Applications of High-Capacity Crossbar Memories in Cryptography

Ulrich Rührmair, Christian Jaeger, Matthias Bator, Martin Stutzmann, Paolo Lugli, *Senior Member, IEEE*, and György Csaba

***Abstract*—This paper proposes a new approach for the construction of highly secure physical unclonable functions (PUFs). Instead of using systems with medium information content and high readout rates, we suggest to maximize the information content of the PUF while strongly reducing its readout frequency. We show that special, passive crossbar arrays with a very large random information content and inherently limited readout speed are suited to implement our approach. They can conceal sensitive information over long time periods and can be made secure against invasive physical attacks. To support our feasibility study, circuit-level simulations and experimental data are presented. Our design allows the first PUFs that are secure against computationally unrestricted adversaries, and which remain so in the face of weeks or even years of uninterrupted adversarial access. We term the new design principle a *"SHIC PUF,"* where the acronym SHIC stands for super high information content.**

***Index Terms*—Crossbar memories, nonvolatile memories, physical cryptography, physical unclonable function (PUF).**

I. Introduction

PHYSICAL unclonable functions (PUFs) are emerging as a new, powerful approach to cryptography and security applications [1]–[7]. Ideally, the security of a PUF should stem from the physical irreproducibility (or uniqueness) and the internal complexity of micro- or nanoscale physical systems. It should be based on the hard technological limitations and the formidable costs related to characterizing and remanufacturing physical objects with nanoscale precision. Contrary to the largest part of mathematical cryptography, its security should not depend on the computational power of the adversary, and should ideally not be vulnerable against the development of more efficient breaking algorithms or increasingly powerful computers.

Historically, the first PUFs were optical systems [1], which exhibited complex internal behavior and high structural information content, but required sensitive and expensive readout machinery. One much discussed recent possibility is to build on-chip PUFs from integrated electrical circuits [2], [3]. For example, the individual, subnanosecond delays between units of an readout machinery can carry a signature that is unique to each circuit. Nevertheless, it turns out that many of the currently suggested PUF circuits can be machine-learned [4], [5] in order to model their behavior. This allows the construction of an imitation device that behaves indistinguishably from the original circuit and which breaks its security.

It can be argued that most of the so far proposed architectures suffer from a common problem: the quantity of structural information that is effectively extracted from the object is too low to fully rule out machine learning or other algorithmic attacks. For the currently known circuit implementations, the "useful" amount of information is on the order of a few parameters (some real numbers with a limited precision) per circuit block, with the number of blocks being on the order of several hundred. For the entire circuit, the relevant information content is, therefore, presumably less than 1 kB. Optical PUFs [1] hold more structural information, but not dramatically: the number of scattering particles used in [1] is on the order of 10^5, even if the speckle pattern is very sensitive to their precise location. Due to these facts, the security of current PUF implementations is in principle susceptible to algorithmic attacks just as mathematical cryptography, and eventually rests on unproven computational complexity assumptions too.

In this paper, we propose a different approach to physical cryptography: we suggest circuits that maximize the effectively extractable structural information content of a physical system while drastically reducing the readout speed. We term this new concept a *"SHIC PUF"* (pronounce as "chique PUF"), where SHIC stands for super high information content. It allows the design of PUFs that remain secure over very long time periods, and which are naturally immune against any algorithmic attacks, including any machine-learning techniques. Their security can even withstand attackers with unlimited computational power. At the same time, the reduced readout speed does not restrict their usability in many relevant applications such as key exchange or credit cards.

Manuscript received July 9, 2009; revised February 8, 2010; accepted April 4, 2010. Date of publication May 3, 2010; date of current version May 11, 2011. This work was supported by the International Graduate School of Science and Engineering, the Institute for Advanced Study, Technische Universität München, and the VERSATILE Project. The review of this paper was arranged by Associate Editor D. Hammerstrom.

U. Rührmair is with the Computer Science Department, Technische Universität München, Munich D-80333, Germany (e-mail: ruehrmai@in.tum.de).

C. Jaeger and M. Stutzmann are with the Walter Schottky Institute, Technische Universität München, Munich D-80333, Germany (e-mail: christian.jaeger@wsi.tum.de; stutz@wsi.tum.de).

M. Bator was with the Walter Schottky Institute, Technische Universität München, Munich D-80333, Germany. He is now with the Paul Scherrer Institute, 5232 Villigen PSI, Switzerland (e-mail: Matthias.Bator@wsi.tum.de).

P. Lugli is with the Institute for Nanoelectronics, Technische Universität München, Munich D-80333, Germany (e-mail: lugli@tum.de).

G. Csaba was with the Institute for Nanoelectronics, Technische Universität München, Munich D-80333, Germany. He is now with the University of Notre Dame, Notre Dame, IN 46556 USA (e-mail: gcsaba@nd.edu).

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/TNANO.2010.2049367

Since memory circuits are naturally optimized to densely hold a large amount of information, it is straightforward to think of a specially designed memory as a promising way to implement SHIC PUFs. Indeed, we show that suitably designed solid-state memories can serve very well for that purposes.

The paper is organized as follows: the reader is provided with background on PUFs in Section II. The special requirements for a memory that can be used as a SHIC PUF are given in Section III. We argue in Section IV that passive crossbar memories represent the solution with highest security and lowest cost for a 2-D IC technology. In Section V, we show that with realistic device characteristics the readout from the crossbar will work reliably, and Section VI demonstrates that the crossbar can be made as slow as desired. Section VII outlines some specific material systems and realization possibilities. In Section VIII, we discuss preliminary experimental results. Section IX discusses a few implementation variants and the eventual limits of our approach. We summarize our study in Section X.

II. State of the Art on PUFs

A PUF is a physical system that maps challenges C_i to responses R_{C_i}, and which meets the following security feature: even if an adversary Eve (E) has unrestricted access to the PUF for a limited time period t, and even if Eve is provided with a large number of challenge-response pairs (C_i, R_{C_i}) of the system, it must still be impossible for her to fully characterize, learn, or understand the behavior of the system. After access to the PUF has been withdrawn, Eve should have a relatively low chance of predicting the correct response R_{C_i} to a randomly chosen, earlier unknown challenge C_i. Eve's actions during access are not restricted to determining as many standard challenge-response pairs (C_i, R_{C_i}) as possible, but she can perform arbitrary physical measurements on the system. This concept has at times also been referred to as a Strong PUF [8]; we use both expressions synonymously in this manuscript.

A simple and illustrative PUF-based cryptographic protocol that can be used for the identification of hardware systems or other entities is the following: in a presetting phase, a central authority CA measures some randomly selected (C_i, R_{C_i}) pairs of the PUF, and stores them in a secret list. Subsequently, the PUF is embedded in a hardware system S, or on a personal security token, and is released to the field. If the system S later wants to identify itself, the CA chooses some earlier measured challenges C_i at random, and sends them to S. If S answers with the correct responses R_{C_i}, then the CA can be certain that she is indeed communicating with S.

