periodically extracted, cycled to room temperature and tested. No observable degradation in their BER has been observed after 178 hours at 250°C, as shown in Fig. 6(a).

We have devised a parameter to evaluate aging of the circuit: $\sigma_{\rm AGING}$ is the standard deviation of the difference between the array output $\Delta V_{\rm ARRAY}$ with respect to the measurement performed before the accelerated aging process. This quantity, ideally zero, is in practice non-zero because of noise and drifts of devices characteristics.

$\sigma_{\rm AGING}$ slowly increases with aging and is 4.9 mV after 178 hours at 250°C. Let us stress that this is an internal indicator of progressive aging even if the circuit still works perfectly without any symptom. At 258°C the same condition is reached after 7 hours. Higher temperatures could not be tested because of the large thermal time constants of the oven. Such a strong temperature dependence is very promising from the point of view of aging in normal operating conditions: if we assume an Arrhenius-type aging process [18], the same degree of aging is reached after a time well in excess of 10 years even at 150°C.

A comparison between our PUFs and those present in the literature is shown in Table I. As can be seen, the BER is lower and the number of trials for a complete brute force attack are much higher than those obtained in the literature.

C. Identification Error Probabilities

There are two important parameters to estimate the performance of a generic authentication system: the *false alarm rate* (FAR), i.e., the probability that an original PUF is not authenticated , and the *false detection rate* (FDR), i.e., the probability that a false PUF is authenticated as the original one. Their expressions are:

$$\mathrm{FAR} = \sum_{i=t+1}^{k_{\rm eff}} \binom{k_{\rm eff}}{i} \mathrm{BER}^i (1-\mathrm{BER})^{k_{\rm eff}-i} \tag{1}$$

$$\mathrm{FDR} = \frac{1}{2^{k_{\rm eff}}} \sum_{i=0}^{t} \binom{k_{\rm eff}}{i} \tag{2}$$

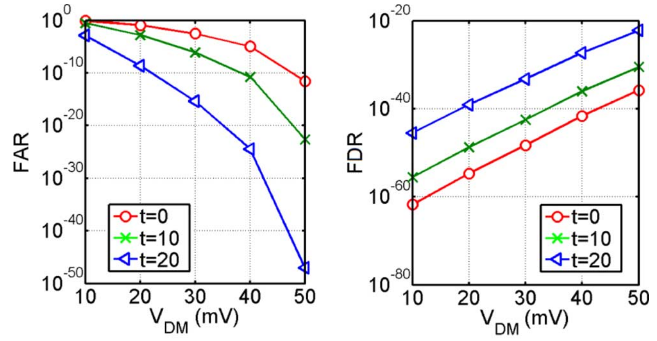
where $k_{\rm eff} = k\,(1 - \mathrm{BRR})$ is the number of valid (i.e., non-rejected) bits in the response, k is the total number of response bits, BRR and BER are the bit rejection rate and the bit error rate, depending on the decision margin, and t is the maximum number of wrong response bits that are tolerated in an authentication.

So, we can obtain the FAR and FDR for our experimental nanokeys as a function of $V_{\rm DM}$, k, and t, where $V_{\rm DM}$ is the reference voltage defined in Section II. In Fig. 7 we show the results for $k = 256$ and for the experimental results with the worst BER (the one measured at 125°C and shown in Fig. 6(a)): let us notice that by increasing t, or by increasing $V_{\rm DM}$, the FDR increases and the FAR decreases. From (1) and (2) it is also clear that by increasing k, the FDR decreases and the FAR increases.

As an optimization of the performance of the authentication system, one could minimize the sum of the two rates FDR and FAR. As can be seen in Fig. 7(b), false rejection rate is always very high for $t = 0$, so it is required that some wrong response bits have to be tolerated in the authentication.

