Security Applications of Diodes with Unique Current-Voltage Characteristics

(Short Paper)

Ulrich Rührmair[1,⋆], Christian Jaeger[2], Christian Hilgers[1], Michael Algasinger[1], György Csaba[3], and Martin Stutzmann[1]

[1] Computer Science Department
[2] Walter Schottky Institute
[3] Institute for Nanoelectronics
TU München, Germany
ruehrmai@in.tum.de, christian.hilgers@mytum.de, csaba@tum.de,
{christian.jaeger,michael.algasinger,stutz}@wsi.tum.de
http://www.pcp.in.tum.de

Abstract. Diodes are among the most simple and inexpensive electric components. In this paper, we investigate how random diodes with irregular $I(U)$ curves can be employed for crypto and security purposes. We show that such diodes can be used to build Strong Physical Unclonable Functions (PUFs), Certificates of Authenticity (COAs), and Physically Obfuscated Keys (POKs), making them a broadly usable security tool. We detail how such diodes can be produced by an efficient and inexpensive method known as ALILE process. Furthermore, we present measurement data from real systems and discuss prototypical implementations. This includes the generation of helper data as well as efficient signature generation by elliptic curves and 2D barcode generation for the application of the diodes as COAs.

Keywords: Physical Cryptography, Physical Unclonable Functions, Certificates of Authenticity, Random Diodes, ALILE Crystallization, SHIC PUFs.

1 Introduction

The use of physical systems with an irregular, at least partly random finestructure recently has gained strong attention in the security and crypto community. In lack of an established, common term, one might call the related field *physical cryptography*, distinguishing it from quantum cryptography or DNA-based approaches. As has been shown in a number of publications starting as early as in the 1980s [1], such disordered physical systems can lead to security applications with enhanced cost efficiency and/or security. Classes of systems that are useful in the area include Strong Physical Unclonable Functions (PUFs) [2] [3] [4], Certificates of Authenticity (COAs) [5] [6], or Physically Obfuscated Keys (POKs) [7] (also called Weak PUFs in [4]).

⋆ Corresponding author.

R. Sion (Ed.): FC 2010, LNCS 6052, pp. 328–335, 2010.

In this paper, we are concerned with the security applications of diodes with irregular $I(U)$ curves. Such diodes have been prepared in our group by a special, crystallization-based fabrication method known as ALILE process [8] [9]. As we are going to show, they can be employed as building blocks for all three named systems, i.e. both for Strong PUFs, COAs and POKs. Furthermore, they are cheap, take very small chip area, and have a good temperature stability. Therefore, so we argue, they have the potential to become a useful and broadly applicable tool in *physical cryptography*.

The paper is organized as follows. In section 2, we explain the ALILE fabrication process for our diodes. Section 3 describes the use of the diodes as COAs or unforgeable labels, and Section 4 discusses their employment as POKs. In Section 5, we illustrate how our diodes can help us to realize a special type of Strong PUF with high information content, which is naturally immune against machine learning attacks. Section 6 concludes the paper.

2 Sample Preparation

For the preparation of the random diodes we use the aluminum-induced layer exchange (ALILE) process [8] [9], which is known to result in polycrystalline films with p-type conduction [10]. This process is used to crystallize amorphous silicon (a-Si) layers exploiting the catalytic effect of aluminum. Here, an Al/oxide/a-Si layer stack is annealed at temperatures below the eutectic temperature of the Al-Si system. Annealing of the sample leads to diffusion of the Si atoms into the Al layer. Crystallite formation occurs where local supersaturation of the Al with Si is achieved. In addition to that, atomic-scale irregularities and defects, e.g. grain boundaries in the Al, can serve as crystallization sites. Thus, the actual crystallization sites can neither be predicted nor controlled, in particular not by the manufacturer of the structure. The same holds for the irregular crystallite growth.

