# Physical Unclonable Functions based on Crossbar Arrays for Cryptographic Applications

Paolo Lugli[1], Ahmed Mahmoud[1], György Csaba[2], Michael Algasinger[3], Martin Stutzmann[3], and Ulrich Rührmair[4,5]

[1]Institut für Nanoelectronics, Technische Universität München, Arcisstrasse 21, 80333 München, Germany
[2]Center for Nano Science and Technology, University of Notre Dame, Notre Dame, IN 46556 USA
[3]Walter Schottky Institut, Technische Universität München, Am Coulombwall 3, 85748 Garching, Germany
[4]Institut für Sicherheit in der Informationstechnik, Technische Universität München, Arcisstrasse 21, 80333 München, Germany
[5]Fraunhofer SIT, Am Parkring 4, 85748 Garching, Germany

**Abstract.** Due to their attractive, regular structure and their simple implementation, crossbar arrays have become one major emerging research area in the fields of nano-devices and electronic circuits. This paper discusses novel applications of crossbars as various types of so-called physical unclonable functions (PUFs) in the field of physical cryptography. The latter is a recent branch of cryptography and security that exploits the inherent, small-scale randomness and disorder in physical structures. PUFs are the currently dominant primitive within this new field. In order to establish the applicability of crossbar structures as PUFs, two crossbars with rectifying junctions are investigated on the basis of real measurement data. In addition, the scalability of these crossbars with respect to their power dissipation and noise margin is evaluated in simulations. The types of PUFs as which crossbars can serve include Weak PUFs and Super High Information Content (SHIC) PUFs. We also discuss whether crossbar-based PUFs allow the erasure and/or re-writing of response information on a single CRP level, i.e., without affecting other PUF-responses.

**KEY WORDS**: Crossbars, ZnO Schottky junction, ALILE crystallization process, physical cryptography, physical unclonable functions (PUFs), SHIC PUFs

## 1 Introduction

As semiconductor technologies approach the end of the roadmap, researchers focus on improving energy efficiency and area consumption to create future information technologies [1]. Crossbar arrays are in principle very well aligned with these goals: Due to their highly regular architecture, they are considered to be the simplest functional electrical circuits, allowing manufacture at the very resolution limits of available nanofabrication methods. Recent work by Green et al., for example, realized crossbar array with a bit density of $10^{11} cm^{-2}$. This means a scale down in size of roughly 37 times compared to the current state of the art in DRAMs [2]. In addition, crossbar architectures are expected to allow a promising reduction in energy consumption due to their potential for nano-scale fabrication [1]. Nevertheless, accessing a single cell within a very large passive crossbar array is accompanied with sneak current paths and crosstalk with neighboring cells, which may hinder arbitrary scaling of the array sizes. Among other things, this paper thus investigates the scalability of passive crossbar arrays consisting of low cost, highly rectifying junctions, which are suited to diminish crosstalk and sneak current paths.

Electronic communication and security devices are pervasive in our life. Just to name two examples, around five billion mobile phones are currently in use worldwide [3, 4], and the world market of chipcards has an estimated volume of three billion pieces per year [5, 6]. Their widespread use makes such devices and tokens a well accessible and, at the same time, a worthwhile target for attackers.

In many cases, hostile attacks on said systems are not directed against the numeric cryptoprimitives which they use, such as the employed encryption schemes, digital signature schemes, or hash functions [7, 8]. Instead, fraudsters can apply malware (such as viruses and Trojan horses) or physical methods in order to extract the secret keys that are contained in the systems. Indeed this method has been applied successfully many times against widespread commercial systems [8–10]. This drives the search for new cryptographic and security mechanisms that can protect secret keys in vulnerable hardware systems.

The recent field of physical cryptography (PhC) addresses the above (and other) issues by exploiting the effects of small scale, random, uncontrollable manufacturing variations in hardware systems. One central topic from PhC are so-called Physical Unclonable Functions or PUFs (see Section 2.3). PhC has developed very rapidly in recent years, with the optimal hardware realization of PUFs with respect to security, costs, and area consumption being one central research topic. This paper hence investigates if and how crossbar arrays based can be used as PUFs with very high information density and low power consumption. In doing so, it builds an unexpected bridge between two hot research topics in the fields of nanoscience on the one hand and cryptography and security on the other hand.

The paper is organized as follows. Section 2 provides some background information about crossbars, physical cryptography and memristors. In section 3, two crossbars with rectifying junctions are analyzed, based on real devices' measurements. In section 4, novel applications of crossbars in the field of physical cryptography, are presented. In addition, different properties of crossbars are analyzed to confirm their applicability in the proposed cryptographic applications.

## 2 Basic Concepts

### 2.1 Crossbar Arrays

*Structure and Manufacture Implementation* Crossbar arrays gained a lot of attention over the last few years due to their attractive small sizing and simple implementation. They are considered to be the simplest functional electrical circuits. In a nutshell, a crossbar array consists of sets of horizontal and vertical parallel metal wires (see figure 1). Schematically, one can describe a crossbar cell as a bistable element characterized by two level of resistances, $R_{on}$ and $R_{off}$, corresponding respectively to the low and high conductance states of the junction. The layer between the crossing wires is

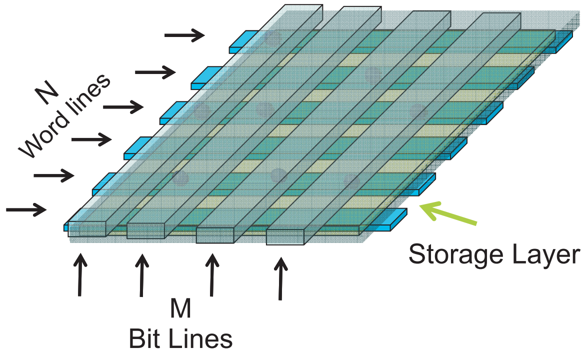

**Fig. 1.** The typical architecture of an $N \times M$ Crossbar array for non-volatile memories

in general nonlinear resistors. Its electric characteristics determine the behavior of the crossbar and its electronic functionality. Crossbar arrays are generally passive circuits with no amplifying/signal restoring components [11]. For any application, crossbars should be fully compatible with silicon technology so that they can be fabricated as a post-process on the top of CMOS circuits, which would provide the electronic control functions.

Crossbar arrays are mostly intended to be used as memories that would require much less space than the current available memories [2, 12]. In addition, logic applications using crossbar arrays have been proposed in [13, 14]. Recently, our group proposed to use crossbars for applications related to cryptography and security [15, 16]. This topic is discussed in this paper.

*Biasing Schemes.* Figure 2 shows three general biasing schemes for crossbar arrays. In all schemes, an input voltage supply is applied to the accessed word line and a current measuring meter is connected to the accessed bit line. These biasing schemes are valid for both reading and writing of the memory bits, yet usually higher input voltages are used in writing. The first scheme is the floating scheme where all the un-accessed bit/word lines are left floating. The second scheme is a single supply biasing scheme where all un-accessed bit/word lines are biased at voltage $V_b$. When $V_b = 0$, it is called "grounded scheme". The third scheme is a double supply biasing scheme where all un-accessed word lines are biased at voltage $V_{b1}$ and all un-accessed bit lines are biased at voltage $V_{b2}$. When $V_{b1}$ and $V_{b2}$ have a reversed values to that of the accessed junction, it is called "reverse biasing scheme". It is worth noting that, when $V_{b1}$ and $V_{b2}$ are equal, the double supply biasing scheme is the same as the single supply biasing scheme.

