Random pn-junctions for physical cryptography

C. Jaeger,[1,a)] M. Algasinger,[1] U. Rührmair,[2] G. Csaba,[3] and M. Stutzmann[1]
[1]*Walter Schottky Institut, Technische Universität München, Am Coulombwall 3, 85748 Garching, Germany*
[2]*Computer Science Department, Technische Universität München, Boltzmannstrasse 3, 85748 Garching, Germany*
[3]*Institute for Nanoelectronics, Technische Universität München, Arcisstrasse 21, 80333 München, Germany*

(Received 30 December 2009; accepted 23 March 2010; published online 27 April 2010)

In this paper, we report on high-rectification pn-diodes (rectification ratios up to 2×10^7) prepared by aluminum-induced crystallization on crystalline Si-wafers, which exhibit highly random I(V) characteristics. We argue that arrays of such diodes can be employed as physical uncloneable functions for cryptography. To resolve the structure of the active diode area, focused-ion beam imaging was used. The I(V) curves of the diodes reveal that both a smaller polycrystalline silicon film thickness and a smaller diode size lead to increasing randomness due to the increasing inhomogeneity of thinner films and due to more pronounced grain boundary effects for smaller diodes. © *2010 American Institute of Physics*. [doi:10.1063/1.3396186]

Traditional cryptographic methods purely rely on mathematical assumptions and are vulnerable against increasingly powerful computers and the development of better breaking algorithms. For this reason physical cryptography receives increasing attention: exploiting the inherent complexity and irreproducibility of physical (nanoscale) systems may provide fundamentally higher security than purely numerical schemes. One of the central tasks in this emerging field is to find systems that can be regarded as secure physical uncloneable functions (PUFs). An ideal PUF (i) contains a very high amount of structural information, (ii) this information can be reliably extracted to create stable challenge-response pairs (CRPs), (iii) the rate at which the information is extractable, and the high number of the CRPs, prevent full characterization within short time by an adversary, and (iv) no computational model can numerically predict or imitate the PUF's challenge-response behavior. It seems that complex, random optical scatterers[1] can serve as secure PUFs, but the required precision measurement and accurate alignment makes this method impractical for practical applications. Electrical realizations would by far be preferable due to their comparatively uncomplicated read-out. Nevertheless, building a secure circuit-based PUF proved to be elusive; small-scale circuits exploiting the inherent hidden internal time delays[2] turned out to be insecure against model building attacks.[3,4]

Diode-backed crossbars are high integration density memory arrays,[5] which are believed to have a large impact on future memory technologies.[6] We propose crossbars with fixed (nonwritable), random information content as PUFs. The information content is stored in random diodes located at each crossing, determining challenge response pairs by their stable, but random, current-voltage characteristics. Due to the random fabrication process, which cannot even be reproduced by the manufacturer himself, every crossbar PUF can practically be regarded unique. The schematics and the bias scheme of such a crossbar are shown in Fig. 1. Diodes with a I_{on}/I_{off} ratio $>10^5$, which have the capability to strongly delimit parasitic currents, can yield an addressable crossbar of $N=n\times n$ capacity.[7,8] If accessible only by a $k<100$ bit/s rate, the crossbar requires time $T>N/k$ (i.e., years) for a full adversarial characterization.[7] Such slow read-out rates can be realized by the parasitic resistances and capacitances in case a gigabit-sized ($n=10^5$) array is realized in one monolithic block with a single decoder/amplifier circuit.[7] The slow read-out rate and the very high random information content are the key components of the proposed system. We called this PUF-category a SHIC PUF in Refs. 7 and 9 where the acronym SHIC stands for super high information content. Crossbar structures with random diodes are one preferable way to implement SHIC PUFs.