To illustrate the natural randomness of the process, Fig. 1 a depicts the first step of crystallization recorded by an optical microscope, showing the random distribution of the initial crystallization sites. Fig. 1 b illustrates the random crystallite development in later states of the process. In the ALILE-based fabrication of our random diodes, we chose n-type crystalline silicon wafers as the substrate (see Fig. 1 c) [11].

Medium rectification rates of the diodes are observed for diodes prepared on highly doped wafers (e.g. $\rho = 0.003 - 0.007\ \Omega cm$). Such diodes, which exhibit random

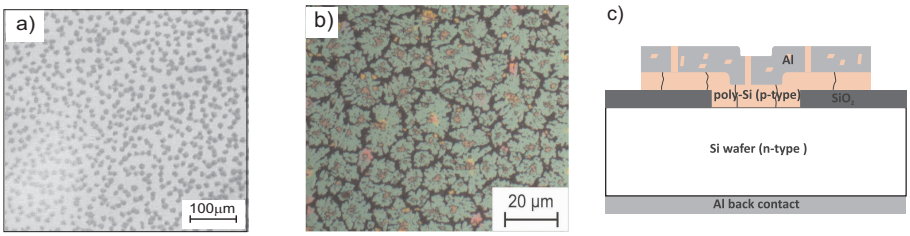

Fig. 1. (a) First crystallites (dark spots) appearing in the Al-matrix during the ALILE process. (b) Irregular growth of the crystallites. (c) Schematic sketch of the diodes' structure.

$I(U)$ characteristics over the whole current-voltage range (see Fig. 2 a), are ideally suited for applications such as electrical COAs (Sec. 3) or POKs (Sec. 4). A very high rectification ratio of the diodes (up to 2×10^7) is obtained for using low doped wafers (e.g. $\rho = 1 - 10\ \Omega cm$); see Fig. 3 a. This high rectification allows the application of the diodes in large crossbars structures with high information density, i.e. as Strong PUFs (see Sec. 5). Further details of the fabrication of ALILE layers and the diode fabrication can be found in [10] [11].

3 Electrically Readable Certificates of Authenticity

The use of a disordered physical structure as unforgeable label in connection with an accompanying digital signature has first been proposed in [1], and was termed Certificate of Authenticity (COA) in [5] [6]. COAs require a unique structure that generates a non-imitable *analog* measurement signal, which must be measured by an *external* measurement device. (Note that in opposition to that, most PUFs generate a digital output and have an integrated measurement device.)

Due to the complex and varying $I(U)$ curves, ALILE-diodes can be employed for said task. They can form cheap COAs whose electrical read-out allows very inexpensive readers.

Prototypical Implementation. To test how many different diodes can be distinguished reliably and repeatedly, we collected measurement data of 16 different individual diodes on one chip (Figure 2 a). For 10 out of 16 diodes we repeated every measurement 5 times, and determined the average $I(U)$ curves by taking the arithmetic mean. We also calculated the maximum deviation and the average deviation from the average $I(U)$ curve. In Figure 2 b, the deviation is given in per cent of the respective average value. We observe a decreasing deviations for higher positive voltages, whereas the deviation is slightly lower in the forward direction of the diodes (negative voltages).

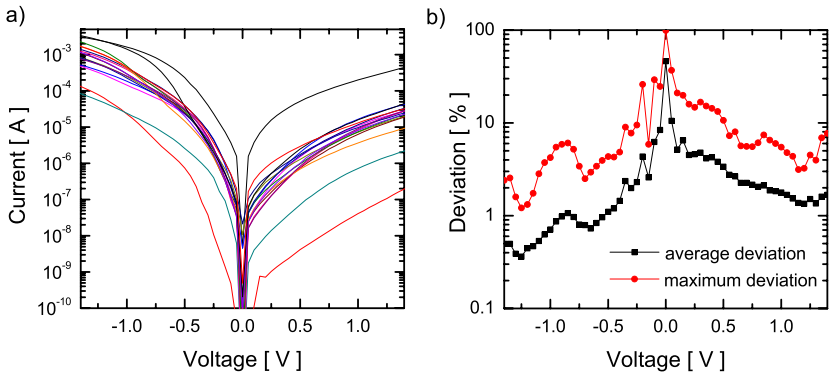

Fig. 2. a) Characteristic $I(U)$-curves of various diodes. b) Average and maximum deviation of the current values upon multiple measurements.

