# Examination of distribution regularities in static RAM microcircuit cells in case of using them as a physically unclonable function in a mutual authentication module

George S. Aliev
Institute of Information Technologies & Telecommunications
North-Caucasus Federal University
georgyaliev@gmail.com
Oleg V. Malsugenov
Institute of Information Technologies & Telecommunications
North-Caucasus Federal University
omalsugenov@ncfu.ru

Oksana S. Mezentseva
Institute of Information Technologies & Telecommunications
North-Caucasus Federal University
28mos05@mail.ru

## Abstract

The item offers a view on the outcomes of a study focusing on static memory microcircuits seen as a physically unclonable function for devices with mutual authentication. An experimental units has been developed, as well as a series of measurements has been performed in static memory microcircuit cells at the point of initialization; an analysis has been performed for values distribution in cells for the measurements series. Values have been calculated for auto-correlational functions at various sets of values. An attempt has been made to explain the observed regularities and define requirements for static RAM microcircuits when using that as a physically unclonable function.



## 1 Introduction

The field of cryptography, based on the structural complexity of optical and electronic physical systems, and called physical cryptography, is one of the most recent advances in the field of cryptography and data protection [Yarm11, Papp02, Papp01, Gass02, Gass03]. Along with quantum cryptography [Eker91, Benn92] and cryptography based on the use of chaotic dynamic systems [Koca01], physical cryptography uses noise-like behavior of physical objects and systems [Papp02]. This allows mostly ensuring higher requirements (as compared to classical algebraic cryptography) for such parameters of cryptographic systems as diffusion and confusion [Shan49].



In: S. Hölldobler, A. Malikov (eds.): Proceedings of the YSIP-3 Workshop, Stavropol and Arkhyz, Russian Federation, 17-09-2019–20-09-2019, published at http://ceur-ws.org

The major object of physical cryptography is a physically unclonable function (PUF), which is a function embodied in a physical structure, and which is easy to evaluate, yet difficult to describe, simulate, or reproduce. A physical structure containing PUF consists of many random components. Such components are introduced through manufacturing process and are uncontrollable. PUF is a physical system that, when requested, generates a unique, unpredictable response. The major requirement for PUF is its irreversibility. A PUF has two important properties absolute impossibility of creating a physical copy of it; impossibility of creating an exact mathematical model of a PUF, i.e. of calculating a response in case the exact inquiry parameters and other pairs of inquiry-responses are known. These features taken together make up the concept of unclonability.

In PUF, randomness can be established by various physical processes and phenomena. Among the PUFs, we can differentiate a class where disorder is introduced by external factors, and a class where internal disorder is used.

The first class PUFs include

- optical PUFs consisting of a transparent material with randomly distributed light reflecting particles introduced in it;
- PUF coatings created on the top layer of integrated circuits.

The other PUF class includes:

- silicon PUFs, which employ random variations of delays in the conductors and gates of field-effect transistors;
- PUFs based on SRAMs, which use deviations existing for the materials used in the equipment manufacture;
- magnetic PUFs, which are produced by adding barium ferrite particles to the paste through production.

The main application areas for PUFs include authentication, data copyprotection on a storage device; development of cryptographic keys. Static random access memories (SRAM) are widely used in computer technology for data storage. A direct storage element (cell) of a SRAM consists of four transistors that implement two inverters with cross-feedback [Oztu08]. Such a cell is always in one of two states, which, in turn, allows using it for storing one bit of information.

An example of such a cell can be seen from an RS-flip-flop, implemented on two 2AND-NOT logical elements. When the voltage is supplied, all the cells of the SRAM are set to one of two possible states; besides, due to the RS-flip-flop symmetry, it is not known beforehand which final state the cell will get, 0 or 1. This state is random and depends on numerous factors [Holo08]. This is due to the microchips manufacturing technology specifics and the multitude of asymmetric elements in each SRAM cell [Yarm11].