*Circuit Models.* Crossbar architectures are ideal candidate for very high integration thanks to their simple topology. It is therefore important to study the scalability of crossbar arrays. For this purpose, approximate equivalent circuit models are necessary to allow the computationally efficient simulation of the crossbars for large circuit sizes. Each cell stores "0" or "1", which corresponds to resistance $R_{off}$ or $R_{on}$, respectively.

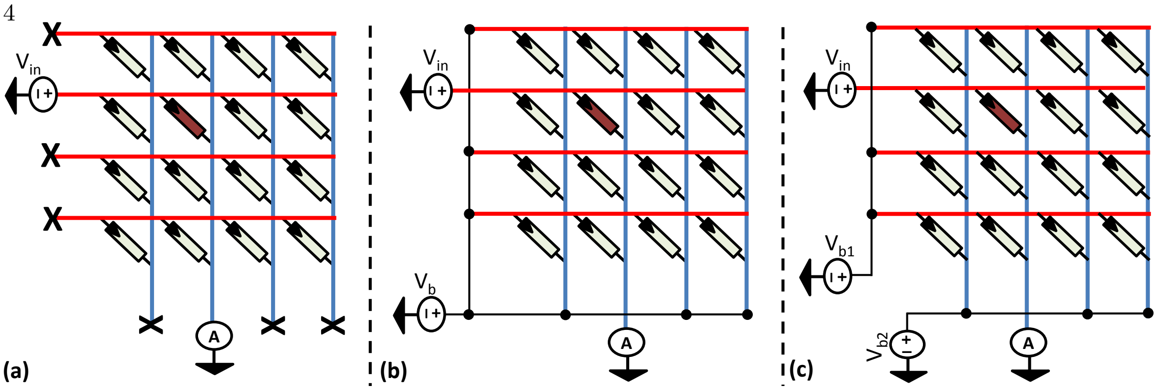

**Fig. 2.** The three general biasing schemes for crossbar arrays.(a) floating scheme (b) single supply biasing scheme (c) double supply biasing scheme

In the circuit performance evaluation, maximum entropy in the array is assumed, which corresponds to an equal number of stored 0s and 1s in random positions.

Since most of the simplification in the crossbar circuit is due to parallel junctions, it is assumed a new general resistance R which has an average $IV$ characteristic of the $R_{off}$ and $R_{on}$. This means that two parallel $R$ have the same $IV$ characteristic of $R_{off}$ parallel to $R_{on}$ (in symbols $R_{off}$ // $R_{on}$).

$$\begin{aligned} R \;//\; R &= R_{off} \;//\; R_{on} \\ R &= 2 \cdot (R_{off} \;//\; R_{on}) \end{aligned} \tag{1}$$

Note that, R can take any other value according to the requirement from the simulation, e.g. simulating worst case conditions where the number of stored 0s and 1s are not equal but their ratio is constantly distributed through the array. Moreover, the direction of the junction was left, in order to keep the circuit models general for any type of junction, e.g. when having a rectifying junction the direction is very important. Figures 3 and 4 show the approximate circuit models for floating scheme and the double supply biasing scheme, respectively. The resistance of the accessed junction called $R_j$ which differ from the general $R$.

In the floating scheme, each un-accessed junction connected to the accessed word line would have a leakage path to the accessed bit line. The leakage path that could be found is first to path through each junction connected to the same bit line but in reverse direction, then path through the un-accessed junctions connected to the accessed bit line (see fig. 3). It is assumed an equal potential for all un-accessed word lines, which is a valid approximation if the ratio of 1s and 0s is constantly distributed as stated earlier when we calculated $R$. This was verified by comparing the approximated circuit model with the complete crossbar circuit elements up to 300 × 300 junctions, whence it is supposed to work even better for larger array size.

Any $N$ parallel junctions can be replaced by an equivalent junction with a resistance equals $R/N$. However, for serial junctions, the equivalent junction resistance is not computed since the junctions generally may have nonlinear $IV$ characteristics. In step 3, in order to replace the $(N-1)$ equal branches without wrong approximation, just one branch is employed to ensure the correct $IV$ characteristic over it. Afterwards, a current dependent current source, which simulates the remaining $(N-2)$ branches, is connected parallel to the employed branch to generate $(N-2)$ times the current in the employed branch.

In the double biasing scheme, since each junction is biased with two supply voltages, all junctions with the same bias are considered to be parallel (see fig. 4). These parallel junctions are replaced by equivalent junctions in the same way described for the floating bias.

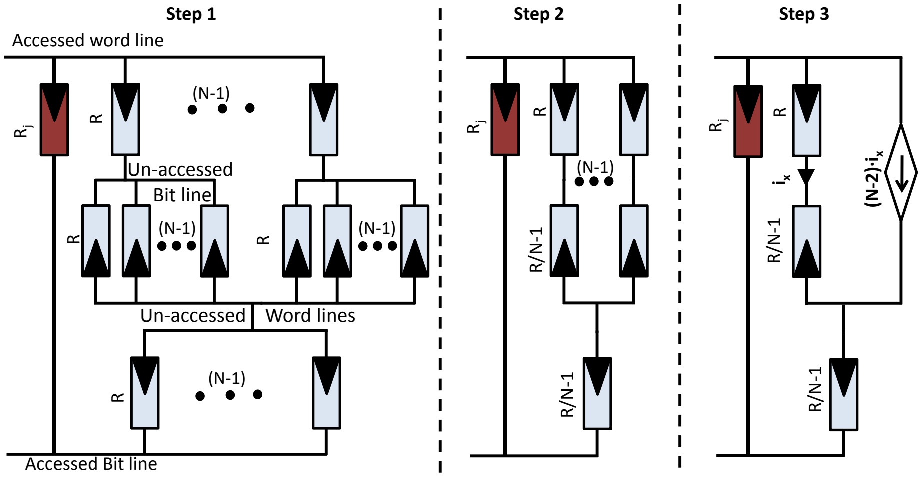

**Fig. 3.** The derivation of the approximate circuit model for a floating biasing scheme. Note that, equal potential is assumed for the un-accessed word lines since based on experiments, for large array size with high entropy equal voltage would stabilize at these lines.

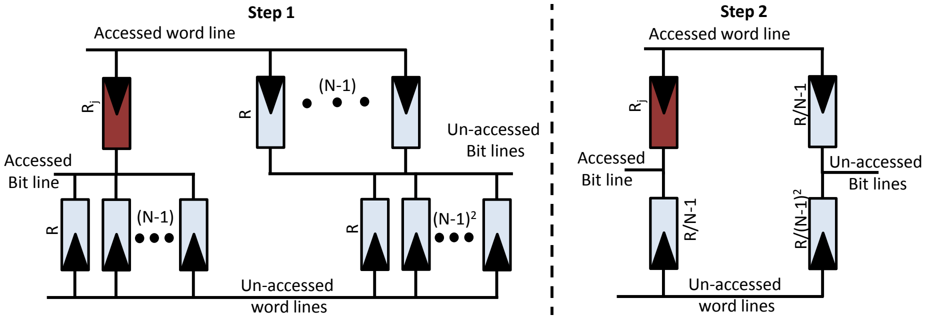

**Fig. 4.** The derivation of the approximate circuit model for the double supply biasing scheme

These circuit models are just approximate because we neglect the wire resistances, the supply resistance and the resistance of the current measuring device. These resistances might become critical when the crossbar is fabricated at the nano-scale.

The main parameters of the crossbars which are studied using the crossbar circuits' simulation are the power dissipation and the noise margin. The power dissipation is calculated as the total power dissipated from the voltage supplies. The noise margin ($N_M$) is calculated as the relative difference between the current reading of the junction in the on and off states, as:

$$N_M = \frac{1}{2} \cdot \frac{I_{on} - I_{off}}{I_{on} + I_{off}} \quad , \tag{2}$$

where $I_{on}$ and $I_{off}$ are the current flowing through the accessed junction when it is in the on-state and off-state, respectively.