As straightforward helper data for reliable diode identification, the average curves were tabbed at the fixed voltages -1.3 V, -0.65 V, 0.65 V and 1.3 V. An obvious condition for reliable identification is that the average current values at each supporting point must at least allow a deviation as large as the maximum deviation shown in Figure 2 b. The maximum deviation values for our supporting points are as follows: 1.60 at -1.3 V; 2.95 at -0.65 V; 5.67 at 0.65 V; 3.96 at 1.3 V.

The data gathered by us shows that even at a (hypothetical) variance of up to 27% all the 16 diodes could still be distinguished reliably. At the same time, the diodes only showed deviation values of up to 6% in our experiments. This confirms the possibility for realiable identification.

Along the same lines, we executed a first estimation of the overall number of diodes that can be distinguished with the four supporting points at said voltage levels. We assumed a maximal, practically occurring measurement variance of 10% in our calculation, and obtained roughly 160 distinguishable diodes within the broad band, and around 200 distinguishable diodes in the whole current range. To further increase the complexity of the unique, analog COA-signal, experiments are on the way in our group to investigate the frequency spectra arising from networks of 10 to 100 random diodes. Such periodic networks of non-linear components can exhibit rich, complex spectra [12].

To collect additional support for the applicability of random diodes as unforgeable labels, we carried out a prototypical COA implementation on the basis of 2D barcodes. Parameters of interest here are the resulting barcode sizes and longterm security.

We started by selecting a suitable 2D-barcode, choosing the widely used Data Matrix Code, and implemented it by use of the libdmtx library [13]. Due to the limited storage capacity of barcodes, shorter signatures than RSA are preferred in the generation of COAs; our implementation is based on the bilinear pairing based scheme by Zhang, Safavi-Naini und Susilo (ZSS) [14], which allows signatures of only 160 bits. For the implementation we chose the PBC library [15] with the elliptic curve type F. We assumed that a single waver with 20 diodes is applied as unique object, and that the following information must be stored on the product: Manufacturer ID, product related information (16+48 bit); helper data (20 x 14 bit); digital signature (160 bit). Using a barcode module width 0.25 mm, this leads to a barcode of size 0.81 cm^2. We succesfully generated such a barcode with data from our real measurement data and for exemplary product related data.

Our diode-based approach to COAs therefore leads to inexpensive labels with barcode sizes of less than 1 cm^2. It allows one of the first electrical COAs with high security and complex analog output; previous COAs were mainly based on optical structures or radiowave scatterers. According to the estimate given in [16], the employed 160-bit elliptic curve signature will be secure until 2019. Signature security until the year 2050 is possible, again on the basis of elliptic curves, with key bitlength around 206 [16] and barcode sizes of still around 1 cm^2.

4 Physically Obfuscated Keys from Random Diodes

Random physical structures can also be used as a non-volatile storage for secret binary keys. Due to their disordered and/or tamper sensitive nature, they may be harder to

extract invasively than binary keys stored in EEPROM, for example. This concept has been termed a Physically Obfuscated Key (POK) [7], a Weak PUF [4] or also an obfuscating PUF [3]. Applications of POKs naturally include any cryptographic protocols based on secret binary keys, including hardware identification schemes of all sort. They are particularly well suited to store keys safely in small, inexpensive mobile systems, where effective key protection is otherwise difficult to achieve. As we are going to show, random ALILE-diodes can also be used as cheap, stable POKs with remarkably high information density.

Reliable Key Extraction. In the application of ALILE-diodes as POKs, our focus lies on the highly robust extraction of a string (the later key) from the $I(U)$ curves in Fig. 2a). In opposition to COAs, our helper data furthermore should not reveal any information about the binary key which it helps to extract from the POK (see also [17]), since the key must remain secret. We applied ideas taken from Linnartz et. al [18], where the y-axis of the verification measurement is split in equal sections, and the measured data points are shifted towards the arithmetic mean of these sections (i.e. away from the section borders in order to avoid bit flips) by the helper data.