Such elements include the lengths of the connecting conductors, their geometrical dimensions, the heterogeneity of silicon physical and chemical properties, the signal delay deviation, etc.

Work [Guaj07] shows that only for a part of an SRAM cells their state after voltage supply is truly random, while it often approaches a uniform distribution. The remaining cells steadily adopt the value of 0 or 1 state. The fact that the number of random values for an SRAM cells states under voltage is limited, has been proven experimentally in [Maes08]. The result showed that more than 90% of the examined SRAM cells were always set to state 0, less than 10% of the cells, to state 1 only, and only less than 1% of the cells were set with an equal probability to 0 or 1 state [Maes08].

These outcomes suggest that PUF-based SRAMs are very unreliable, especially with respect to programmable matrices (FPGA). This can be accounted for by the fact that, due to the regular topology of the FPGA, any symmetric element (e.g., an RS-flip-flop) implemented on the FPGA nearly always contains predictable asymmetry. Therefore, the proposed study presents an attempt to examine the values distribution patterns in specialized SRAM microcircuit cells during their initialization.

## 2 Identifying static features for SRAM cell values

As samples, ten static HM62256 RAMs from different manufacturers (Hynix, Toshiba, Hyundai) were used. The main goal for this stage was to identify the statistical properties of the values in the static RAM microcircuit cells when using them as physically unclonable functions. The main objectives for the study included: determining the number of stable and unstable memory cells, the number of stable and unstable bits, detecting periodic patterns in the development of the static RAM microcircuit initialization values. Figure 1 offers a view on the scheme of the experimental device.

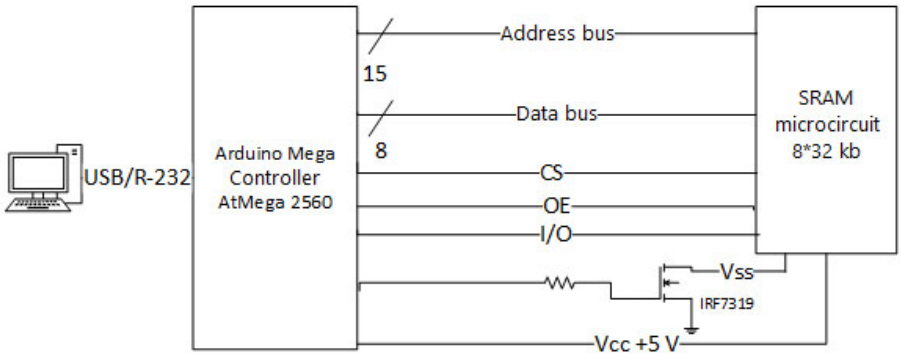


Figure 1: Experimental device scheme.

It consists of a universal Arduino Mega module based on the Atmel 2560 processor, static RAM microcircuits, a quick-release panel for memory microcircuits, a transistor switch for controlling the device power supply. Each memory microcircuit was polled 100 times 100 ms after the power was turned on. The most typical outcomes of the values distribution in the SRAM microcircuit cells can be seen on distribution maps 2-4. An analysis of the data presented shows that for all the examined samples the following condition was met

$$N_{stab} * 8 < n_{stab} \tag{1}$$

where $N_{stab}$ is the number of stable bytes, nstab is the number of stable bits. Expression 1 is valid for all the examined samples. This confirms that part of the bits in unstable cells maintain stable values. This fact limits the range of random values generated in the memory cells through initialization. For example, using an initialization vector of 8 bytes (64 bits), provided that the probability of the occurrence of values in each byte is distributed uniformly, produces, under brute-force-on, $2^{64} = 18446744073709551616$ values, while if it is not 8 but 4 bits change in each byte, the others remaining stable, then under the condition of brute-force-on, the number of unique combinations shall be reduced down to $2^{32} = 4294967296$ values. In the case a static memory microcircuit is used as a pseudo-random sequence generator, then the probability density function is to be as close to uniform as possible. If using static RAM as a carrier for the initialization vector and key data, then lack of stable cells will not allow using them.