Typically, only a very small subset of the possible (C_i, R_{C_i}) pairs is used for the secret list of the CA and in the communication of the CA and the device. In contrast, the adversary E must know all (or almost all) possible (C_i, R_{C_i}) pairs in order to falsely claim ownership of the PUF. This is due to the fact that E has no way of knowing, which are the C_i challenges that the CA uses for testing.

The advantage of the described protocol is that it avoids the storage of digital keys in hardware systems, where they often be readout easily by invasive, side channel, or virus attacks. It also obviates the execution of computationally intensive asymmetric cryptoschemes in mobile device, since the security of the aforementioned scheme is built solely on the high challenge-response complexity of the PUF.

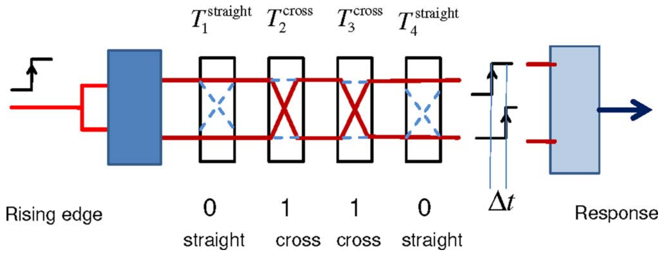


Fig. 1. Illustration of the arbiter PUF.

The first concrete implementation of a PUF was proposed in [1] and consists of an optical token with a very large number of randomly distributed light scatterers. A laser beam directed toward the token creates an interference pattern on a subsequent screen. One usually regards the angle and point incidence of the laser beam as the challenge C_i of this PUF, while the interference pattern (or a suitably chosen image transformation of it) is interpreted as the response R_{C_i}. The described PUF offers quite high internal complexity and security, but it is also quite impractical, with its readout apparatus being external, large, expensive, and sensitive to perturbations.

One important integrated, electrical example is the so-called arbiter PUF illustrated in Fig. 1. It consists of a sequence of k multiplexers, which are conditioned by a sequence of external bits $X[1], \ldots, X[k]$ [2], [3]. The incoming signal is split into two signals, which race against each other on two paths that are determined by the values of the $X[i]$. At the end of the structure, an "arbiter" consisting of a latch determines whether the top or bottom path arrived first, and correspondingly outputs a zero or a one. The arbiter PUF thus maps a k-bit input challenge $C_i = X[1], \ldots, X[k]$ to a 1-bit response R_{C_i}. Unfortunately, the effectively extracted information content is relatively low, and amounts just to a few delay values per multiplexer stage. This results in security problems; the arbiter PUF [4], [5] and also all subsequently improved versions (XOR arbiter, feed-forward arbiter) have been broken successfully by machine-learning algorithms [6].

Applications that have been proposed for PUFs are secure credit cards, access cards and passports, unforgeable labels for valuable goods, identification of entities in insecure networks, secure key exchange, and tamper-sensitive hardware. PUF-like structures called physically obfuscated keys have been used in the context of tamper-sensitive hardware and IP protection.

It is an open research problem to find integrated electrical PUFs that can reach the complexity of known optical implementations [1]. Furthermore, one would ideally like to develop PUFs whose security is strictly independent of the computational power of an attacker. Current design strategies in which several system subcomponents interact and produce readout values at high frequencies, may not suffice in order to meet these goals. To illustrate our point, consider a hypothetical

PUF-circuit with the following properties: it generates 1-bit responses R_{C_i}, allows a readout rate of 10 MHz, and has 10-Mb of relevant random structural features. Within seconds, a list of challenge-response pairs containing, in principle, all relevant information about this PUF can be extracted from it. From this point onward, its security is only upheld by the unproven computational hypothesis that the structural information cannot be extracted efficiently from the gathered data, and cannot be used for modeling and predicting the PUF subsequently. Similar considerations apply to the described optical PUF [1], which contains less than 10^5 scatterers and allows quite high readout bitrates.

Furthermore, the number of PUF components that interact with each other cannot be increased indefinitely, since this may result in stability issues, fading signals, and simplified effective behavior of the system due to averaging effects. Electrical PUFs suffer the most from this restriction.

The concept of an electrical PUF is somewhat related to the idea artificial fingerprint devices [9] (AFDs). In one proposed AFD, for example, a unique signature of the circuit is generated from polysilicon thin-film transistor characteristics and used instead of digitally stored keys [10]. However, this signature can be straightforwardly extracted from invasive or semiinvasive electrical measurements [11], and the behavior of the random structure can be easily imitated digitally by a lookup table. AFDs cannot provide fundamentally higher security than protected digital keys due to the small amount of easily accessible structural information contained in them.

III. ROM Memories as SHIC PUFs

Our approach to circumvent the known problems in the design of secure PUFs was to readout a very large amount of independent structural information while drastically reducing the readout speed—we termed this concept a SHIC PUF in Section I. Since memory circuits are already optimized in terms of information density and readout stability, it is suggestive to borrow concepts from this area in order to implement our idea. The C_i challenge becomes a memory address, and the R_{C_i} response is the information stored therein.

In order to be used as a SHIC PUF, a fixed content memory circuit (ROM), containing N bits of information, should satisfy the following requirements.

1) The readout speed is limited by the design of the circuit to k b/s for a small value of k.
2) The time T_{full} required for complete circuit characterization ($T_{\text{full}} = N/k$) exceeds the application lifetime of the circuits or the maximal access time of an adversary (depending on the application, it should be on the order of several days, weeks, or even years).

Further requirements, which are not essential, but can significantly improve security, are as follows.

3) The N-bit content of the memory is physically random. It is caused by irregularities in the manufacturing process, which even the manufacturer cannot fully control.
4) The readout speed is limited directly and intrinsically by the construction of the memory cells, bit and word lines, and not by an artificially slow-access module. It cannot be sped up by an invasive attacker who cuts off the module and uses different, faster circuitry to access the memory.

Reasonable values for the memory size are $N = 10^{10}$ bits and $k = 100$ b/s, resulting in $T_{\text{full}} = 10^8$ s or approximately three years. We will use these parameters as *"design target"* in the rest of this paper.

Since the targeted 10-Gb information content is well within the reach of today's semiconductor memories, there are numerous realization possibilities, provided that we only aim to meet requirements 1) and 2). Any sufficiently large memory with two access modules will do: the memory is first written with random bits, using a fast-access module. Then, this module is burnt or cut off, and only the second, slow module remains for readout. The advantage of such implementation is that novel technology is not required to realize the SHIC PUF.

If we add requirement 3) to our list, there are still plenty of options. For example, it is known that a nonwritable SRAM cell on power-up latches into a state that is decided by the tiny asymmetry between its two inverters (transistors) [12]. An array of such SRAM cells could carry the required large and physically random information content. It could also be possible to modify flash-based or phase-change memory designs to operate as a SHIC PUF, by exploiting the randomness of transistor characteristics (or the state or the information-carrying phase-change layer). Since the structural information is not modified during the lifetime of the device, no writing circuitry is required for this memory.

If we aim for maximal security, however, and assume that it may be feasible for Eve to tamper with the peripheral circuits of the memory block, then the memory must also meet requirement 4). This seems difficult to satisfy for a memory built from conventional microelectronic technologies, since even slow semiconductor memories are operating in the megahertz regime. In addition, our sought technology should maximize the information content per chip area. The footprint of a single bit should be small (ideally $A < 100$ nm × 100 nm) so that the $N = 10^{10}$-bit memory would fit in a few centimeter-square area.