TABLE I
COMPARISON WITH PREVIOUSLY PROPOSED PUFS

	Pappu [8]	**Lofstrom [11]**	**Lee [12]**	**Suh [14]**	**First Prototype [16]**	**Second Prototype [17]**
BER in standard conditions	**< 5%**	**< 1.3%**	**< 0.7%**	**-**	**< 0.01%**	**< 0.009%**
BER in worst conditions	**-**	**< 5%**	**< 4.8%**	**< 0.48%**	**< 0.1%**	**< 0.1%**
Number of trials for brute force attack	**10^6**	**6216**	**1.4x10^{20}**	**523776**	**32640**	**10^{25}**
Technology	**Optical-laser**	**CMOS 0.35 µm**	**TSMC 0.18 µm**	**15 Xilinx Virtex4 LX25 FPGAs (90 nm)**	**STM CMOS 90 nm**	**STM CMOS 90 nm**
Power Dissipation (µW)	**-**	**250-100**	**-**	**-**	**30**	**38**
Area (mm^2)	**-**	**0.023**	**1.47**	**-**	**0.018**	**0.035**



(a) (b)

Fig. 7. Experimental FDR (a) and FAR (b) of the second prototype P_2 as a function of the decision margin and of t. The length of the response (k) is 256.

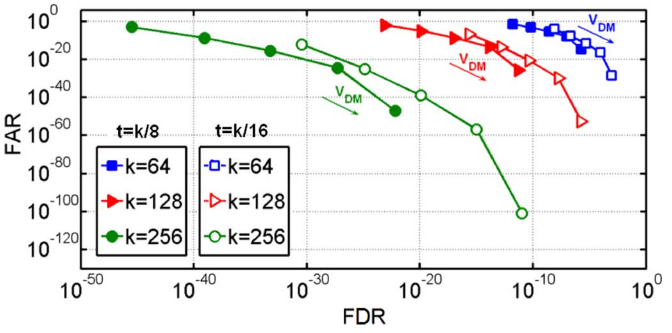


Fig. 8. Experimental receiver operator characteristic (ROC) of the second prototype P_2 at 125°C as a function of the decision margin and of k for $t = k/16$ (empty symbols) and for $t = k/8$ (full symbols).

However, the choice of the parameters t, V_{DM} and k is dependent on the specifications of the authentication system. Choosing a decision margin $V_{\mathrm{DM}} = 44$ mV, both FDR and FAR are lower than 10^{-25}. The apparent tradeoff between FDR and FAR is often represented in a single graph, called the receiver operator characteristic (ROC) and shown in Fig. 8 as a function of the decision margin, for different values of k and $t = k/16$ (empty symbols) and $t = k/8$ (full symbols) .

IV. Resistance to Non-Invasive Attacks

As described in [12], [13], an attack to a PUF can be performed by means of a model-building attack. In the case of our circuit, the knowledge of one response bit can be expressed as an unequality that reduces the space of the possible array outputs. In general, if x is a vector of N real elements containing all the inverter outputs and T is the number of response bits collected by means of measurements on the nanokey, the attack consists in finding a solution x' such that $A'x' > 0$,where $A' \in \Re^{T \times N}$ is a matrix that contains the information of the inverters accessed for each trial. Each row of A' contains $M/2$ elements equal to 1, $M/2$ elements equal to -1 and $N - M$ zeros.

Since the space of possible solutions is limited by a finite number of inequalities, equal to the number of challenge-response pairs obtained during the attack, the number of possible solutions is infinite. One can select the solution that minimizes the error $\varepsilon = \sqrt{\varepsilon_{STD}^2 + \varepsilon_{\mathrm{MEAN}}^2}$, where ε_{STD} and $\varepsilon_{\mathrm{MEAN}}$ are the moduli – respectively – of the difference vectors between the standard deviations and between the mean values of x and x'. In the worst case we assume here, the attacker knows such