Our data base were the $I(U)$-curves of the 16 diodes that we already used in section 3. Once more, we set the four supporting points at -1.3 V, -0.65 V, 0.65 V and 1.3 V. Our aim is to extract one bit from the current value at each of the four supporting points, four bits in total per $I(U)$-curve. Inspired by [18], we proceeded as follows: Firstly, we calculated at each supporting point k ($k = 1, \ldots, 4$) the median c_k of the current values of all diodes at this supporting point. Secondly, for each supporting point k, we divided the current-axis into 8 sections. Each section i ($i = 1, \ldots, 8$) its determined by its lower border b_i^k and upper border b_{i+1}^k, where $b_i^k = ((p+1)/(1-p))^{i-4} \cdot c_k$ for $i = 1, \ldots, 8$. In other words, the sections are of equal length on a logarithmic scale, and center around $b_4^k = c_k$. We choose $p = 0.5$ to compensate measurement errors of up to +/-50%. We further denote the arithmetic mean of the section i (with the borders b_i^k and b_{i+1}^k) as $m_{i,i+1}^k$. As is supported by our measurement data, we assume that the measurement points are distributed approximately uniformly over all sections. Under these circumstances, the helper data leaks few/none information about the extracted bit; see also [18].

During the enrollment phase of the POK at the manufacturer, we generate for every measurement s_k at the supporting point k helper data h_k in the following way:

$$h_k = \frac{m_{i,i+1}^k}{s_k} \quad \text{for the unique} \quad i \in \{1, \ldots, 8\} \quad \text{that satisfies} \quad b_i^k \leq s_k < b_{i+1}^k \quad (1)$$

During the verification the extracted bit $x(k)$ can be computed with a verification measurement v_k at supporting point k:

$$x(k) = \begin{cases} 0 & \text{if} \quad b_{2i}^k \leq h_k v_k < b_{2i+1}^k \\ 1 & \text{if} \quad b_{2i+1}^k \leq h_k v_k < b_{2i+2}^k \end{cases} \quad (2)$$

With $p = 0.5$ we could obtain 11 different bit strings out of the 16 diodes, while the helper data leaks less information about the bit strings. This means that at least 3 bits

per diode can be extracted in a stable manner and at an error compensation rate of 50% measurement deviation. Our results suggest the usability of one of the simplest and smallest electrical components – namely diodes – as POKs.

5 Machine Learning Resistant Strong PUFs via Crossbar Structures

A Strong PUF is a physical system S which meets the following requirements: (i) S can be excited with external stimuli or challenges C_i, upon which it reacts with corresponding responses R_{C_i}. (ii) It is infeasible, even for the original manufacturer of S, to produce a second system S' which has the same challenge-response-behavior as S. (iii) It is difficult for an adversary to correctly predict an unknown response R_C to a randomly chosen challenge C numerically, without conducting an actual measurement on S. This security feature shall hold even if many other challenge-response pairs (C_i, R_{C_i}) are known to the adversary, or if he had previous physical access to S for a limited period, during which he could conduct any physical measurement on S. In theory, these properties can be met due to the high disorder/information content and/or the complex internal model of S.

Applications of Strong PUFs include identification and key establishment between central authorities and mobile decentral systems [2] [19]. Their complex challenge-response behavior is sufficient to guarantee security in such applications. No execution of costly asymmetric schemes in the mobile systems is necessary.