IV. SHIC PUFs Built from Crossbar Architectures

Cross-point architectures are the simplest functional nanodevices, possessing a very regular geometry and using only two-terminal passive devices. They hold a great promise in nanoelectronics, where fabrication challenges prohibit making a more complex, arbitrarily interconnected circuit. Circuit architectures built from memristive crossbars [13] are being actively researched today [14]. Crossbar architectures used as SHIC PUFs could, hence, achieve the highest device density, which is feasible by a certain technology node, making the PUFs small, highly secure against tampering, and potentially cheap.

The sketch of a crossbar array is shown in Fig. 2. A particular bit at the intersection of the horizontal and vertical lines is addressed by activating the corresponding bit and word lines and measuring the current flowing through the crossing. Usually, each junction is a multilayered structure showing nonlinear characteristics. We assume that only the storage array is

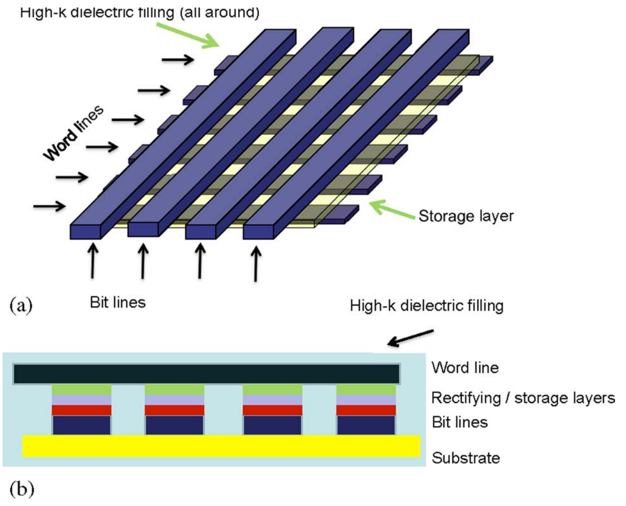

High-k dielectric filling (all around)
Word lines
Storage layer
Bit lines
(a)
High-k dielectric filling
Word line
Rectifying / storage layers
Bit lines
Substrate
(b)

Fig. 2. Schematic illustration of a crossbar memory. (a) From a perspective view. (b) From the side view.

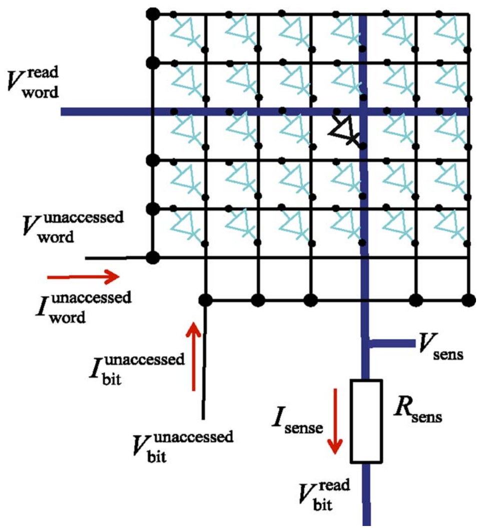

$V_{\text{word}}^{\text{read}}$
$V_{\text{word}}^{\text{unaccessed}}$
$I_{\text{word}}^{\text{unaccessed}}$
$I_{\text{bit}}^{\text{unaccessed}}$
$V_{\text{bit}}^{\text{unaccessed}}$
V_{sens}
I_{sense}
R_{sens}
$V_{\text{bit}}^{\text{read}}$

Fig. 3. Biasing scheme of a crossbar array.

implemented by crossbar technology and the readout apparatus is a silicon-based circuit [15].

A crossbar used as SHIC PUF is different from a standard crossbar memory in the following aspects.

1) The SHIC PUF-crossbar does not need to be writable. Through all its lifetime, it carries a hard-wired information content, defined by the storage layer, which is unique and random for each instance of the fabricated memory. The storage layer is an inhomogeneously conducting material, with resistance changing on the size scale of the $2F$ pitch size of the crossbar. (F is the lithography resolution.)
2) The space between the bit and word lines may be filled with a high-k (high dielectric constant) material, which creates large interwire and junction capacitances.
3) The entire memory is built as one monolithic block, where the number of bit and word lines being around $n = \sqrt{N} \approx 10^5$. This prevents the attacker from accelerating the readout by reading multiple memory banks in parallel.

The most unusual character of a PUF-crossbar is the 3), as mentioned earlier: large memory circuits are usually realized from multiple banks in order to reduce access time and improve noise margin and yield. We demonstrate in the next section that reliable readout in such large banks is nevertheless possible.

V. Accessing Information in Large Crossbar Circuits

The circuit schematics of a biased crossbar circuit are illustrated in Fig. 3. We assume that the accessed word and bit lines are biased on $V_{\text{bit}}^{\text{read}}$ and $V_{\text{word}}^{\text{read}}$ voltage, respectively. The unaccessed wires are on a fixed $V_{\text{bit}}^{\text{unaccessed}}$ and $V_{\text{word}}^{\text{unaccessed}}$ voltage.

For simplicity, all junctions of the aforementioned circuit are drawn by the same diode symbol, but their *I–V* characteristics are obviously different, carrying the random structural information. If only one bit of information is extracted per junction, we can refer to the diode as being in the "ON" or "OFF" state. There is a sense resistor (R_{sens}) connected to the accessed word line, which can have a low or a higher value, depending on whether current or voltage measurement is done by the sense amplifier.

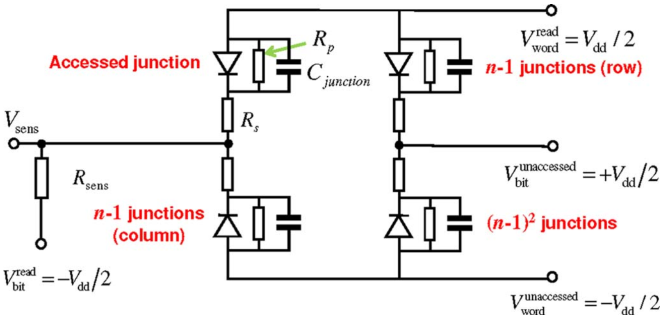
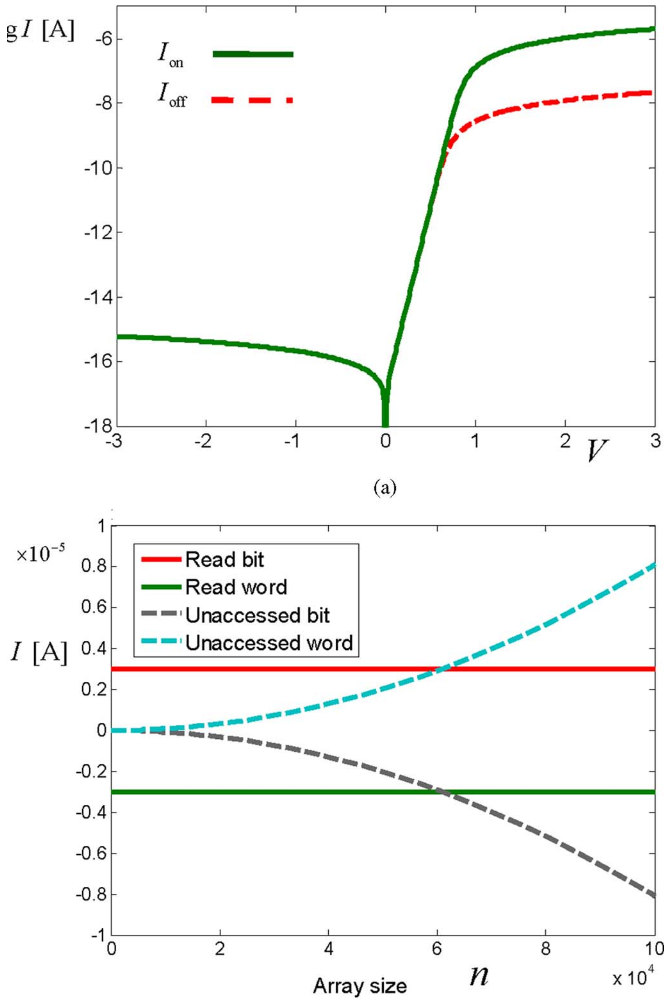