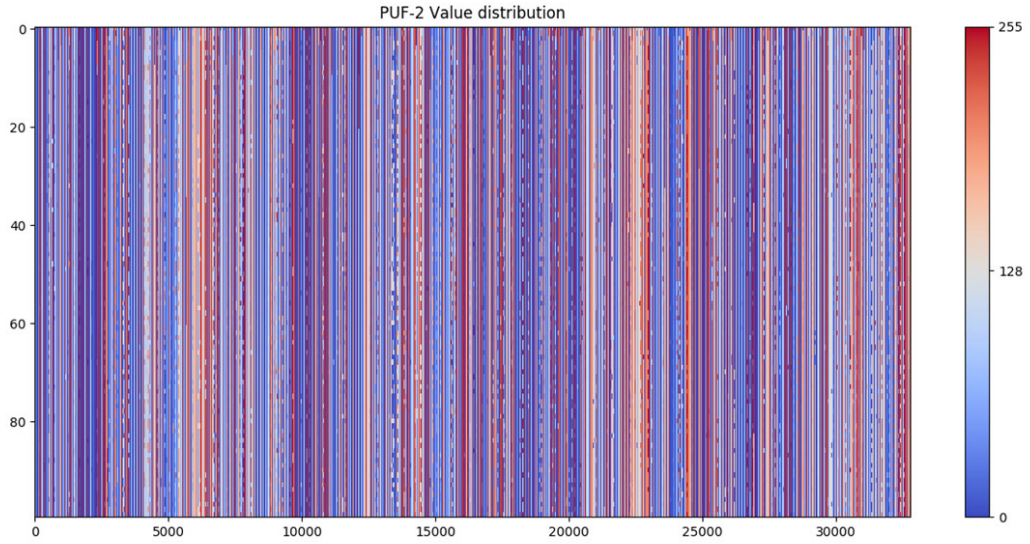


Figure 2: Distribution map for the values in the SRAM #2 sample for 100 measurements.

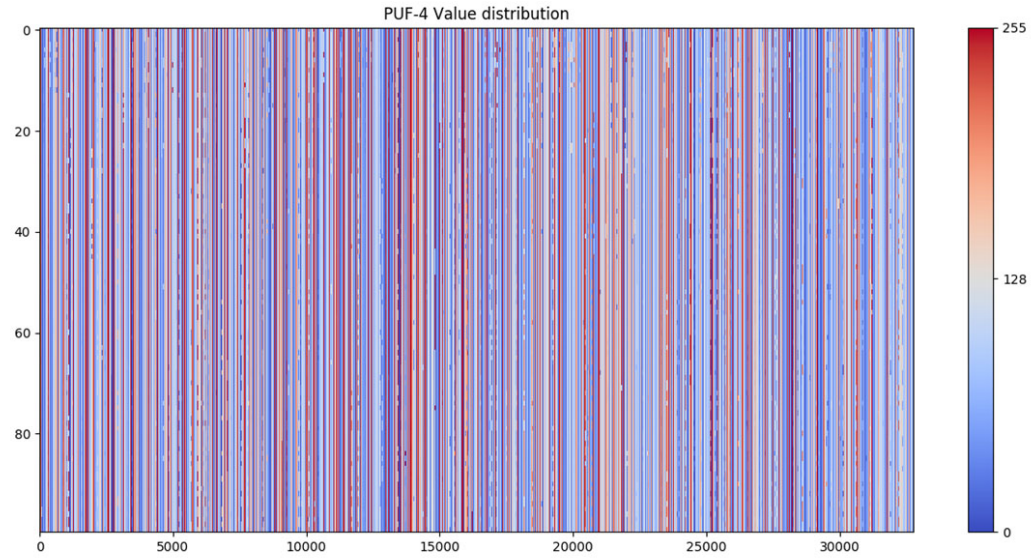


Figure 3: Distribution map for the values in the SRAM #4 sample for 100 measurements.