Current candidates for electrical Strong PUFs contain only a relatively small (max. several hundreds) of *interacting* components. Thus, relatively few (again some hundred) internal parameters completely determine their behavior. This is one of the main reasons why basically all of them have been attacked successfully by machine learning techniques [3] [20]. An alternative design route to Strong PUFs, that has been suggested by our group in [21], is to employ as many (up to billions), densely packed random subunits as possible, which are read out *individually* and *independently* of each other. Our principle is comparable to a read-only memory with maximal size, random information content, and intrinsically limited read-out rate. We showed in [21] that large, monolithic, memory-like crossbar structures (Fig. 3b) based on random diodes are very well suited to realize this approach. Due to their simple and regular geometry, they can reach optimal information densities (up to 10^{10} to 10^{11} bits per cm^2). The crossbars can be designed in such a way that (i) parallel read-out of different memory units (i.e. diodes) is impossible; (ii) faster read-out than a preset limit leads to overloading and immediate destruction of the wiring, rendering the remaining structure unreadable. Note that the slow read-out rate is not enforced by an artificially slow access module or the like, but by the inductive and resistive capacitances of the structure itself [22].

The resulting Crossbar PUFs are provably immune against machine learning attacks: Their security merely depends on the access time of the adversary, and on the ratio of the already read-out bits vs. the number of overall bits stored in the structure. Modeling attacks subsequent to the read-out are fruitless, since all components are independent of each other. The exact security properties of Crossbar PUFs thereby depend on the employed circuit technology. With a 30nm technology, for example, Crossbar PUFs

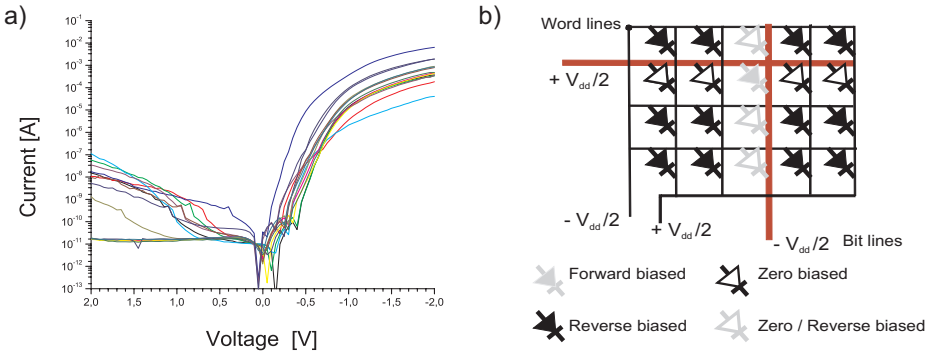

Fig. 3. a) $I(U)$ curves of diodes with high rectification rates; b) schematics of a crossbar structure

of size 1 cm^2 could achieve security of up to 3 years of continuous, uninterrupted adversarial access, while enabling read-out rates of 10^3 bits per second [21]. They could easily be implemented in plug-in devices and on chipcards. Note that all current Arbiter PUFs and variants that run at a 1 MHz CRP frequency become susceptible to modeling attacks after less than a second of uninterrupted adversarial read-out [3] [20].

One prerequisite left open in [21] was whether random diodes with a rectification ratio of at least 10^5 could be produced by inexpensive techniques. Such high rectification rates are necessary to realize stable read-out and to limit parasitic current paths in the monolithic, large crossbar [21] [22] . We have now been able to fabricate diodes with even higher rectification by use of the ALILE process (Fig. 3 a). They indeed enable the first electrical PUFs that remain secure in the face of adversarial access of up to years and against machine learning attacks, further illustrating the security potential of random diodes. We suggest the term SHIC PUFs (pronounce as *"chique PUFs"*) for this new type of PUF, where the acronym SHIC stands for Super High Information Content.

6 Summary

We have argued on the basis of real measurement data and prototypical implementations that random, irregular diodes can be applied for the construction of COAs, POKs and Strong PUFs at the same time. They have the advantage of being one of the smallest and simplest electrical components, and that they can be produced by inexpensive methods. This gives them a strong potential for physical cryptography applications.

Acknowledgements

The presented work was conducted within the Physical Cryptography Project at the TU München. We acknowledge financial support by the International Graduate School of Science and Engineering (IGSSE) and the Institute for Advanced Study (IAS) at the TU München. We thank Michael Scholz and Matthias Bator for useful discussions.