As already mentioned, the information content of a crossbar-based SHIC PUF stems from the random characteristics of the individual diodes at the crossings, which ideally are caused by a nonreproducible preparation process. Random TFT components in a small addressable (memorylike) configuration were already proposed as artificial fingerprint devices (AFD).[10,11] We would like to mention here that an AFD is fundamentally different from a SHIC PUF, which requires a very large number of CRPs—for example, on the

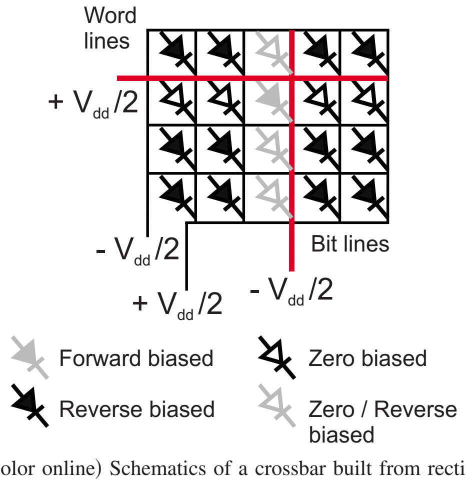

FIG. 1. (Color online) Schematics of a crossbar built from rectifying junctions. A *nxn* size crossbar to be accessible requires diodes with at least $I_{on}/I_{off}>n$ rectification ratio. By applying the presented biasing scheme, the light gray diode is addressed by biasing it in forward direction ($V=V_{dd}$), while all other diodes are zero biased or reverse biased ($V=-V_{dd}$).

[a)] Electronic mail: jaeger@wsi.tum.de.

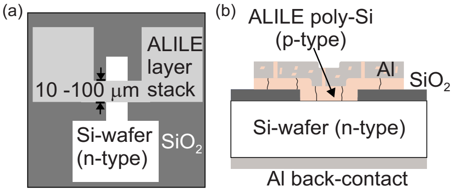

FIG. 2. (Color online) (a) Sketch of the silicon wafer covered with SiO$_2$. The active area is structured by wet chemical etching and by defining the ALILE precursor layers in a mask step. (b) Schematics of a vertical cut through the pn-diode structure. The poly-Si is prepared by ALILE on an n-type Si wafer.

order of 10^{10} different CRPs for the implementation presented in Ref. 7.

Although the aluminum-induced layer exchange (ALILE) method[12,13] already has been used to prepare crossbar structures,[7] in this paper we focus on the fabrication of the individual diodes, which are produced by aluminum-induced crystallization on n-type Si-wafers.[14] Hereby, silicon/Al/oxide/amorphous silicon (a-Si) layer structures are annealed at temperatures below the eutectic temperature of the Al-Si system (577 °C), leading to a complete layer exchange and the crystallization of the a-Si.[12,13] After the annealing step, a closed polycrystalline silicon (poly-Si) layer is formed on the substrate, which is covered with a network of Al+Si-islands (hillocks).[12,15,16] The inherently random nature of such crystallization processes makes them interesting for producing diodes with unique properties, since the actual crystallization sites cannot be predicted or controlled. Indeed, random I(V)-characteristics were found, whereas the diode characteristics strongly depend on the wafer doping, diode size, and poly-Si thickness.

N-type silicon wafers (ρ=0.003–0.007 Ω cm and ρ =1–10 Ω cm) covered with a 100 nm thick thermal oxide [dark gray area, Fig. 2(a)] were used as a substrate for the crystallization process. To define the active area (10^2, 20^2, and 100^2 μm^2), the SiO$_2$ was structured by photolithography and removed by wet chemical etching in buffered HF solution [white area, Fig. 2(a)]. After a second lithography step,[17] the precursor layers for the ALILE process (Al/oxide/a-Si) were deposited. The details of the layer preparation are described elsewhere.[18] In the following, the photoresist was removed leaving behind the precursor layers only in the prestructured area [light gray area, Fig. 2(a)]. After that, the samples were annealed in dry N$_2$ atmosphere at 550 °C until the layer exchange was completed. The poly-Si layer thickness was 20, 50, and 100 nm. A sketch of the diode structure after annealing is shown in Fig. 2(b). Electrical contacts to the diodes were made by directly contacting the Al+Si-hillocks top layer formed after the layer exchange and Al evaporated on the backside of the Si wafers, resulting in a sandwich structure.