Note that for all the crossbar circuit simulations presented in this paper, the dimension of the junction is scaled down to $100 \times 100\ nm^2$. This is in order to provide the expected results of the crossbar in the nano-scale, which is the target for a dense integration.

## 2.2 Memristors

Memristors (resistive switches) were discovered by Chua in 1971 [17]. They are considered as the fourth lumped circuit element besides resistors, capacitors and inductors. A memristor can be seen as a two terminal device whose resistance depends on the history of current and voltage over the device. The $IV$ characteristics show a hysteresis which is a direct indication of such memory effect. Recently, memristors were built using transition metal oxides with highly doped oxygen vacancies in the upper part which provide a relative high conductivity like that of semiconductors [18]. Nevertheless, the lower part is almost free of oxygen vacancies to keep the insulating property of the oxide at this portion. This dominates a high resistance over the whole device.

On applying a threshold biasing voltage across the structure some vacancies from the upper part will move to the lower part as well. Consequently, the overall resistance across the structure will be reduced. Conversely, on applying a reverse threshold voltage, the vacancies in the lower part will escape back again, whence the overall resistance becomes high again [19].

Molecular junctions also showed very similar behavior of memristors [18, 20]. Such memristor element can be incorporated into the crossbar architecture to provide the storing elements. Hence, the state of the memristor being at high/low resistive state would determine its logic state "0"/"1".

## 2.3 Physical Cryptography

As mentioned in the introduction, physical cryptography is a recent form of cryptography and security which explicitly exploits the hardware-intrinsic, nanometer-scale randomness in circuits and other devices. Two aspired goals are to avoid the storage of secret keys in vulnerable hardware, and to evade the usual unproven computational assumptions that are omnipresent in classical cryptography. There are a large number of different concepts or so-called "primitives" within physical cryptography [21] [22], with one central concept being so-called Physical Unclonable Functions (PUFs).

In general, a PUF is a (partly) disordered physical system $S$ that can be challenged with so-called external stimuli or challenges $C_i$, upon which it reacts with corresponding responses $R_{C_i}$. These responses shall depend on the applied challenge and on the structural disorder which is present in the PUF. It is usually assumed that this small-scale disorder cannot be controlled or reproduced exactly, not even by the PUF's original manufacturer, and is unique to each PUF. Furthermore, the responses are assumed to be stable upon multiple measurements. The dependence of the PUF-responses on the disorder in the PUF is a notable feature; it is contrary to the design of most digital electronic systems and circuits, in which the inevitable manufacturing variations shall deliberately not affect the input-output behavior.

There are several subtypes of PUFs, each possessing its own security features and applications; two extensive surveys are provided in [21, 22]. Two central PUF types are Weak PUFs and Super High Information Content (SHIC) PUFs, whose implementation via crossbars is going to be discussed in this paper.

*Weak PUFs.* Weak PUFs are the conceptually simplest form of PUFs. They may have very few challenges — in the extreme case just one, fixed challenge. Their response(s) $R_{C_i}$ are used to derive a standard digital secret key, which is subsequently processed by the embedding system in the usual fashion, e.g., as a secret input for some cryptoscheme. Contrary to SHIC PUFs (see below), the responses of a Weak PUF are never meant to be given directly to the outside world. They are not freely accessible for external parties once the device has been released to the field, but are supposed to remain secret and inside the security system.

Weak PUFs thus are nothing else than a special type of non-volatile memory (NVM). Their advantage is that they may be harder to read out invasively with respect to NVM, due to their intrinsic disordered features. Furthermore, their responses (from which the secret key is derived) may depend sensitively upon the state of the surrounding layers in the hardware. This can provide Weak PUFs with some natural form of tamper sensitivity: Removal and/or perforation of their surroundings usually alters their response forever, which automatically disables recovering of the original key by the attacker. Another advantage of Weak PUFs compared to NVM is that they may save process steps during production, thus cutting on costs. They can also be used for key storage in hardware systems which (for one reason or the other) do not allow or contain NVMs.

One typical implementation example of a Weak PUFs is the so-called SRAM PUF [23–25], in which the "random" binary content (0 or 1) of SRAM cells after power-up is used as a source of random key bits. The content depends on random manufacturing variations and thus varies from cell to cell, but is relatively stable for each cell in many power-ups. Moreover, simple semiconductor elements like diodes have been suggested as Weak PUFs in [16, 26].

*SHIC PUFs.* A Super High Information Content PUF must contain a very large amount of information or entropy, with typical values reaching up to $10^{10}$ bits of information, and a correspondingly large number of possible challenges. The information can only be read out only at an inherently limited, relatively slow rate (typical values are around $10^2 - 10^4$ bits per second). Even though the challenges of a SHIC PUF can be applied and the responses can be read out freely by everyone who has got physical access to the PUF, a full characterization in short time should be practically infeasible due to the large number of possible challenges and the slow read-out speed.

More specifically, the properties of a SHIC PUF are as follows.

1. A SHIC PUF contains an extraordinarily high amount of response-relevant random information and have a very high information density (values suggested in [15] are $10^{10}$ extractable bits contained in around 1 $\text{cm}^2$).
2. The read-out speed of a SHIC PUF (i.e. the frequency by which it produces responses) is limited to low values (typical values suggested in [15] are $10^2-10^4$ bits per second). This speed limitation should be an inherent property of the PUF's design and its physical properties. Faster read-out attempts should be impossible or should overload and destroy the structure.
3. A SHIC PUF must have a very large number of challenges. Together with the slow read-out speed, this shall prevent the full read-out/characterization of the PUF in short time, even though the challenges and responses are freely accessible to an adversary.
4. The challenge-response-pairs (CRPs) of a SHIC PUF are mutually independent, i.e., the pairwise mutual information of any two responses of theirs is zero.

One natural application of SHIC PUFs are PUF-based identification schemes (compare [27]). They are usually run between a central authority (CA) and a hardware system carrying a (unique) SHIC PUF $S$. One assumes that the CA had earlier access to S, and could establish a large, secret list of CRPs of $S$. Whenever the hardware wants to identify itself to the CA at some later point in time, the CA selects some CRPs at random from this list, and sends the challenges contained in these CRPs to the hardware. The hardware applies these challenges to $S$, and sends the obtained responses to the CA. If these responses match the pre-recorded responses in the CRP-list, the CA believes the identity of the hardware.

One advantage of the above scheme is that it avoids the storage of secret digital keys in (potentially vulnerable) NVM. Another upside is that it evades the usual unproven assumptions (such as the assumed hardness of the factoring and discrete logarithm problem) in the identification protocol. Finally, it exacerbates the need for computationally costly execution of asymmetric cryptographic protocols in low-cost mobile devices. Other known applications of SHIC PUFs cover key establishment (similar to the protocols in [27, 28] for Strong PUFs), authentication, as well as two-player protocols like oblivious transfer [29]. It has been argued already in [15] that SHIC PUFs can be constructed very well on the basis of large, monolithic crossbar arrays. This approach is further developed in this paper.

*Erasing and Re-Writing Information in PUFs.* With the protocols and applications of PUFs getting more complex, a recently emerging topic is if the value of a single response can be erased from a PUF, or deliberately altered ("written") into a PUF, without altering any other responses [30]. This question arises as the same PUF may be used in many protocols and possibly by many parties succesively. If a secret key has been derived from PUF responses by two parties in an earlier protocol, they would like to prevent that future holders of the PUF can derive the same key by reading out the same responses. For the example of PUF-based session key exchange protocols, this issue has been discussed in all detail in [30].