References

1. Bauder, D.W.: An Anti-Counterfeiting Concept for Currency Systems. Research report PTK-11990. Sandia National Labs, Albuquerque, NM (1983)
2. Pappu, R., Recht, B., Taylor, J., Gershenfeld, N.: Physical One-Way Functions. Science 297, 2026–2030 (2002)
3. Rührmair, U., Sölter, J., Sehnke, F.: On the Foundations of Physical Unclonable Functions, http://eprint.iacr.org
4. Tuyls, P., Schrijen, G.J., Skoric, B., van Geloven, J., Verhaegh, N., Wolters, R.: Read-Proof Hardware from Protective Coatings. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 369–383. Springer, Heidelberg (2006)
5. Vijaywargi, D., Lewis, D., Kirovski, D.: Optical DNA. In: Financial Cryptography 2009, pp. 222–229 (2009)
6. DeJean, G., Kirovski, D.: RF-DNA: Radio-Frequency Certificates of Authenticity. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 346–363. Springer, Heidelberg (2007)
7. Gassend, B.: Physical Random Functions, MSc Thesis, MIT (2003)
8. Nast, O., Wenham, S.R.: Elucidation of the layer exchange mechanism in the formation of polycrystalline silicon by aluminum-induced crystallization. Journal of Applied Physics 88, 124–132 (2000)
9. Nast, O., Hartmann, A.J.: Influence of interface and Al structure on layer exchange during aluminum-induced crystallization of amorphous silicon. Journal of Applied Physics 88, 716–724 (2000)
10. Antesberger, T., Jaeger, C., Scholz, M., Stutzmann, M.: Structural and electronic properties of ultrathin polycrystalline Si layers on glass prepared by aluminum-induced layer exchange. Appl. Phys. Lett. 91, 201909 (2007)
11. Jaeger, C., Algasinger, M., Rührmair, U., Csaba, G., Stutzmann, M.: Random pn-junctions for physical cryptography. Appl. Phys. Lett. (Submitted 2010)
12. Berkemeier, J., Dirksmeyer, T., Klempt, G., Purwins, H.-G.: Pattern Formation on a Nonlinear Periodic Electrical Network. In: Zeitschrift für Physik B Condensed Matter. Springer, Heidelberg (1986)
13. Laughton, M.: (2009), http://www.libdmtx.org/documentation.php
14. Zhang, F., Safavi-Naini, R., Susilo, W.: An efficient signature scheme from bilinear pairings and its applications. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 277–290. Springer, Heidelberg (2004)
15. Lynn, B., et al. (2009), http://crypto.stanford.edu/pbc/
16. Lenstra, A.K.: Selecting cryptographic key sizes. Journal of Cryptology (2001)
17. Guajardo, J., Kumar, S., Schrijen, G., Tuyls, P.: FPGA Intrinsic PUFs and Their Use for IP Protection. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 63–80. Springer, Heidelberg (2007)
18. Linnartz, J.P., Tuyls, P.: New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. In: Kittler, J., Nixon, M.S. (eds.) AVBPA 2003. LNCS, vol. 2688, pp. 393–402. Springer, Heidelberg (2003)
19. Suh, G.E., Devadas, S.: Physical Unclonable Functions for Device Authentication and Secret Key Generation. In: DAC 2007, pp. 9–14 (2007)
20. Rührmair, U., Sehnke, F., Soelter, J., Stoyanova, V., Dror, G., Schmidhuber, J.: Machine Learning Attacks on Physical Unclonable Functions (Submitted 2010)
21. Rührmair, U., Jaeger, C., Bator, M., Stutzmann, M., Lugli, P., Csaba, G.: Cryptographic Applications of High-Capacity Crossbar Memories. IEEE Transactions on Nanotechnology (Submitted 2009)
22. Csaba, G., Lugli, P.: Read-out design rules for molecular cross bar architectures. IEEE Transactions on Nanotechnology 8(3), 369–374 (2009)