To gain insight into the growth of the closed poly-Si layer over the oxide/Si-wafer edge, focused-ion beam (FIB) micrographs in SEM mode were made (Fig. 3). Due to the high material contrast of this method,[19] Al, Si, and SiO$_2$ can be clearly distinguished. We observed a smooth transition of the crystallized poly-Si from the SiO$_2$ to the Si wafer, which seems to be facilitated by the tapered SiO$_2$ etching edge. The poly-Si/Si wafer interface is not resolved by the FIB image. Therefore, it is indicated by a horizontal dotted line. Within the closed poly-Si, an Al island can be seen, which indicates the poly-Si/wafer interface. Small Al clusters have already been observed in former studies,[20] which were reported to constitute 5% of the closed poly-Si. A statistic made from all our FIB micrographs is in good agreement with this value. These Al islands are considered to form parasitic rectifying Schottky diodes with the Si-wafer, as we found rectifying I(V)-curves in test samples where Al was evaporated directly on the Si wafer.

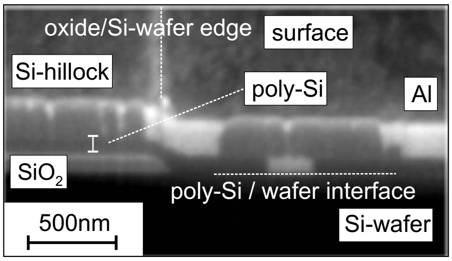

FIG. 3. FIB image of the poly-Si/Al+Si-hillocks layer system at the oxide/Si-wafer edge (vertical dashed line). The poly-Si/Si-wafer interface is indicated by the dashed horizontal line. Due to the high material contrast of this method, the Al, Si, and SiO$_2$ can be clearly distinguished.

In the following, we will present I(V)-characteristics obtained from measurements at room temperature of the different pn-diodes (Fig. 4). Since we observe considerable scattering of the diodes on one chip (which is highly appreciated for the application in cryptography), we always chose the best diode for each parameter set. For those diodes prepared on the highly doped wafer [Fig. 4(a)], we found only a weak rectifying behavior. This can be explained by the comparably high carrier concentrations of the Si-wafer ($n \approx 10^{19}$ cm^{-3}) and the poly-Si film [$p = 5 \times 10^{18}$ cm^{-3} to 9×10^{19} cm^{-3} (Ref. 18)]. For such high carrier concentrations the depletion region width is of the order of 10 nm and it can therefore be assumed that considerable tunneling prevails. These diodes already have some use in cryptography, since they exhibit very random I(V) characteristics,[9] but their rectification is insufficient for crossbar applications. For the weakly doped wafer, on the other hand, the I(V)-curves of the diodes exhibit high rectification ratios up to 2×10^7 [Fig. 4(b)]. In that case, the depletion region is fully located within

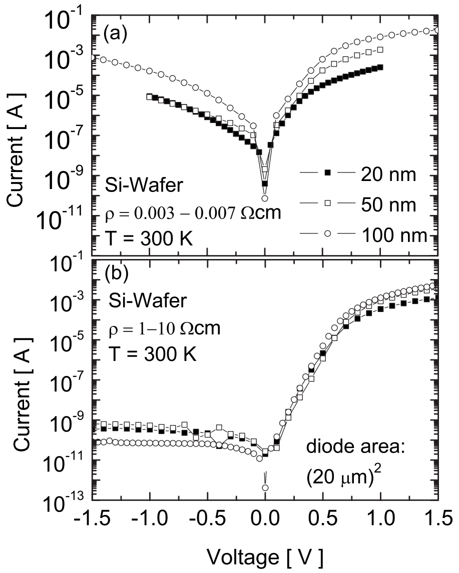

FIG. 4. Current-voltage characteristics of 20, 50, and 100 nm thin poly-Si diodes on (a) the highly doped and (b) the weakly doped Si-wafer. Due to the different scattering of the curves, always the best diode was chosen for each parameter set.