Unfortunately, it turns out that erasure of responses at a single CRP level is difficult to achieve with many currently existing Strong PUF architectures (see [21, 22] for an overview), in which many components interact and jointly generate a response: In order to change one response, at least one component needs to be altered; but this single new component will then change many responses, not just one. The situation is different for crossbar-based SHIC PUFs and Weak PUFs, however, as we will argue in this paper, since each response arises from an independent, spatially isolated cross point.

## 3 Scalable Crossbar Arrays with Rectifying Junctions

Crossbars were initially suggested to be used with molecular junctions in order to continue the scaling trends predicted by Moore's law [31]. The array size scaling of this approach was found to be limited, since the noise margin and the power dissipation degrade rapidly with increasing the size due to sneak current paths [2, 11].

It was thus suggested to add a rectifying element in order to mitigate the crosstalk and leakage paths between accessed and un-accessed cells. Implementing a molecular rectifier is still a challenging research goal [32]. Hence, we consider here building a crossbar with a 1D-1R junction, that is, a diode in series with a memristor. The state of the memristor determines the value of the corresponding bit.

If a diode with excellent rectification ratio could be used, there would not be any problem with the scaling of the size of the memory with respect to the power dissipation or the noise margin using the floating or reverse bias scheme. Although Silicon diodes could provide such performance over other diodes. Nevertheless, Si processes are not compatible with the transition metal oxides of standard memristors [33]. In addition, the high temperature required for their fabrication prevents their integration with CMOS in the post-processing steps.

## 3.1 Crossbars with ZnO-based Schottky Junctions

In [34], ZnO-based Schottky junctions were used as the rectifying elements, in building the crossbar, with NiO based-switching memory elements. It was suggested to use Ag interface with the ZnO diode to provide a better performance [35]. A rectification ratio of $10^8$ was recorded using the mentioned diode structure at $\pm 2\,\mathrm{V}$ [34]. Moreover, the investigated NiO based memristor recorded an on/off ratio around 1000 [34]. Figure 5 shows the measuremental $IV$ characteristics of the ZnO Schottky diode and the NiO memristor, respectively. One of the main advantages of the investigated ZnO diode and NiO memristor, is the low fabrication temperature around $100°C$.

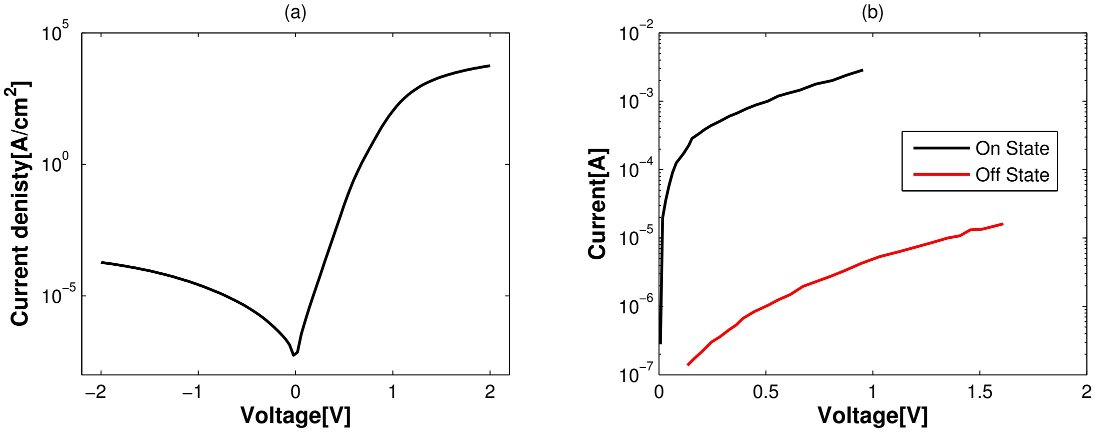

**Fig. 5.** Measurement data adopted from [34]. (a)The measurment of a typical J-V characteristics of a $6 \times 6$ $\mu m^2$ ZnO Schottky diode which composed of (Ti-Au)/ZnO/Ag layers. (b)The measurement of a typical $IV$ characteristics of a $6 \times 6$ $\mu m^2$ NiO memristor which composed of Au/NiO/Au layers

Assuming the floating bias scheme, the noise margin is reduced quadratically with the increase in the size of the memory. This is because the values of the sneak current mainly depends on the current through the reverse junctions demonstrated in the circuit model. Thus, as the size of the memory increases the sneak currents increase quadratically and they are added to the final reading current. As a result, the noise margin is reduced. According to the simulation results, the memory size, employing the floating scheme, would be limited to few Mbits due to the reduction in the noise margin (see fig. 6a). Moreover, the power dissipation also increases almost quadratically with the size of the memory, since the power dissipated in the sneak paths is mainly dependent on the current through the reverse junctions.

After examining other schemes, it was found that the reverse biasing scheme provides the optimum performance for both the noise margin and power consumption. Ideally, the noise margin, employing the reverse biasing scheme, should not be affected by the memory size scaling since no sneak paths contribute in reading (see fig. 6b). Regarding the power dissipation, it increases quadratically with the memory size but at a little higher value compared to the floating bias because the complete voltage

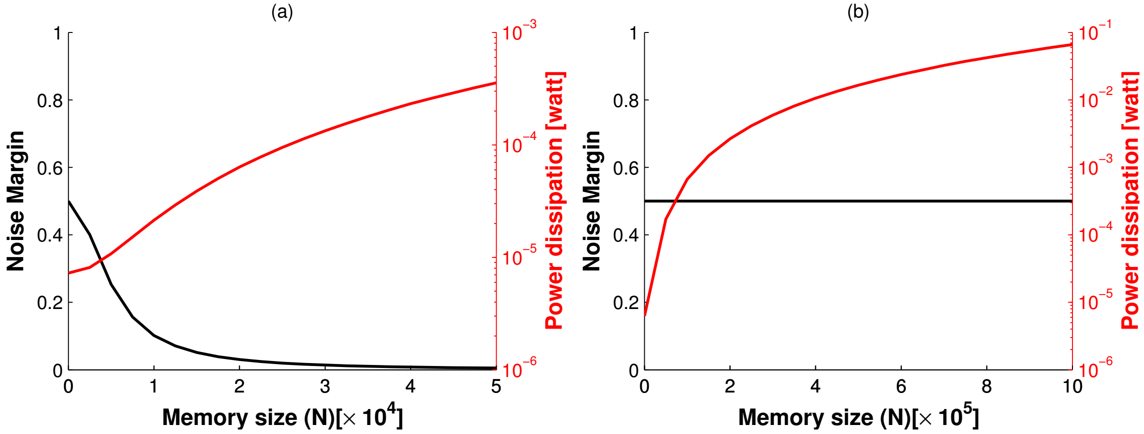

**Fig. 6.** (a)The effect of scaling the memory size, employing the floating scheme, on the noise margin and the total power dispation. (b)The effect of scaling the memory size, employing the reverse bias scheme, on the noise margin and the total power dissipation. The simulation is done using LTSpice on the model of an isolated ZnO-based Schottky diode connected to NiO based-switching memory element.

is dropped over the reverse junctions which means higher off current values. Hence, at $N = 10^4$ we shall have power dissipation of $(10^8 \cdot I_{reverse})$ which is equal to the power dissipated in the accessed cell, assuming rectification ratio of $(= 10^8)$.Thus, a 100 Mbit memory could be built using this junction structure in the presence of power constrain, yet unlimited size is still possible -from the noise margin point- if there is no constrain are given on the power consumption.