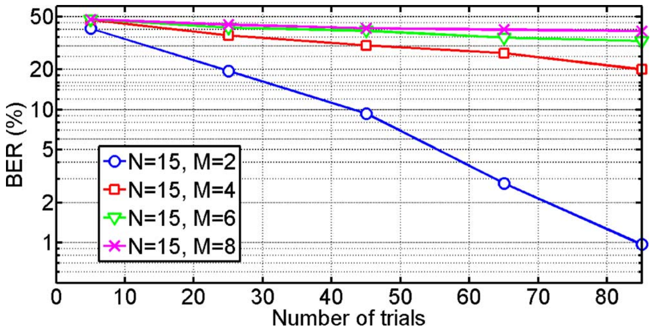


Fig. 9. Simulated BER as a function of the number of trials and M in the case of a model-building attack.

statistical information on the distribution of x, for example because he could perform Monte-Carlo circuit simulations on the original design. Finally, the BER has been estimated on the total amount of possible CRPs. The number of trials to reach a given BER grows with M and N, as shown in Fig. 9.

We have simulated this type of attack at the system level. To reach a BER lower than 0.1% in the case of the first prototype ($\mathrm{N} = 256$, $\mathrm{M} = 2$) 5086 trials have been necessary, that is lower than the number of trials required for a complete brute force attack (32,640). The case of the second prototype is too computationally expensive to simulate. However, the extremely large number of trials required for a complete brute force attack in this version (10^{25}) gives us room to sustain even a significant suppression of trials obtainable with a model-building attack.

Another non-invasive attack is the differential power analysis (DPA) [4]. Theoretically, since the characteristic $I_{\mathrm{DD}}(V_{\mathrm{OUT}})$ has a maximum for $V_{\mathrm{OUT}} = V_{\mathrm{DD}}/2$, it could be possible to obtain information about the output voltages of the inverter array, analyzing the supply current of the nanokey during its operations. In reality, this kind of attacks is used for digital circuits, in which the spikes in current are large. In our case, the variation of power consumption due to the slightly different operating points of the array inverters cannot be easily evaluated. In fact, the standard deviation of the inverter output distribution is very small (about 40 mV) and then also the variation of the current consumption.

V. Conclusion

A circuit for secure authentication, exploiting the intrinsic variability of the electrical characteristics of nanoscale MOS transistors, has been proposed, fabricated and tested in several operating conditions and with accelerated aging. An internal compensation based on a process monitor ensures a very good robustness to process, temperature and voltage supply variations. Moreover, the concept of decision margin for the automatic elimination of the erratic bits of the response in the authentication provides an additional degree of freedom for matching the specifications on authentication performance. Measurements on the proposed IC have shown a 38 μW power consumption and BER lower than 0.009% in standard conditions and lower than 0.1% with operation at 125°C or with a 10% voltage supply variation, which is a factor 4 lower than the best result in the literature [14]. Finally, by performing accelerated aging tests, a lifetime much in excess of the common ten-year requirement at 150°C has been extracted.

Analyzing experimental results, we have shown the possibility to achieve FAR and FDR lower than 10^{-25}. This first prototype used to test the concept and the validity of our proposed solutions contains only $\mathrm{N} = 256$ inverters and each response bit is obtained by $\mathrm{M} = 2$ array outputs, and is therefore vulnerable to brute force attacks (32,640 attacks might be sufficient to fully understand the nanokey operation). The resistance of the nanokey to brute force attacks has been increased increasing M. In fact, in the second prototype $\mathrm{M} = 16$ and the number of trials for a complete brute force attack is 10^{25}. Further improvements can be obtained for larger values of M and N.

References

[1] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Topics in Cryptology – CT RSA 2006*, Berlin, Germany, 2006, pp. 115–131.

[2] D. Molnar, A. Soppera, and D. Wagner, "Privacy for RFID through trusted computing," in *Workshop on Privacy in the Electronic Society*, Alexandria, VA, 2005, pp. 31–34.

[3] R. Anderson and M. Kuhn, "Tamper resistance – A cautionary note," in *Proc. 2nd Usenix Workshop on Electronic Commerce*, Oakland, CA, Nov. 1996, pp. 1–11.

[4] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology*. New York: Springer Verlag, 1999, vol. LNCS 1666, pp. 388–397.