Accessed junction
R_p
$C_{junction}$
$V_{\text{word}}^{\text{read}} = V_{\text{dd}}/2$
n-1 junctions (row)
V_{sens}
R_s
R_{sens}
$V_{\text{bit}}^{\text{unaccessed}} = +V_{\text{dd}}/2$
n-1 junctions (column)
$(n\text{-}1)^2$ junctions
$V_{\text{bit}}^{\text{read}} = -V_{\text{dd}}/2$
$V_{\text{word}}^{\text{unaccessed}} = -V_{\text{dd}}/2$

Fig. 4. Equivalent circuit of a crossbar array. Each diode symbol (with the corresponding R_s and R_p serial and parallel resistances) represents an "average" junction, i.e., all the junctions connected in parallel to the same two nodes.

Assuming that the series resistances of the wires are negligible (or they can be approximated by a lumped resistance), one can construct a simple equivalent circuit model of the array, which is shown in Fig. 4. Here an equivalent ("average") lumped circuit element substitutes the junctions connecting to the accessed word/bit line and the rest of the array. Junctions connected to the accessed bit line can directly interfere by the readout process, while others just add to the net current inflow (and dissipation) of the structure.

To interrogate the selected bit in the crossbar array, we apply the bias scheme of Fig. 4. Most of the unaccessed junctions ($(n-1)(n-1)$ of them) are reverse-biased ($V_{\text{word}}^{\text{unaccessed}} = -V^{dd}/2$, $V_{\text{bit}}^{\text{unaccessed}} = V^{dd}/2$), minimizing the magnitude of parasitic currents. The interrogated junction is the only forward-biased in the array ($V_{\text{word}}^{\text{read}} = V^{dd}/2$, $V_{\text{bit}}^{\text{read}} = -V^{dd}/2$), unaccessed junctions connecting to the accessed bit and word lines get zero bias.

As an illustration, Fig. 5(a) shows two typical diode *I–V*) curves, with a high and low series resistance, representing the binary information carried by the junction. Fig. 5(b) shows the



(a)

(b)

Fig. 5. (a) *I–V* characteristics of a diode-backed junction, using $I_s = 10^{-17}$ A, $R_p = 5 \times 10^{15}$ Ω, an ideality factor of 1.5 and serial resistances of $R_s = 1$ MΩ and $R_s = 100$ MΩ for the ON and OFF state of the junction, respectively. (b) Current inflow at different array sizes, as simulated by SPICE, at $V^{dd} = 2.0\,V$.

sense current and the parasitic currents as a function of array size. For about $n \approx 6 \cdot 10^4$ array sizes, the net current flowing through the reverse-biased (unaccessed) junctions begins to exceed the "useful" current flowing through the accessed bit and word line. This causes unnecessary power dissipation, but the parasitic current on a single bit/word line [on average (I/n)] still remains small. Noise margin is high, as most of the parasitic paths avoid the accessed bit and word lines. Taking into account the bit and word line resistances would reduce the noise margin, but the calculations show that the diode-backed crossbar memory is scalable to very large array sizes, at least in the region of $n > 10^5$, $N > 10^{10}$, as required by the specified design target.

We did not investigate the construction of the memory-decoding circuit. For lithographic crossbars ($F > 100$ nm), the decoder must be straightforward to build, even if decoding a $10^5 \times 10^5$ size memory block would be quite unusual and impractical in conventional memory designs. For nonlithographic crossbars, several constraints arise at the construction of the "nano–micro" link. The reader is referred to the literature [16]–[18] for the solutions currently being researched.

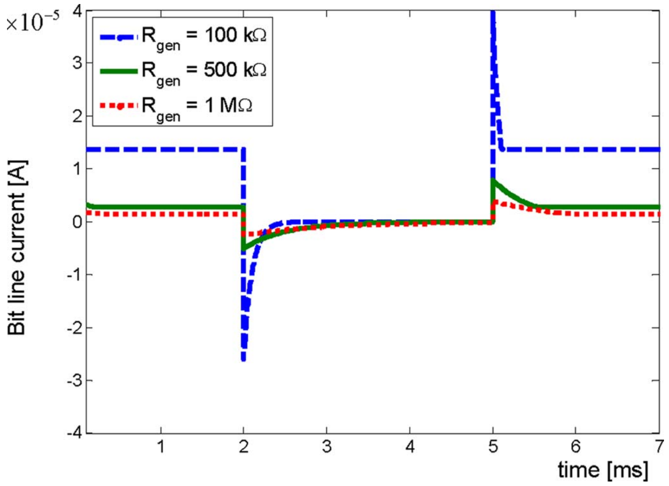


Fig. 6. Complete read cycle of the crossbar memory. The curves show the time dependence of I_{sens} current and the bias voltages. At $t = 2$ ms, the accessed junction is unbiased (reverse-biased) and at $t = 5$ ms, biased again.

VI. Slow ReadOut Speed and Security Against Invasive Attacks

Time-dependent behavior of the crossbar can be modeled by running a transient simulation on the circuit of Fig. 4. It is required to consider the serial (Thevenin equivalent) resistance of the voltage generators that drive the accessed/unaccessed bit and word lines—these R_{gen} generator resistances are not shown in Fig. 4.

Assuming that the series resistance of the bit/word wires is negligible (or can be approximated by a lumped resistance) and that the wires survive any current density, it is the generator resistance R_{gen} and the net capacitance of the word line C_Σ that determines the $\tau = R_{\text{gen}} C_\Sigma$ time constant of the circuit.