**External Resistances Effects** The noise margin of the reverse biased scheme is kept ideal because we assume a negligible resistance for the power supply and the current measuring device. In reality the noise margin would also degrade with increasing the memory size, since the reading current from the accessed cell is branched, when the equivalent resistance of the reverse diodes is comparable to the resistance of the measuring device. The effect of changing the value of the measuring device's resistance on limiting the maximum array size of the crossbar was investigated based on a minimum noise margin of 0.35. It was found that for the measuring device's resistance of $10\,\Omega$, $100\,\Omega$, $1\,\mathrm{K}\Omega$ and $10\,\mathrm{K}\Omega$, the maximum array sizes of the crossbar are $1.15 \cdot 10^5$, $4 \cdot 10^4$, $1.5 \cdot 10^4$ and $10^4$, respectively. These values depend also on the technology scale, since as the devices scale down not only the diode's current is reduced but also thinner wires -higher resistances- would be acquired by the measuring device. Hence, memory scaling is highly dependent on the layout of the crossbar and its input/output circuitry.

Such resistances have almost no effect on the simulation of the floating scheme. These resistances just reduce the voltage drop over the accessed junction, whence the noise margin is barely affected.

One interesting point to note is that the total power dissipation is also affected by the increase of the resistance value, since it limits the maximum current that can follow in the circuit. To illustrate that, assume we have resistance (R) connected in series with parallel diodes. Regardless to the $IV$ characteristic of the diodes, the maximum current that can follow in such circuit would be smaller than ($V_{dd}/R$) if almost the whole voltage drop is over the resistance. Hence, after certain increase in the resistance, the power dissipation saturates but the noise margin is dramatically affected.

### 3.2 Crossbars with ALILE Junctions

A crystallization process called Aluminum-Induced Layer Exchange (ALILE) provides some interesting properties for the diodes built using it to be employed in crossbars for physical cryptography applications. ALILE has been intensively investigated since 1990s [36]. It is a crystallization process for polycrystalline silicon where a substrate of Aluminum/Aluminum-oxide/Amorphous silicon layer stack is annealed at high temperatures. This results in a complete layer exchange between aluminum and silicon layers. In addition, a random grain structure is generated because of the impurities and the structural defects which act as crystallization regions [16]. In [16], it was found that for a weakly doped wafer, the diodes produced with ALILE have high rectification ratios reach up to $2 \cdot 10^7$. In addition, there is a high randomness in the diodes characteristics due to the large grain sizes. This randomness significantly increases with decreasing the diode's dimensions. Normally, IC designers would like to have fixed characteristics for the devices employed, yet in physical cryptography applications, randomness is highly appreciable.

Figure 7a (adopted from [26]) shows the $IV$ characteristic of 12 different diodes within the same wafer. As can be noted the difference in the on-current spreads over more than 2 orders of magnitude.

Unlike crossbar with ZnO Schottky junction, no memristor is employed to store the value of each junction. The applications of crossbars with ALILE junctions are discussed in the next section. Figure 7b shows the effect of scaling the crossbar size on both the noise margin and the power dissipation using the reverse bias scheme. As can be noted, similar results to that of the crossbar with ZnO Schottky diode, are obtained. Nevertheless, there are some degradation in the noise margin, since the rectification ratio of ALILE diode is less than that of the ZnO Schottky diode.

## 4 Crossbars as Physical Unclonable Functions

We will now discuss the application of crossbar arrays as Weak PUFs and SHIC PUFs, respectively, as well as erasing and rewriting information in these PUFs on a single CRP level.

### 4.1 Crossbar as Weak PUFs

It is suggestive to use one or more small-size crossbar arrays of ALILE diodes as a Weak PUF [26]. Due to manufacturing variations, in particular due to random

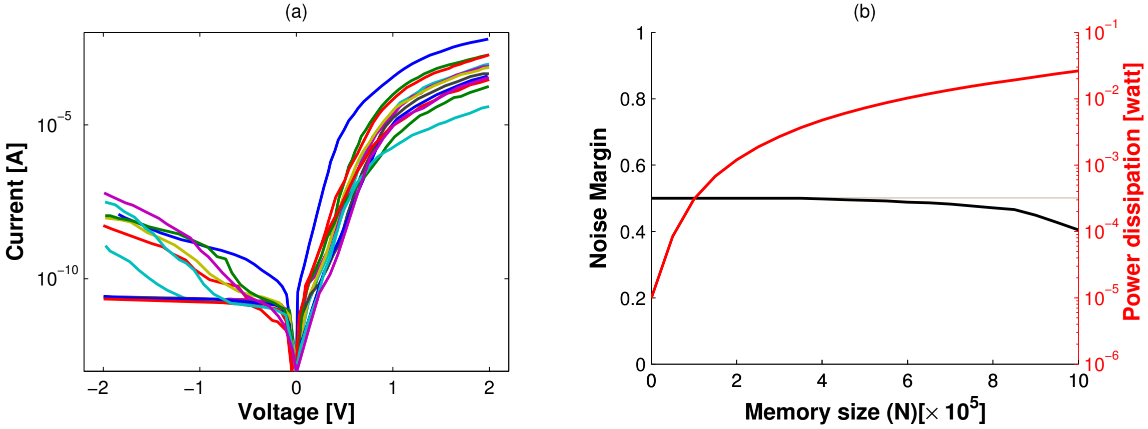

**Fig. 7.** (a)The $IV$ characteristics for different diodes of the same dimensions $10\times10\mu\text{m}^2$ and on the same wafer fabricated with ALILE process, adopted from [26]. (b)The effect of scaling the memory size, employing the reverse bias scheme, on the noise margin and the total power dissipation. Models of the ALILE diodes with the highest and lowest forward current where employed as the on and off junctions, for simulating the crossbar circuit.

crystallization phenomena in the ALILE process, each of these diodes has a random, distinct current-voltage characteristic. This curve strongly varies from diode to diode in up to four orders of magnitude, as shown in Fig. 7a. At the same time, the curve of each single diode is very stable against aging and multiple measurement [16, 26]. Using appropriate error correction methods, a few bits (typically around three bits) can be extracted reliably from each single diode [26]. The security of the diodes against invasive read-outs seems relatively high. At the very least, the random structure and disorder that determines the random $IV$ curves is hidden inside the diodes at the p-n-junction, where it seems hard to access without destroying the entire structure, which would in itself render its characteristics unreadable and unrecoverable.

ZnO-based Schottky probably are not well suited as Weak PUFs, since the differences in fabrication from diode to diode presumably are not large enough.

*Stability against Aging and Environmental Conditions.* The described ALILE diodes are known to be very stable against aging and multiple read-out [26, 16, 15]. However, it is known that the $IV$ characteristics of diodes in general depend on the temperature (see fig. 8). In order to mitigate the stability problem that would arise due to this temperature dependence, it was suggested to measure the intended diode characteristic with respect to a reference diode [16], since the same temperature dependence is expected for all diodes. Another solution would be a differential output reading which is realized by measuring two different diodes at a time to express one bit value. If the first diode has higher current reading, a stored bit equals to “1” is assumed otherwise “0” is assumed. Furthermore, error correcting code (ECC) circuits are usually employed in the post-processing of the cryptography process in order to tolerate some