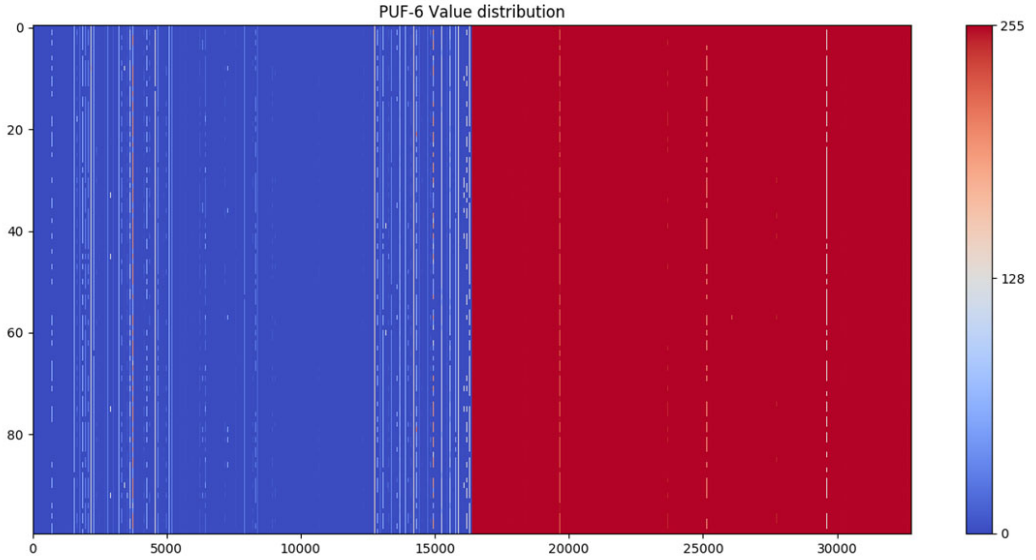


Figure 4: Distribution map for the values in the SRAM #4 sample for 100 measurements.

Therefore, an optimization arises concerning reducing the predictability of the initialization vector on the one hand and, on the other, regarding increasing the reliability of detecting the initialization vector shift in the memory sculpture.

The distribution maps for the values in memory cells for the most typical samples (2, 4 6) for 100 measurements can be seen from Figures 2 through 4. Cell addresses are plotted on the abscissa and the measurement number can be seen on on the ordinate axis. Each map has a color highlight to shows the value in the memory cell within the range of 0 to 255. As the maps above show, samples 2 and 4 have a fairly random distribution, while sample

2 features periodically repeating areas with zero and unit values predominating. Sample 6 (and generally, all the samples 6 to 10) have two distinct areas with the values 0 and 1 predominating.

Solid vertical lines on the maps indicate stable values; the color indicates the value in a particular cell. Broken vertical lines denote unstable cells. The pseudo-sound alternation of solid and broken lines, as well as the different color of solid lines, is an important feature of an ideal physically unclonable function proposed for use in a mutual authentication device.

## 3 Identifying autocorrelation for a discrete binary value

Studying the periodicity, and its quantitative evaluation, was performed through the autocorrelation function calculation. In general, the following expression is used to calculate the autocorrelation function.

$$C(\tau) = (x, x_\tau) = \int_{-\infty}^{+\infty} x(t)\, x(t-\tau)\, dt \tag{2}$$

In the event of a discreet signal, expression (2) shall be modified in the following way

$$C(n) = \sum_{j=-\infty}^{+\infty} x_j\, x_{j-n} \tag{3}$$

Subject to [Blah86] for a discreet binary sequence expression (3) shall be modified like follows

$$C(n) = \sum_{j=0}^{Nk-1} (-1)^{a_j + a_{j+\tau}}\ for\ 0 \leq \tau \leq Nk-1 \tag{4}$$

In view of normalization, expression (4) shall look like

$$C(n) = \frac{1}{Nk-1} \sum_{j=0}^{Nk-1} (-1)^{a_j + a_{j+\tau}}\ for\ 0 \leq \tau \leq Nk-1 \tag{5}$$

where $Nk$ is the total number of bits in the SRAM cells, $\tau$ is the shift in bytes respective the zero address, $a_j$ is the j-th bit value.