Fig. 6 shows the simulation of a complete read cycle, using a junction capacitance of $C_{\text{junction}} \approx 10^{-14}$ F and assuming generator resistances of $R_{\text{gen}} = 100\,\text{k}\Omega$, $R_{\text{gen}} = 500\,\text{k}\Omega$, and $R_{\text{gen}} = 1\,\text{M}\Omega$. At the beginning ($0 < t < 2$ ms), the crossbar is readout using the bias scheme of Fig. 4. At $t = 2$ ms, the generators abruptly unbias the accessed junction, i.e., both $V_{\text{word}}^{\text{read}}$ and both $V_{\text{bit}}^{\text{read}}$ switch polarity. At $t = 5$ ms, the polarity of this wires switch again; therefore, the interrogated junction is forward-biased again.

The simulations of Fig. 6 show that, for the parameters we choose, at least a few milliseconds must elapse between the subsequent readouts for the sense current/voltage to stabilize. The resulting readout speed of around 100 b/s corresponds well to the specifications in Section III.

Smaller values of R_{gen} lead to faster readout cycles and, at the same time, a higher capacitive peak current during the charge up of the bit or word lines. The wire can be overloaded and destroyed by this. R_{gen} has to be chosen in such a way that the driven word line is not destroyed; consequently, the speed of a large crossbar memory is limited by the finite current-carrying ability of the nanoscale wires. Faster readout attempts will inevitably result in rapid destruction of these wires, rendering the structure unusable/unreadable.

The $C_{\text{junction}} \approx 10^{-14}$ value we used in the calculations is about an order of magnitude higher than the geometric capacitance could alone provide. An elementary capacitance calculation ($C = \epsilon_r \epsilon_0 (A/d)$) gives $C = 10^{-15}$-F capacitance for an $A = 100\,\text{nm} \times 100\,\text{nm}$ junction (using $d = 1$ nm and $\epsilon_r = 10$). Additional parasitic capacitances, interwire capacitances, and equivalent capacitances associated with carrier mobilities can increase the junction capacitance to the desired value. Another possibility to increase capacitances is filling the gaps of the structure with high-k materials, with a dielectric constant being in the $\epsilon_r \approx$ 100–1000 range. Such very high-k materials (ferroelectrics) were widely investigated and characterized for ferroelectric memory applications and their technology is compatible with standard silicon processing [19], though they considerably complicate the fabrication process. A lower C_{junction} value may also suffice, but the R_{gen} should be increased to maintain the same τ time constant. An excessively high R_{gen} decreases the noise margin of the memory.

If more than a single bit of information is stored in the junctions (analogously to multibit storage in modern memories), then the required measurement precision will further slow down circuit operation. Another mode of operation is to compare the resistances of two randomly selected junctions. This may also provide compensation against power supply fluctuations and certain aging effects.

The adversarial attacker could try to manipulate or entirely replace the readout circuitry of the memory in order get quick access to its content. This can be done by using a smaller value for R_{gen} (i.e., decreasing the time constant) and/or reading out multiple bits in parallel.

Both of these approaches are prevented, however, if the wires have been set to have only a limited $i_{\max}^{\text{in}}$ current-carrying capability. Decreasing the value of R_{gen} m-fold will result in m times larger peak currents and destroys the wire. Reading multiple (say h) bit values simultaneously loads the corresponding bit/word line with $h \times i_{\text{static}}$ current and exceeds the value of $i_{\max}^{\text{in}}$ already for small h. As our simulation results show, the $i_{\max}^{\text{in}}$ current limit could still be a few times larger than the i_{static} steady-state current flow, meaning that a regime exists, where the crossbar would still be reliably readable, but at the same time secure.

A predetermined breaking point could be defined on the nanowires to control the maximum allowable current densities. The cryptographic application can tolerate, if a number bit or word lines are damaged during fabrication as the bad C_i, R_{C_i} pairs could be ignored in the cryptographic protocol.

If the crossbar is fabricated by state-of-the-art lithographic technology or with sublithographic resolution, tampering with the internal structure of the crossbar array seems to be technologically impossible, even for adversaries with practically unlimited financial resources. This prevents attacks in which the adversary would split the crossbar into several subblocks and reads them out in parallel or fabricate contacts to access inner nodes. The dense and regular structure of a crossbar and the transistorless construction of the storage block most likely prevents attacks that are conceivable for circuits made with conventional microelectronic technologies such as cryptographic processors [11].

VII. Realization Possibilities for the Random Information Content

One crucial component of the crossbar memory is the information-carrying layer. Ideally, its irregular structural features should result in a truly random information content of the memory. There are several suggestive random physical processes, which form the sought type of nanostructures.

1) One possibility involves a phase change material, which is illuminated by a random image (such as a series of unaligned speckle patterns), resulting in an inhomogeneously conducting media [20]. This method is not manufacturer resistant [5], meaning that a fraudulent manufacturer could generate more than one memory of the described type with the same information content.
2) Alternatively, a very thin oxide layer with a nonuniform thickness can provide a tunneling current, which is different from junction to junction.
3) Also crystallization processes exhibit an inherent randomness: the exact location of nucleation sites depend on atomic-scale defects or roughness of material surfaces. One example would be amorphous silicon, crystallized with a laser beam again in combination with a speckle pattern. For phosphorous-doped amorphous Si:H (a-Si:H), a resistivity change between crystallized and noncrystallized areas of 100 and 10^6 can be obtained for a P-concentration of 10^{-5}% and 2% in the initial layer, respectively. These crystallization processes can reach resolutions below 100 nm due to the small heat diffusion length in the silicon [21]. A polycrystalline material can be doped as well, resulting in an inhomogenously doped semiconductor.

One particular advantage of these processes is that they can be made compatible with modern semiconductor manufacturing technology.

VIII. Generating the Information by Random Crystallization Processes

To illustrate the feasibility of a randomly conducting layer, we have performed experiments on a medium prepared with a random recrystallization process. Such crystallization processes are particularly attractive for our goal, since the nucleation site cannot be calculated or predicted, and the nucleation process is governed by atomic-scale inhomogeneities of the starting material.

We chose the aluminum-induced layer exchange (ALILE) process [22]–[24], which is used to crystallize amorphous silicon layers. In a typical ALILE process (which is illustrated in Fig. 7), an Al/amorphous Si (a-Si) layer stack, separated by a thin oxide film [see Fig. 7(a)], is annealed at temperatures below the eutectic temperature of the Al–Si system. Annealing of the sample leads to diffusion of Si atoms into the Al layer.

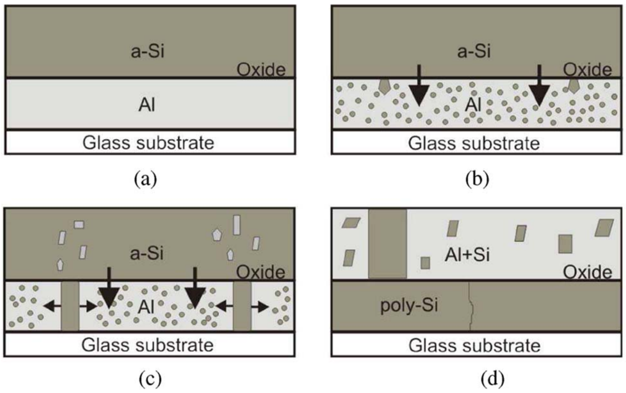


Fig. 7. Steps of the ALILE process. (a) Al/amorphous Si layer stack on glass substrate as starting configuration. (b) and (c) During the annealing, Si nuclei form in the Al and grow in size. (d) Finally, a closed polycrystalline layer has formed replacing the Al.