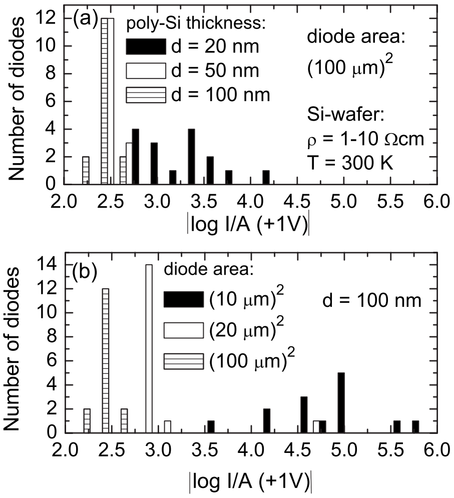

FIG. 5. (a) Histogram of $|\log I/A(+1\ \text{V})|$ at 1 V for the different diode thicknesses for a diode size of (100 μm)^2. (b) Histogram of $|\log I/A(+1\ \text{V})|$ at 1 V for the different diode sizes for a poly-Si thickness of 100 nm.

the c-Si, and one-sided abrupt junctions should prevail. Nevertheless, the thin poly-Si emitter layer leads to considerable randomness in the I(V)-curves.

To identify possible design rules for the proposed crossbar structures, it is of importance to understand the origin of the randomness in our diode characteristics. Figure 5(a) displays a histogram of $|\log I/A(+1\ \text{V})|$ measured at 1 V for the (100 μm)^2-diodes on the weakly doped Si-wafer depending on the film thickness. While the randomness (spread of the histogram over the $|\log I/A(+1\ \text{V})|$) is comparable for the 50 and 100 nm thick films, it is considerably larger for $d_{\text{poly-Si}}=20$ nm. This shows that a smaller film thickness leads to increasing inhomogeneity of the films, which results in the observed increase in diode randomness. It can be also seen that the average forward current is decreasing for smaller film thicknesses, as it was already observed for the diodes on the highly doped wafer [compare Fig. 4(a)]. This can be attributed to a higher series resistance for thinner poly-Si films. In addition to the film thickness, the diode size has a considerable influence on the randomness of the I(V)-curves [Fig. 5(b)]. For a poly-Si thickness of 100 nm, where only little randomness should stem from the film thickness itself, we find little randomness for the (100 μm)^2 and (20 μm)^2-diodes. Smaller diodes, on the other hand, exhibit randomness over more than two orders of magnitude. This can be attributed to a stronger fluctuation of the grain boundaries in the active area for smaller diodes, while for large diodes grain boundary effects are averaging out. This is consistent with the grain size of our poly-Si films of 1–5 μm. An additional source of randomness should be the presence of the small Al clusters/Si-wafer junctions (see Fig. 3), which basically are in parallel to the much larger poly-Si/Si-wafer pn-junctions.

As can be seen in Fig. 5(b), the current values for a fixed voltage of all diodes on one chip are randomly distributed. This is important, since in a crossbar PUF, a threshold current could separate the current values identified as "0" or "1." Here, the highest information content will be obtained for a "1"/"0" ratio of one.