The meaning of function $C(n) = \pm 1$ points at the correlation between the discreet sequence bits or the location of the signals in phase opposition. The value $C(n) = 0$ shows that there is no correlation between the binary sequence and its copy shifted $\tau$ bits respective the original. From the point of ensuring the initialization vector safety, the detection of a correlation indicates a decrease in the number of unique combinations and, as a consequence, a decrease in resistance to brute force attacks. The calculation results for the autocorrelation function for samples 2, 4, and 6 are shown in Figures 5-7.

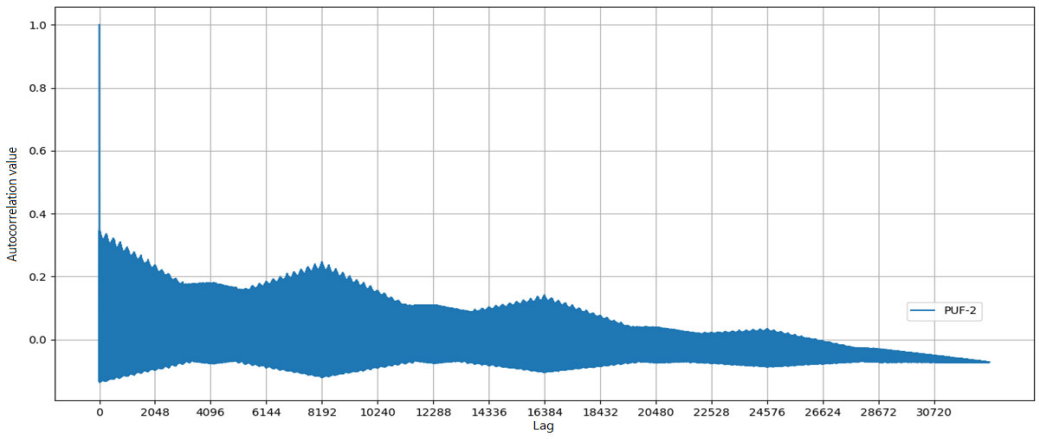


Figure 5: Dependence of autocorrelation function for sample 2 on tau discreet binary sequence shift.

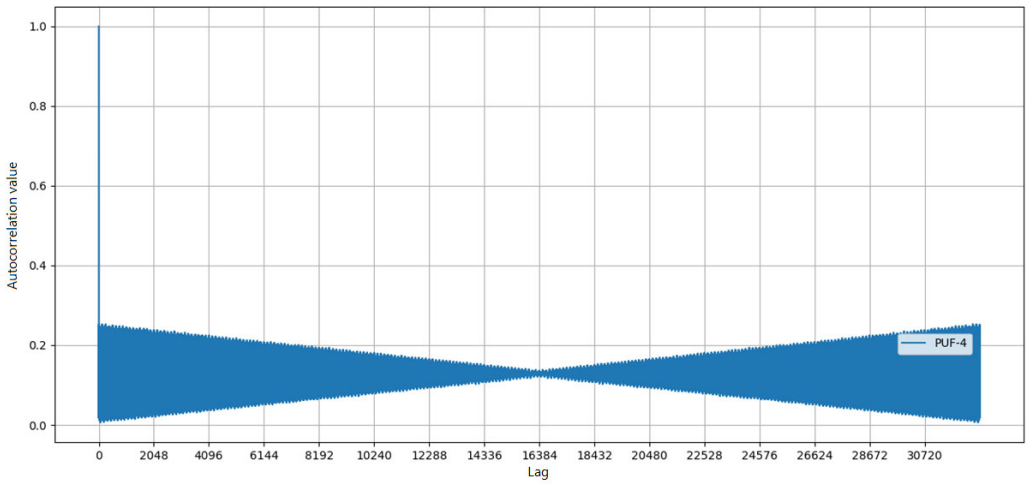


Figure 6: Dependence of autocorrelation function for sample 4 on tau discreet binary sequence shift.