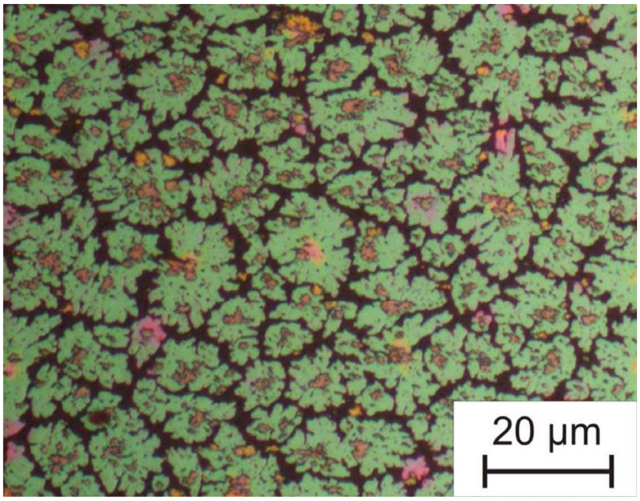


Fig. 8. Top-view optical microscopy image of the resulting ALILE layer.

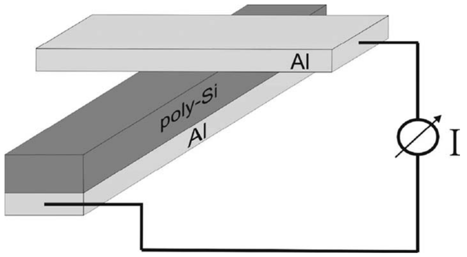


Fig. 9. Schematic illustration of a crossbar junction built by the ALILE process.

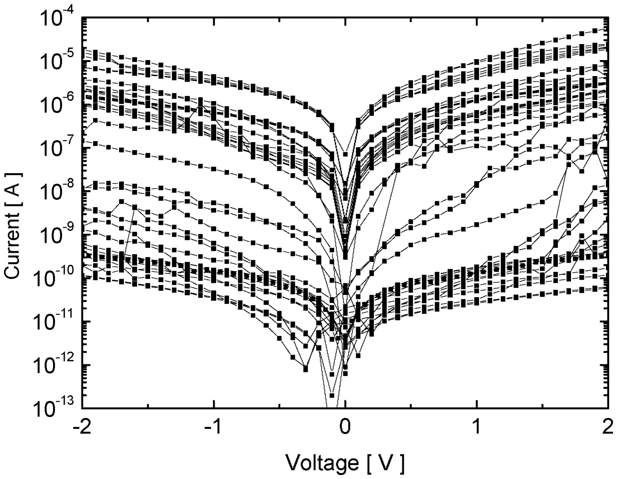


Fig. 10. Arbitrarily chosen measurements on ALILE poly-Si/Al junctions. Random resistive values are present due to the inhomogeneous structure of the poly-Si film.

Crystallite formation occurs, where local supersaturation of the Al with Si is achieved [see Fig. 7(b)]. In addition to that, irregularities and defects, e.g., grain boundaries of the Al, can serve as crystallization sites. As nuclei have appeared, they grow until they reach the substrate. From this point, crystallites grow laterally [see Fig. 7(c)] until a closed poly-Si layer has formed [see Fig. 7(d)]. After the process is completed, the silicon and aluminum layers exchanged their respective positions and the a-Si has been crystallized.

By adjusting the initial Al/Si layer thickness ratio, an incomplete poly-Si layer composed of not fully interconnected grains can be achieved. An example illustrating the randomness of such an incomplete ALILE layer is shown in Fig. 8, where the greenish area represents the crystallized silicon grains and the black surrounding the glass substrate. In this case, the Al remaining on top of the poly-Si layer has been removed by wet chemical etching. The ratio between the area covered with crystallites and the bare glass can be adjusted by the Al/Si thickness ratio. The size of the crystallites is determined by the annealing temperature and the initial layer thickness. Since the crystallized silicon grains are Al-doped after the layer exchange process, this method results in conducting (Si-grains) and nonconducting (bare glass) regions in a truly random arrangement. Fully crystallized layers also reflect the randomness of their formation process and show inhomogeneous conductivity.

We have fabricated small-size crossbar structures having a crystallized layer as the information carrier. In order to obtain an Al back contact, we used the reverse configuration of the ALILE process [25] to fabricate Al/poly-Si wires with a width of 1–4 μm (see Fig. 9) on quartz glass substrates. Hydrogen passivation is used to reduce the hole carrier concentration in the poly-Si. The details of the hydrogenation process can be found elsewhere [23]. Then Al wires of the same size were evaporated with a mask, aligned perpendicular to the Al/poly-Si wires as sketched in Fig. 9.

Fig. 10 shows some measured *I*–*V* curves on these junctions. It is clear that the *I*–*V*curve shows sufficient randomness. We are currently working on scaling the feature sizes down to the 100-nm regime; this is required to obtain our *design target* (see Section III) within a reasonably small (cm^2 size) active chip surface.

The presented layer stack already shows a weakly rectifying behavior, due to the Schottky-type contact between Al and poly-Si layers. This nonlinearity is yet insufficient to make the crossbar addressable and a separate diode layer is necessary to realize the selector elements.

There are several technologies in the recent literature giving solutions for the fabrication of the diode layer or the entire crossbar. Crossbar memories can be made from standard semiconductor material systems (silicon, poly-Si) and oxide-based switching layers [26], [27]. Molecular switching elements are researched to achieve true nanometer-scale storage [27], [28]. Crossbar memories are proposed to be built from semiconductors that enable low-temperature processing, higher integration densities (such as ZnO) [29], and back end of the line fabrication. This later possibility is especially promising: a low-cost crossbar layer placed on top of a silicon IC can also serve as a coating PUF [30], physically protecting the underlying circuitry. It would also be possible to use high-capacitance, high-resistance amorphous semiconductors (such as amorphous silicon suboxides [31]).

IX. Implementation Variants and Limits

There are several possible device variants for the crossbar PUF, depending on the application area and the desired level of security. The design target outlined in Section III results in a structure that may withstand about three years of *continuous* adversarial access until full characterization ($T = N/k = (10^{10}\ \text{bits})/(100\ \text{b/s}) = 10^8\ \text{s} \approx 3$ years).

If the memory is realized as nonlithographic crossbar (with feature size in the 10-nm range), and the $k = 100$ b/s readout rate can be maintained, then a centimeter-square-size block stays secure for several decades. For lithographic crossbars, a few years should be achievable.

The total adversarial access time and the security lifetime of a product must be distinguished; during the few years lifetime of a credit card, for example, the maximal, hypothetical adversarial access time will never go beyond a few days (card is stolen and brought back unnoticed), and will typically be significantly lower. So a cheap, few millimeter-square-area lithographic crossbar can already provide a practically sufficient level of security. The ALILE technology described in Section VIII can be readily used for a number of applications, including credit cards, passports, and key exchange. These applications realistically require only a T of several days.