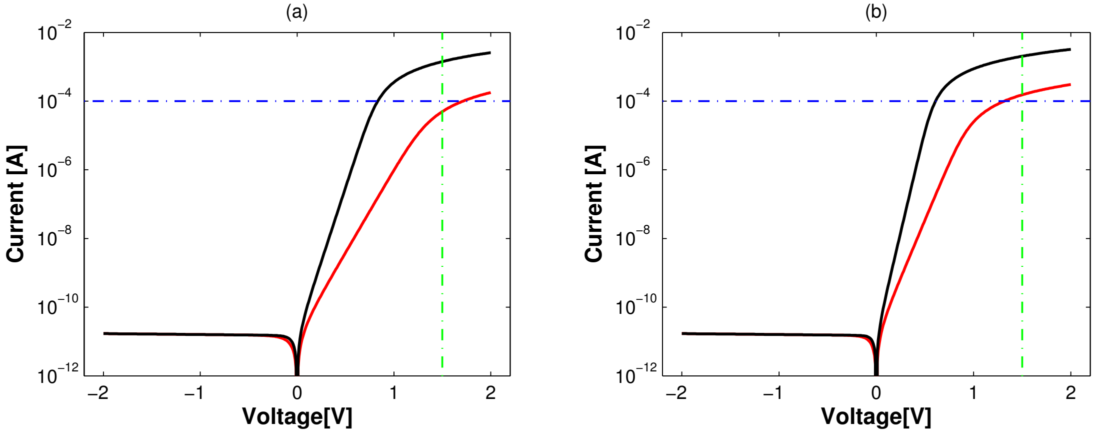

**Fig. 8.** The temperature effect on stability. The figures are the $IV$ characteristics of two models of diodes, at temperature difference $100°C$. Assuming a measuring voltage=1.5 V and $I_{th}$=$10^{-4}$ A, in case (a) the second diode is assumed to be off, yet in case (b) it is read as on. If differential reading is employed, the current of the first diode is higher in both temperatures. In addition, small variation in the measuring voltage would still provide the correct result.

percentage of reading error. Thus, the crossbar with ALILE diodes could provide a robust physical cryptography device.

*Erasing and Rewriting Information.* We now investigate if – and how – information can be erased from Crossbar PUFs. Since the information is contained in the diode current-voltage characteristics, any erasure operation must target the diodes, changing their $IV$-curves irreversibly. The "erasure operation" works as follows. A specific diode in the crossbar array is chosen by selecting the corresponding bit and word lines of the crossbar structure, similar to the read-out procedure for the crossbars. Then a short voltage pulse of 4 V to 5 V is applied in reverse direction to the diode. This induces a breakdown in the ALILE diode, which destroys the individual information present in the $IV$ curve, and makes all curves after erasure "standardized" and very similar in shape.

This effect has been observed by us in *all measured diodes*; three illustrative examples for $IV$-curves before and after breakdown are shown in Fig. 9. While the large variations in the original curves range over four orders of magnitude, there is little individuality left after breakdown, and the curves after breakdown also differ strongly from the original curves. Considering the development of the relative positions of the curves over the full voltage range shows that not even the relative positioning of the curves is preserved. In other words, the information in the curves is reliably and irrecoverably erased.

The fact that the new curves are uncorrelated to the old ones is a consequence of the physical effect behind the breakdown of the diodes. Our explanation of this mechanism is the presence of a thin natural oxide film between the p- and n-layers, effectively resulting in a p-i-n-structure. Such an additional i-layer would strongly

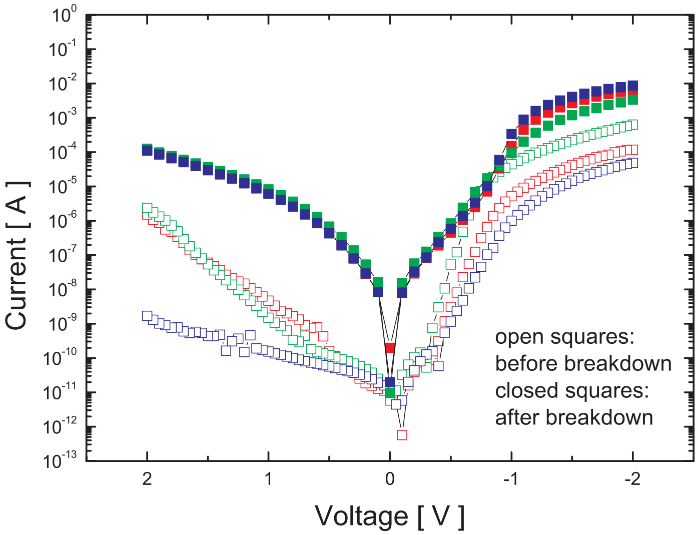

**Fig. 9.** The curves of three exemplary diodes (red, blue and green) before and after breakdown, adopted from [30]

reduce the tunneling current in reverse direction (as observed by us), which otherwise had to be expected to be high due to the large hole carrier concentration in the ALILE layers (up to $10^{19}$ $\mathrm{cm}^{-3}$) [16]. The assumption of an intermediate oxide layer is further supported by the fact that diodes which were exposed to hydrofluoric acid (HF) vapor prior to the deposition of the ALILE layers *did not show* comparable rectification rates; the HF vapor is known to remove Si-oxide, leading to a destruction of the possible p-i-n -structure [16]. The described voltage pulse in reverse direction then simply burns and removes this i-layer.

### 4.2 Crossbars as SHIC PUFs

As mentioned previously, another physical cryptography application of large, scalable crossbar arrays are so-called SHIC PUFs. They can be implemented by using a crossbar array whose junction are ALILE diodes. The high rectification rates of these diodes of up to $2 \cdot 10^7$ allow very large and scalable crossbar arrays.

*Transient Analysis and Slow Read-Out Speed.* The transient properties of a crossbar-based SHIC PUF are of paramount importance. In common memory applications of crossbars, a high read-out speed is desirable: the faster, the better. This is not the case for SHIC PUFs. One main property of SHIC PUFs is, in fact, that it should be impossible to read the whole device content through (i.e., all CRPs) in short time. To ensure this, the read-out of each bit needs to be slow, and it should be impossible for adversaries to speed up the read-out procedure. Typically aspired read-out speeds of SHIC PUFs should be around $10^2$ to $10^4$ per second.

In general, the time constant for reading a single bit in a crossbar memory, with reverse biasing for un-accessed word/bit lines, can be calculated as:

$$\tau = (R_{supply} + R_{wireW} + R_{wireB} + R_{junction}) \cdot (C_W + C_B + C_{interW} + C_{interB}) \quad (3)$$

$R_{supply}$ is the resistance due to wiring to the supply voltage and the measuring device, $R_{junction}$ is the junction resistance, $R_{wireW}$ and $R_{wireB}$ are the resistance due to the accessed word and bit line respectively. $C_W$ and $C_B$ are the capacitance due to the reverse bias junction connected to the accessed word and bit line respectively, hence $C_W = C_B = (N-1) \cdot C_{junction}$. $C_{interW}$ and $C_{interB}$ are the inter-wire capacitance between the accessed word/bit line and the neighboring un-accessed word/bit lines, respectively.

The employed technology scale determines the wire resistances which usually do not contribute with large percentage in the overall resistance. Nevertheless, the wire dimensions determine the value of the maximum current that can pass through the wires in addition it has a great influence on $R_{supply}$ since connections to outer decoder/encoder circuits have to go down to this scale. For normal crossbar memories application, the junction resistance should dominate the total resistance so that the voltage drop is mostly over the active layer to reduce the power dissipation and the reading time. However, in SHIC application the wires are suggested to force high resistance for the $R_{supply}$ in order to provide slow reading [15]. Moreover, fuses may be employed to limit the maximum current that can pass through the wires in order to prevent parallel reading of different junctions.

Regarding the capacitances, in standard crossbar memory applications the junction capacitance is dominant, since a low $k$ material is used to achieve small reading time. To the contrary, in SHIC PUF applications high $k$ materials would be employed in order to intentionally slow down the read-out speed [15]. Some materials based on NiO doped with Li/Al and Ti provide particularly high electric permittivity of up to $(\epsilon_r \approx 10^4 - 10^5)$ [37, 38]. Such materials would potentially be suited for SHIC PUFs, even though their practical compatibility with standard crossbar processes still needs to be investigated experimentally.