[5] E. Biham and A. Shamir, "Differential fault analysis of secret key crypto systems," presented at the Advances in Cryptology, Crypto'97, Santa Barbara, CA, 1997.

[6] Y. Yousuf and V. Potdar, "A survey of RFID authentication protocols," *Advanced Information Networking and Applications*, pp. 1346–1350, 2008.

[7] S. Skorobogatov and R. Anderson, "Optical fault induction attacks," in *Cryptographic Hardware and Embedded Systems Workshop, CHES 2002*, Heidelberg, Germany, vol. LNCS 2523, pp. 2–12.

[8] R. Pappu, "Physical one-ways functions," Ph.D. dissertation, Massachusetts Inst. Technol., Cambridge, MA, 2001.

[9] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, pp. 2026–2030, 2002.

[10] P. Tuyls, B. Škori, A. H. M. Akkermans, and W. Ophey, "Information-theoretic security analysis of physical uncloneable functions," in *FC'05: Financial Cryptography and Data Security 2005*, pp. 141–155.

[11] K. Lofstrom, W. R. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *IEEE ISSCC Dig.*, 2000, pp. 372–373.

[12] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication application," in *Symp. VLSI Circuits Dig.*, 2004, pp. 176–179.

[13] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijik, and S. Devadas, "Extracting secrete keys from integrated circuits," in *Symp. VLSI Circuits Dig.*, 2005, pp. 1200–1205.

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

[15] Y. Su, J. Holleman, and B. Otis, "A 1.6 pJ/bit 96% stable chip-ID generating circ uit using process variations," in *IEEE ISSCC Dig.*, 2007, pp. 406–407.

[16] D. Puntin, S. Stanzione, and G. Iannaccone, "CMOS unclonable system for secure authentication based on device variability," in *Proc. ESSCIRC 2008*, Edinburgh, Scotland, U.K., Sep. 2008, pp. 130–133.

[17] S. Stanzione and G. Iannaccone, "Silicon physical unclonable function resistant to a 10^{25}-trial brute force attack in 90 nm CMOS," in *Symp. VLSI Circuits 2009 Dig.*, Kyoto, Japan, Jun. 2009, pp. 116–117.

[18] F. H. Reynolds, "Thermally accelerated aging of semiconductor components," *Proc. IEEE*, vol. 62, pp. 185–211, Feb. 1974.

Stefano Stanzione was born on March 16, 1982. He received the Master degree in electrical engineering from the University of Pisa, Italy, in 2006. In 2010, he received the Ph.D. degree from the University of Pisa, working on the design of passive radio frequency identification (RFID) transponders.

He is currently working in IMEC-NL as a researcher on ultra-low-power analog design in energy harvesting applications.

Daniele Puntin received the M.S. degree in electronic engineering from University of Pisa, Italy, in 2005. During his Ph.D. fellowship, his research activity focused on CMOS low-cost and low-power design.

Working as a consultant engineer in Altran Italia, he developed real-time video processing techniques and EMI electronic design solutions and testing. He is currently an officer in the Italian Navy with Lieutenant Junior Grade.

Giuseppe Iannaccone (M'98–SM'10) received the M.S. and Ph.D. degrees in electrical engineering from the University of Pisa in 1992 and 1996, respectively.

He is an Associate Professor of electronics at the University of Pisa, Italy. His interests include the fundamentals of transport and noise in nanoelectronic and mesoscopic devices, the development of device modeling and TCAD tools, and the design of extremely low-power circuits and systems for RFID and ambient intelligence scenarios. He has published more than 140 papers in peer-reviewed journals receiving more than 1100 citations and more than 100 papers in proceedings of international conferences. Prior to joining the University of Pisa in 1996, he was a researcher with the Italian National Research Council.

Prof. Iannaccone has coordinated several European and National Projects involving multiple partners and has acted as the Principal Investigator in several research projects funded by public agencies at the European and National levels and by private organizations. He acts as a reviewer for several funding agencies in Europe and is or has been on the technical committee of several international conferences in the field of semiconductor technology and design. His website is: www.iannaccone.org.