Small crossbar blocks will have lower RC constants than large memory banks. High-k materials still can help to keep capacitances high and access rates low. Our group is currently investigating a variant of the ALILE technology, which allows to further slow down the readout rates by introducing a large number of slow traps at the crossbar junctions.

If the access rate of single memory block is extremely low (k is only a few bits per second), then the crossbar can be partitioned into smaller, parallel accessed blocks without compromising security. For sublithographic crossbars, a number of smaller memory blocks may also provide ultimately high security, since invasive attacks (such as microprobing) become practically impossible at this scale.

If multilevel storage is applied, the tradeoff between size, security, and resolution can be improved yet further.

X. Conclusion

This paper proposed a new design paradigm for the construction of secure PUFs. While the standard approach is to employ many interacting components and high readout speeds, we suggest to use as many single, densely packed, independent subunits as possible while drastically reducing the readout frequency. This new principle allows the construction of the first PUFs which are secure even against computationally unbounded adversaries, and in the face of weeks or years of uninterrupted adversarial access. The slower readout speed seems no severe disadvantage in typical appliances such as key exchange, credit cards, or hardware tamper detection.

We suggested crossbar arrays as a preferable way to implement SHIC PUFs. Crossbar arrays lead to electrical SHIC PUFs that can be integrated conveniently on a chip. They reach ultimate information densities and are potentially cost effective, since they have a regular geometry and use only two-terminal passive devices. Due to their simple layout, they can be produced at the limit of current nanofabrication, which gives them high security against invasive attacks and increases their security lifetime. We further showed that it is possible to enforce the slow readout speed required for SHIC PUFs as an intrinsic property of the crossbar's wiring and cell architectures, and not only by an intentionally slow-access module, which might potentially be circumvented or cut off.

We have backed our new design proposal by a discussion of several concrete implementations, circuit simulation data, and an experimental feasibility study. Our research suggests that it should be possible to build a USB-stick-type device with dimensions of a few millimeter × 1 cm × 1.5 cm, which is secure for ideally up to tens of years, and which can be used for user identification, hardware identification, key exchange, and other security appliances. Other implementation variants tailored for specific settings can be made yet smaller and cheaper and integrated conveniently in existing microelectronic systems. For further information about ongoing research, referred to [32].

Acknowledgment

The authors would like to thank I. Szentmiklosi, M. Pra, T. Jun, M. Scholz, and X. Ju for valuable discussions and raising excellent questions. This study was conducted in the course of the Physical Cryptography Project of the Technische Universität München.

References

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[2] D. B. Gassend, D. Clarke, M. van Dijky, and S. Devadas, "Silicon physical random functions," presented at the CSC, Washington, DC, Nov. 18–22 2002.

[3] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[4] D. Lim, "Extracting secret keys from integrated circuits," M.Sc. dissertation, MIT, Cambridge, MA, 2004.

[5] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas, "Identification and authentication of integrated circuits," *Concurrency Comput., Pract. Exp.*, vol. 16, no. 11, pp. 1077–1098, 2004.

[6] U. Rührmair, J. Sölter, and F. Sehnke. (2009). On the foundations of physical unclonable functions, *Cryptology ePrint Archive: Rep. 2009/277* [Online]. Available: http://eprint.iacr.org/2009/277

[7] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," Cryptology ePrint Archive, Rep. 2010/251, 2010. Available: http://eprint.iacr.org/

[8] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. 9th Int. Workshop CHES 2007 (LCNS)*, vol. 4727, New York: Springer-Verlag.

[9] S. Maeda, H. Kuriyama, T. Ipposhi, S. Maegawa, Y. Inoue, M. Inuishi, N. Kotani, and T. Nishimura, "An artificial fingerprint device (AFD): A study of identification number applications utilizing characteristics variation of polycrystalline silicon TFTs," *IEEE Trans. Electron Devices*, vol. 50, no. 6, pp. 1451–1458, Jun. 2003.

[10] S. Maeda, H. Kuriyama, T. Ipposhi, S. Maegawa, and M. Inuishi, "An artificial fingerprint device (AFD) module using poly-Si thin film transistors with logic LSI compatible process for built-in security," in *Proc. IEDM Tech. Dig. Int. Electron Devices Meeting*, 2001, pp. 34.5-1–34.5-4.

[11] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov, "Cryptographic processors-A survey," *Proc. IEEE*, vol. 94, no. 2, pp. 357–369, Feb. 2006.

[12] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardware-Oriented Secur. Trust (HOST 2008)*, Jun., pp. 67–70.

[13] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, pp. 80–83, May 2008.

[14] G. Snider, "Computing with hysteretic resistor crossbars," *Appl. Phys. A*, vol. 80, pp. 1165–1172, 2005.

[15] G. F. Cerofolini, G. Arena, C. M. Camalleri, C. Galati, S. Reina, L. Renna, and D. Mascolo, "A hybrid approach to nanoelectronics," *Nanotechnology*, vol. 16, pp. 1040–1047, 2005.

[16] A. DeHon, S. C. Goldstein, P. J. Kuekes, and P. Lincoln, "Nonphotolithographic nanoscale memory density prospects," *IEEE Trans. Nanotechnol.*, vol. 4, no. 2, pp. 215–228, Mar. 2005.

[17] R. Beckman, E. Johnston-Halperin, Y. Luo, J. E. Green, and J. R. Heath, "Bridging dimensions: Demultiplexing ultrahigh-density nanowire circuits," *Science*, vol. 310, pp. 465–228, Oct. 21, 2005.

[18] D. B. Strukov and K. K. Likharev, "Defect-tolerant architectures for nanoelectronic crossbar memories," *J. Nanosci. Nanotechnol.*, vol. 7, pp. 151–167, 2007.

[19] S. K. Dey and R. Zuleeg, "Processing and parameters of sol-gel PZT thin-films for GaAs memory applications," *Ferroeloectrics*, vol. 112, pp. 309–319, 1990.

[20] P. Nangle, "Programming method for non-volatile memory," U.S. Patent 7106622, Sep. 12, 2006.

[21] S. D. Brotherton, "Polycrystalline silicon thin film transistors," *Semicond. Sci. Technol.*, vol. 10, pp. 721–738, 1995.

[22] T. Antesberger, C. Jaeger, M. Scholz, and M. Stutzmann, "Structural and electronic properties of ultrathin polycrystalline Si layers on glass prepared by aluminum-induced layer exchange," *Appl. Phys. Lett.*, vol. 91, pp. 201909-1–201909-3, 2007. DOI: 10.1063/1.2803072.

[23] C. Jaeger, T. Antesberger, and M. Stutzmann, "Hydrogen passivation of ultra-thin low-temperature polycrystalline silicon films for electronic applications," *J. Non-Cryst. Solids*, vol. 354, no. 19–25, pp. 2314–2318, May 2008. DOI: 10.1016/j.jnoncrysol.2007.09.040.

[24] O. Nast, T. Puzzer, L. M. Koschier, A. B. Sproul, and S. R. Wenham, "Aluminum-induced crystallization of amorphous silicon on glass substrates above and below the eutectic temperature," *Appl. Phys. Lett.*, vol. 73, pp. 3214–3216, 1998.