To give some rough estimation for the slow reading time value, assume $10^5 \times 10^5$ crossbar array is built in a nano-scale process. The overall resistance would be in the range of several $M\Omega$ and the overall capacitance of the crossbar using the high k material shall be in the range of several pF . Hence, we could end up with a reading rate of about 1000 bit/sec. This would mean to read the whole $10^{10}$ bit memory, more than 3 years of continuous reading is required. Hence, with this slow reading, crossbars can be used to realize SHIC devices. Similarly, crossbars with the NiO memristor in series with ZnO diode can be used to realize reconfigurable and erasable PUFs.

*Security against Invasive and Modeling Attacks.* It is interesting to examine which attack possibilities remain for a well-equipped attacker on the described crossbar-based SHIC PUFs. First of all, crossbar-based SHIC PUFs are naturally immune against so-called modeling attacks [39], which currently constitute the most dangerous attacks on many known PUF architectures. In these attacks, an adversary collects a large set of CRPs of a PUF, and then tries to extrapolate other PUF-CRPs from the known CRPs. Modeling attacks are not applicable to any SHIC PUFs, however, since their CRPs are all pairwise independent in an information theoretic sense.

Furthermore, under the provision that they operate at the desired low read-out speeds, a full read-out of the SHIC PUF in short time is also impossible. A natural option for an attacker would hence be to accelerate the read-out speed of a crossbar SHIC PUF. However, this speed is not a property of an artificially slow access module, which could potentially be cut off or circumvented. It is a transient property of the design of a crossbar SHIC PUF itself. Any faster read-out would require higher voltages, and they would hence overload and destroy the wires (see Section 4.2 and [15]).

An alternative possibility might be to read out the value of the bits invasively or by microscopic techniques, potentially allowing parallel read-out of the structure at many crosspoints. However, the random and secret configuration of each diode is kept in the inner layers of the device. This makes it difficult to access it without destryoing the structure. Furthermore, invasive access to the wiring next to each crosspoints seems extremely difficult, since the crossbars can be fabricated at the current resolution limits of nanofabrication due to their very simple structure.

A final, rather hypothetic approach would be to replace or strengthen the crosspoint interconnects so that the crossbar wiring can survive high currents without burning. This would allow faster read-out speeds. The approach could be realized either by using thicker metal layer or using metal that has higher conductivity (e.g. gold) to replace the thin interconnects. If fuses were used, a complete rerouting could be employed to avoid the fuses and allow direct contacts. This attack would require immense time and cost investment, and formidable nanofabrication capabilities. It seems slightly fictional, especially if the crossbar was fabricated at the limits of current nanofabrication methods. Nevertheless, even this approach can be thwarted if the SHIC crossbar is fabricated in such a way that also the wires themselves have unique and varying current-voltage characteristics, which affect the IV curves of the diodes at the crosspoints. This has already been observed in [16].

*Stability against Aging and Environmental Conditions.* For crossbars with ALILE diodes, the same arguments apply as in the corresponding paragraph of Section 4.1. With respect to crossbars with NiO memristor in series with ZnO diode, the value of each bit would depend only on the state of the memristor. This is normally stable regardless to any environmental or electrical variation. This is because only high threshold voltage would change the value of the bit, whence no accidental change is expected to any of the memory bits without intention. Consequently, using a high capacitive crossbar with rectifying junction, in general, can be used robustly for the SHIC PUF applications.

*Erasing and Rewriting Information.* ALILE-based SHIC PUFs allow an erasure of operation according to the same principles as described in Section 4.1. However, the rectification rates of the diodes after the erasure operation are strongly reduced, as can be observed from Fig. 9. Another problem is that the on current of the diodes after erasure is about equal to the off current of the diodes before erasure. The presence of many "erased" diodes in the crossbar hence creates parasitic paths in the large, monolithic crossbar arrays, diminishing their read-out accuracy and functionality. The described method hence is only suited for a limited number of erasure operations within the PUF.

In order to allow a SHIC-like PUF that allows an arbitrary number of erase and write operations, crossbars based on NiO with ZnO Schottky diodes can be used. The diodes in such a material system do not show large fabrication variations, and the content of all cells after fabrication is zero. Nevertheless, one could assume that each SHIC-like PUF is defined by a comparably small set of random bits (say $10^4 - 10^6$ bits), which are spread randomly by write operations within the huge memory. Only these valid bits would be known and written by the CA in the example identification protocol of Section 2.3. After reading any of these valid bits, it would be is possible to erase this bit by rewriting another value to it without affecting the remaining bits. Note that a complete reconfiguration of all bits would not possible in our case due to the inherited slow writing.

## 5 Conclusion

In this paper, we investigated crossbar arrays and their use as physical unclonable functions (PUFs) in the field of physical cryptography. We started by giving some background on crossbar arrays, memristors and physical cryptography. We then presented general approximated circuits equivalent for different biasing schemes of crossbar arrays. These circuits allowed the computationally efficient simulation of crossbar arrays of large sizes. Afterwards, real measurement results for low-cost, highly rectifying junctions required for scalable crossbar arrays were given. The effect of scaling the crossbar size, on both the noise margin and the power dissipation, was investigated for different biasing schemes based on the real device measurements. Finally, we argued that crossbar arrays are good candidate for different physical cryptography applications. We suggested that small arrays of ALILE diodes can be used as Weak PUFs, and that very large, monolithic crossbars with ALILE or ZnO diodes are suited as SHIC PUFs. We further addressed if and how single responses can be erased or deliberately changed ("re-written") in crossbar PUFs. Such erasure or re-writing can become necessary in several PUF-based protocols in order to make previously exploited CRP information inaccessible for future holders of the PUF.

Our work builds an interesting bridge between two recently emerging and strongly developing scientific fields, nanocircuits on the one hand and cryptography and security on the other hand. We expect that many other nanotechnologies could, in principle, be used advantageously in cryptography and security applications. The necessary requirements in security applications (such as slow read-out speed or maximal fabrication variation) may even lead to new, fascinating design parameters for nanoscientists, making the mutual transfer of concepts beneficial for both disciplines. We therefore expect strong activity in this interdisciplinary field in the upcoming years.

## Acknowledgements

This work was partially supported by TUM International Graduate School for Science and Engineering and by the TUM Institute of Advanced Study.