Moreover, the prepared ALILE pn-diodes exhibit a very good long-time stability showing no noticeable changes in the I(V)-characteristics, at least over the examined time span of 1 year. This is obviously crucial for proper device operation. Also the temperature stability of the diodes is sufficient, since we found a change in the forward current for diodes on the weakly doped wafer of approximately a factor of 2 for changing the temperature between −25 and 40 °C. This is negligible compared to the huge span of current values of over more than two orders of magnitude caused by the inherent randomness of the ALILE process (cf. Fig. 5). A comparison of different diodes could also be used for extracting the stored information, which would compensate for unwanted temperature effects.[11] Furthermore, the reliably extracted information content per diode merely needs to be on the order of one or a few bits.[9]

The actual fabrication of the proposed crossbar PUFs could be achieved by ion implantation of the word lines to a Si-wafer and by using structured ALILE layers as bit lines.[7] The scope of this work is to test the potential of the ALILE preparation method and to derive design rules for crossbar PUFs, rather than to fabricate the crossbar structure, which is for the most part a technological task.

In conclusion, we found that poly-Si diodes prepared by ALILE on Si-wafers exhibit sufficient randomness and rectification for the use in the proposed crossbar structures. The diode size and film thickness have a considerable influence on the randomness of the resulting I(V)-curves. Therefore, ALILE poly-Si layers can help to increase the randomness in the design of the proposed crossbar PUFs. Furthermore, the diode size has to be adjusted to the grain size of the films.

This work was conducted within the Physical Cryptography Project at the TU München. We acknowledge financial support by the IGSSE and the IAS of the TU München.

[1] R. Pappu, B. Recht, J. Tayler, and N. Gershenfeld, Science **297**, 2026 (2002).
[2] G. Suh and S. Devadas, Proceedings of the 44th Annual Conference on Design Automation, 2007, p. 9.
[3] D. Lim, Master thesis, MIT, 2004.
[4] U. Rührmair, J. Sölter, and F. Sehnke, http://eprint.iacr.org, 2009.
[5] M. R. Stan, P. D. Franzon, S. Goldstein, J. C. Lach, and M. M. Ziegler, Proc. IEEE **91**, 1940 (2003).
[6] S. Möller, C. Perlov, W. Jackson, C. Taussig, and S. R. Forrest, Nature (London) **426**, 166 (2003).
[7] U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, and G. Csaba, "Applications of High-Capacity Crossbar Memories in Cryptography," IEEE Trans. Nanotechnol. (to be published).
[8] G. Csaba and P. Lugli, IEEE Trans. Nanotechnol. **8**, 369 (2009).
[9] U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba, and M. Stutzmann, Financial Cryptography and Data Security 2010, LNCS 6052.
[10] S. Maeda, H. Kuriyama, T. Ipposhi, S. Maegawa, and M. Inuishi, Tech. Dig. - Int. Electron Devices Meet. **2001**, 759.
[11] S. Maeda, H. Kuriyama, T. Ipposhi, S. Maegawa, Y. Inoue, M. Inuishi, N. Kotani, and T. Nishimura, IEEE Trans. Electron Devices **50**, 1451 (2003).
[12] O. Nast and A. J. Hartmann, J. Appl. Phys. **88**, 716 (2000).
[13] O. Nast and S. R. Wenham, J. Appl. Phys. **88**, 124 (2000).
[14] On crystalline silicon wafers this process has been initially called solid phase epitaxy in literature (Refs. 15 and 20).
[15] G. Majni and G. Ottaviani, Appl. Phys. Lett. **31**, 125 (1977).
[16] P. Widenborg and A. G. Aberle, J. Cryst. Growth **242**, 270 (2002).
[17] C. Jaeger, T. Antesberger, and M. Stutzmann, J. Non-Cryst. Solids **354**, 2314 (2008).
[18] T. Antesberger, C. Jaeger, M. Scholz, and M. Stutzmann, Appl. Phys. Lett. **91**, 201909 (2007).
[19] T. K. Olson, R. G. Lee, and J. C. Morgan, The 18th International Symposium for Testing and Failure Analysis, ISTFA 92, Los Angeles, 1992.
[20] G. Majni and G. Ottaviani, J. Cryst. Growth **46**, 119 (1979).