[25] J. H. Kim and J. Y. Lee, "Al-induced crystallization of an amorphous Si thin film in a polycrystalline Al/ native SiO_2/amorphous Si structure," *Jpn. J. Appl. Phys.*, vol. 35, pp. 2052–2056, 1996.

[26] C. de Graaf, P. H. Woerlee, C. M. Hart, H. Lifka, P. W. H. de Vreede, P. J. M. Janssen, F. J. Sluijs, and G. M. Paulzen, "A novel high-density low-cost diode programmable read only memory," in *Proc. Int. Electron Devices Meeting*, Dec. 8–11, 1996, pp. 189–192.

[27] M. Johnson, A. Al-Shamma, D. Bosch, M. Crowley, M. Farmwald, L. Fasoli, A. Ilkbahar, B. Kleveland, T. Lee, T.-Y. Liu, Q. Nguyen, R. Scheuerlein, K. So, and T. Thorp, "512-Mb PROM with a three-dimensional array of diode/antifuse memory cells," *IEEE J. Solid-State Circuits*, vol. 38, no. 11, pp. 1920–1928, Nov. 2003.

[28] G. Csaba and P. Lugli, "Read-out design rules for molecular cross bar architectures," *IEEE Trans. Nanotechnol.*, vol. 8, no. 3, pp. 369–374, May 2009.

[29] M. Pra, G. Csaba, C. Erlen, and P. Lugli, "Simulation of ZnO diodes for application in non-volatile crossbar memories," *J. Comput. Electron.*, vol. 7, no. 3, pp. 146–150, Sep. 2008.

[30] P. Tuyls, G.-J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-proof hardware from protective coatings," in *Proc. CHES 2006*, pp. 369–383.

[31] R. Janssen, A. Janotta, D. Dimova-Malinovska, and M. Stutzmann, "Optical and electrical properties of doped amorphous silicon suboxides," *Phys. Rev. B*, vol. 60, pp. 13561–13572, 1999.

[32] C. Jaeger, M. Algasinger, U. Rührmair, G. Csaba, and M. Stutzmann, "Random pn-junctions for physical cryptography," *Appl. Phys. Lett.*, vol. 96, 172103, 2010. DOI: 10.1063/1.3396186.

Ulrich Rührmair studied mathematics at Ludwig-Maximilians-Universität München, Munich, Germany, and received the M.Sc. degree from the University of Oxford, Oxford, U.K.

He is the Founder and is currently the Head of the Physical Cryptography Project, Technische Universität München, Munich. His research interests include complexity theory at large and cryptography and security, in particular, alternative approaches such as quantum cryptography, DNA-based cryptography, and physical cryptography.

Christian Jaeger was born in Würzburg, Germany, in 1979. He received the Diploma degree in physics from Technische Universität München, Munich, Germany, in 2006, where he is currently working toward the Ph.D. degree at Walter Schottky Institute.

He was also involved with the Universitat de Barcelona, Barcelona, Spain and at the Research Center for Photovoltaics, National Institute of Advanced Industrial Science and Technology, Tsukuba, Japan. His research interests include the crystallization of amorphous silicon for large-area electronics and cryptographic applications.

Matthias Bator was born in Grudziadz, Poland. He received the Diploma degree in physics from Technical University Munich, Munich, Germany, in 2008. He is currently working toward the Ph.D. degree at Paul Scherrer Institute, Switzerland.

His current research focuses on the fabrication of multiferroic, in particular, magenetoelectric thin films by pulsed laser deposition and their characterization using X-ray and neutron diffraction techniques.

Martin Stutzmann was born in Frankenberg, Germany, on November 19, 1956. He received the Physics Diploma (*summa cum laude*) degree from the University of Marburg, Marburg, Germany, in 1980, the Licence de Physique degree from Université Paris VII, Paris, France, in 1982, with a fellowship from the German National Academic Foundation, and the Ph.D. (*summa cum laude*) degree, in 1983 under the supervision of J. Stuke. He received the Habilitation degree in experimental physics, in 1990.

During 1975–1976, he was in military service. From 1982 to 1983, he was a Research Scholar at Stanford University, where he was involved in the research on paramagnetic states in hydrogenated amorphous silicon and germanium. From 1983 to 1985, he was a Postdoctoral Researcher at Xerox Palo Alto Research Center, Palo Alto, CA, in the group of R. A. Street, where he was involved in the research on the light-induced metastability and substitutional doping of amorphous silicon. During 1985–1993, he was a Research Staff Member in the group of M. Cardona at the Max Planck Institute for Solid State Research, Stuttgart, Germany, where he was involved in the research on hydrogen in semiconductors, porous silicon, silicon sheet polymers, and spin-dependent recombination. Since 1993, he has been the Director of the Walter Schottky Institute, Technical University Munich, Munich, Germany, where he is the Chair of Experimental Semiconductor Physics II. His current research interests include semiconductor heterostructures and devices for bioelectronics, sensors, spintronics, and photovoltaics. Since 1995, he has been the Editor-in-Chief of the *Physica Status Solidi.*

Dr. Stutzmann received the Walter Schottky Prize of the German Physical Society in 1988. In 2006, he was Elected Fellow of the American Physical Society. He has been the Chair or Co-Chair of more than ten international scientific meetings. He has been involved with numerous scientific committees, e.g., for national and international conferences, the German Science Foundation, and the Alexander-von-Humboldt Foundation.

Paolo Lugli (SM'07) received the Graduate degree in physics from the University of Modena, Modena and Reggio Emilia, Italy, in 1979, and the M.Sc. and Ph.D. degrees in electrical engineering from Colorado State University, Fort Collins, in 1982 and 1985, respectively.

In 1985, he joined the Physics Department, University of Modena, as a Research Associate. From 1988 to 1993, he was an Associate Professor of solid-state physics at the Engineering Faculty, 2nd University of Rome, Tor Vergata, where he became a Full Professor of optoelectronics in 1993. In 2003, he joined the Technical University of Munich, Munich, Germany, where he is currently the Head of the Institute for Nanoelectronics. He has authored more than 250 scientific papers and or coauthored the books "The Monte Carlo Modeling for Semiconductor Device Simulations" (Springer, 1989) and "High Speed Optical Communications" (Kluwer Academic, 1999). His research interests include the modeling, fabrication, and characterization of organic devices for electronics and optoelectronics applications, the design of organic circuits, the numerical simulation of microwave semiconductor devices, and the theoretical study of transport processes in nanostructures.

Dr. Lugli was the General Chairman of the IEEE International Conference on Nanotechnology, Munich.

György Csaba was born in Budapest, Hungary, in 1974. He received the M.S. degree from the Technical University of Budapest, Budapest, Hungary, in 1998, and the Ph.D. degree from the University of Notre Dame, Notre Dame, IN, in 2003.

During 2004–2010, he was a Research Assistant at the Technical University of Munich, Munich, Germany. In 2010, he joined the faculty of the University of Notre Dame. His research current interests include in modeling of nanoscale systems (especially magnetic devices) and exploring their applications for nonconventional circuit architectures.