## References

1. E. Linn, R. Rosezin, C. Kügeler, and R. Waser, “Complementary resistive switches for passive nanocrossbar memories,” *Nature Materials*, vol. 9, no. 5, pp. 403–406, 2010, DOI:10.1038/NMAT2748.
2. J. Green, J. Choi, A. Boukai, Y. Bunimovich, E. Johnston-Halperin, E. DeIonno, Y. Luo, B. Sheriff, K. Xu, Y. Shin *et al.*, “A 160-kilobit molecular electronic memory patterned at 1011 bits per square centimetre,” *Nature*, vol. 445, no. 7126, pp. 414–417, 2007, DOI:10.1038/nature05462.
3. “http://www.cbsnews.com/stories/2010/02/15/business/main6209772.shtml.”
4. “http://www.bbc.co.uk/news/10569081.”
5. “http://www.eurosmart.com/images/doc/Eurosmart-in-the-press/2006/ cardtechnologytoday_dec2006.pdf .”
6. “http://www.gsaietsemiconductorforum.com/2010/delegate/documents/ GASSELGSALondon20100518presented.pdf. Slide 23.”
7. B. Schneier and P. Sutherland, *Applied cryptography: protocols, algorithms, and source code in C.* John Wiley & Sons, Inc. New York, NY, USA, 1995, DOI:10.1.1.116.9117.
8. R. Anderson, *Security Engineering: A guide to building dependable distributed systems.* Wiley Publishing, 2008.
9. T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. Shalmani, “On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme,” *Advances in Cryptology–CRYPTO 2008*, pp. 203–220, 2008, DOI:10.1007/978-3-540-85174-5_12.
10. T. Kasper, M. Silbermann, and C. Paar, “All you can eat or breaking a real-world contactless payment system,” *Financial Cryptography and Data Security*, pp. 343–350, 2010, DOI:10.1007/978-3-642-14577-3_28.
11. G. Csaba and P. Lugli, “Read-out design rules for molecular crossbar architectures,” *Nanotechnology, IEEE Transactions on*, vol. 8, no. 3, pp. 369–374, 2009, DOI:10.1109/TNANO.2008.2010343.
12. S. Jo, K. Kim, and W. Lu, “High-density crossbar arrays based on a Si memristive system,” *Nano letters*, vol. 9, no. 2, pp. 870–874, 2009, DOI:10.1021/nl8037689.
13. Y. Chen, G. Jung, D. Ohlberg, X. Li, D. Stewart, J. Jeppesen, K. Nielsen, J. Stoddart, and R. Williams, “Nanoscale molecular-switch crossbar circuits,” *Nanotechnology*, vol. 14, p. 462, 2003, DOI:10.1088/0957-4484/14/4/311.
14. M. Ziegler and M. Stan, “CMOS/nano co-design for crossbar-based molecular electronic systems,” *Nanotechnology, IEEE Transactions on*, vol. 2, no. 4, pp. 217–230, 2004, DOI:10.1109/TNANO.2003.820804.
15. U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, and G. Csaba, “Applications of high-capacity crossbar memories in cryptography,” *Nanotechnology, IEEE Transactions on*, vol. 10, no. 3, p. 489, 2011.
16. C. Jaeger, M. Algasinger, U. Rührmair, G. Csaba, and M. Stutzmann, “Random pn-junctions for physical cryptography,” *Applied Physics Letters*, vol. 96, p. 172103, 2010, DOI:10.1063/1.3396186.
17. L. Chua, “Memristor-The Missing Circuit Element,” *IEEE Transactions on Circuit Theory*, 1971, DOI:10.1109/TCT.1971.1083337.

18. D. Strukov, G. Snider, D. Stewart, and R. Williams, "The missing memristor found," *Nature*, vol. 453, no. 7191, pp. 80–83, 2008, DOI:10.1038/nature06932.
19. D. Niu, Y. Chen, and Y. Xie, "Low-power dual-element memristor based memory design," in *Proceedings of the 16th ACM/IEEE international symposium on Low power electronics and design.* ACM, 2010, pp. 25–30, DOI:10.1145/1840845.1840851.
20. L. Chua, "Nonlinear circuit foundations for nanodevices, Part I: The four-element torus," *Proceedings of the IEEE*, vol. 91, no. 11, pp. 1830–1859, 2003, DOI:10.1109/JPROC.2003.818319.
21. R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," *Towards Hardware-Intrinsic Security*, pp. 3–37, 2010, DOI:10.1007/978-3-642-14452-3_1.
22. U. Rührmair, S. Devadas, and F. Koushanfar, "Security based on physical unclonability and disorder," in *Introduction to Hardware Security and Trust, M. Tehranipoor and C. Wang (ed.), Springer*, 2011, to appear.
23. D. Holcomb, W. Burleson, and K. Fu, "Initial sram state as a fingerprint and source of true random numbers for rfid tags," in *Proceedings of the Conference on RFID Security.* Citeseer, 2007.
24. ——, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, pp. 1198–1210, 2008, DOI:10.1109/TC.2008.212.
25. J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," *Cryptographic Hardware and Embedded Systems-CHES 2007*, pp. 63–80, 2007, DOI:10.1007/978-3-540-74735-2_5.
26. U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba, and M. Stutzmann, "Security applications of diodes with unique current-voltage characteristics," *Financial Cryptography and Data Security*, pp. 328–335, 2010, DOI:10.1007/978-3-642-14577-3_26.
27. R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, p. 2026, 2002, DOI:10.1126/science.1074376.
28. P. Tuyls and B. Škorić, "Strong authentication with physical unclonable functions," *Security, Privacy, and Trust in Modern Data Management*, pp. 133–148, 2007, DOI:10.1007/978-3-540-69861-6_10.
29. U. Rührmair, "Oblivious transfer based on physical unclonable functions," *Trust and Trustworthy Computing*, pp. 430–440, 2010, DOI:10.1007/978-3-642-13869-0_31.
30. U. Rührmair, C. Jaeger, and M. Algasinger, "An Attack on PUF-based Session Key Exchange, and a Hardware-based Countermeasure: Erasable PUFs," *Financial Cryptography and Data Security.*
31. W. Wu, G. Jung, D. Olynick, J. Straznicky, Z. Li, X. Li, D. Ohlberg, Y. Chen, S. Wang, J. Liddle *et al.*, "One-kilobit cross-bar molecular memory circuits at 30-nm half-pitch fabricated by nanoimprint lithography," *Applied Physics A: Materials Science & Processing*, vol. 80, no. 6, pp. 1173–1178, 2005.
32. K. Stokbro, J. Taylor, and M. Brandbyge, "Do Aviram- Ratner Diodes Rectify?" *J. Am. Chem. Soc*, vol. 125, no. 13, pp. 3674–3675, 2003, DOI:10.1021/ja028229x.
33. G. Kim, K. Kim, J. Seok, H. Lee, D. Cho, J. Han, and C. Hwang, "A theoretical model for Schottky diodes for excluding the sneak current in cross bar array resistive memory," *Nanotechnology*, vol. 21, p. 385202, 2010, DOI:10.1088/0957-4484/21/38/385202.
34. G. Tallarida, N. Huby, B. Kutrzeba-Kotowska, S. Spiga, M. Arcari, G. Csaba, P. Lugli, A. Redaelli, and R. Bez, "Low temperature rectifying junctions for crossbar non-volatile memory devices," in *Memory Workshop, 2009. IMW'09. IEEE International.* IEEE, 2009, pp. 1–3, DOI:10.1109/IMW.2009.5090598.
35. N. Huby, G. Tallarida, M. Kutrzeba, S. Ferrari, E. Guziewicz, L. Wachnicki, and M. Godlewski, "New selector based on zinc oxide grown by low temperature atomic layer deposition for vertically stacked non-volatile memory devices," *Microelectronic Engineering*, vol. 85, no. 12, pp. 2442–2444, 2008, DOI:10.1016/j.mee.2008.07.016.
36. O. Nast, T. Puzzer, L. Koschier, A. Sproul, and S. Wenham, "Aluminum-induced crystallization of amorphous silicon on glass substrates above and below the eutectic temperature," *Applied Physics Letters*, vol. 73, p. 3214, 1998, DOI:10.1063/1.122722.
37. J. Wu, C. Nan, Y. Lin, and Y. Deng, "Giant dielectric permittivity observed in Li and Ti doped NiO," *Physical review letters*, vol. 89, no. 21, p. 217601, 2002, DOI:10.1103/PhysRevLett.89.217601.
38. Y. Lin, J. Wang, L. Jiang, Y. Chen, and C. Nan, "High permittivity Li and Al doped NiO ceramics," *Applied Physics Letters*, vol. 85, p. 5664, 2004, DOI:.1063/1.1827937.
39. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security.* ACM, 2010, pp. 237–249, DOI:10.1145/1866307.1866335.