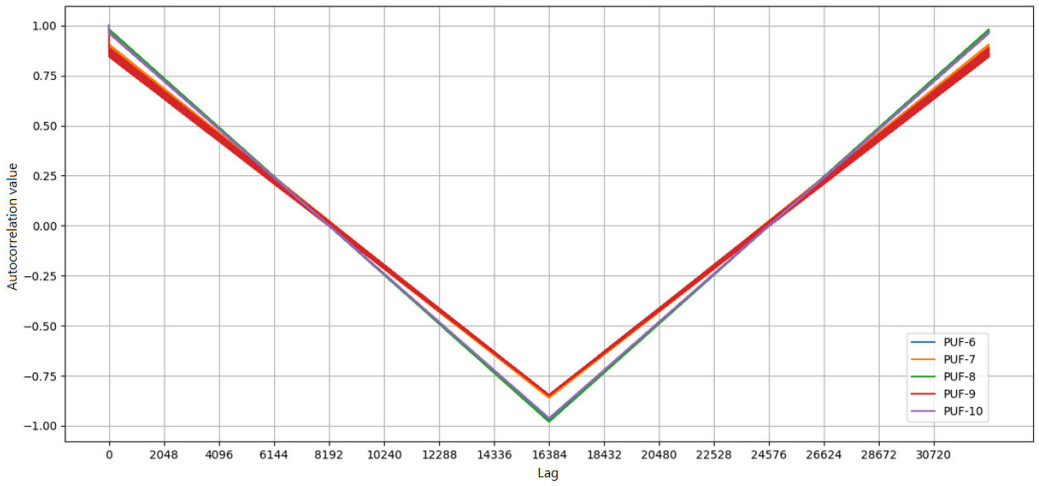


Figure 7: Dependence of autocorrelation function for samples 6-10 on tau discreet binary sequence shift.

As can be seen from the graphs, all the autocorrelation function values have a clearly observed periodicity. An analysis of the static RAM microcircuit design shows that most manufacturers use a modular layout, where the microcircuit consists of several memory banks placed on a single chip, yet spaced apart spatially.

Common to memory banks are power buses, the data/address multiplexer. Therefore, samples 1, 2, 4, 6-10 contain two banks of 16 kB each, whereas the remaining samples are built of 4-kilobyte blocks. Without getting deeper into the details of the microcircuit solution, we can mention the implementation feature associated with the mirror image of the microcircuits semiconductor layers mask.

The analysis of numerical values in view of the recommendations made in the literature and in article [Bohm10, Blah86] result in the following similarity criteria: at $0 \leq C_n \leq 0.25$ the autocorrelation is absent or poorly expressed; $0.25 < C_n \leq 0.7$ the autocorrelation is moderately expressed, i.e. insufficient for clear identification of periodic patterns; $C_n > 0.7$ prominent autocorrelation.

Therefore, in case of the given dependencies, only sample 4 has a weak autocorrelation, i.e. has low self-similarity. The use of this criterion can be accounted for by the need to use, for the initialization vector, sequences, which are poorly similar to each other with a slight difference in the initial shift. Given the insignificance of

the total unique sequence value for the considered samples $2^{15} = 32768$, it is rather important not to create an additional possibility for a successful attack on unauthorized access to the transmitted initialization vector. This vulnerability can be implemented by repeated intercepting and analyzing the transmitted initialization vector and restoring the static RAM card.

Therefore, ensuring protection of a mutual authentication module against unauthorized cloning, will take ensuring the closest to uniform distribution of values in stable and unstable cells.

## 4 Examination of PUF cell values distribution based on the static RAM

The study included an analysis of the stable and unstable cells values for static RAM samples. Figures 8-10 show the frequency graphs for the values appearance of stable cells in the SRAM samples 2, 4 and 6.

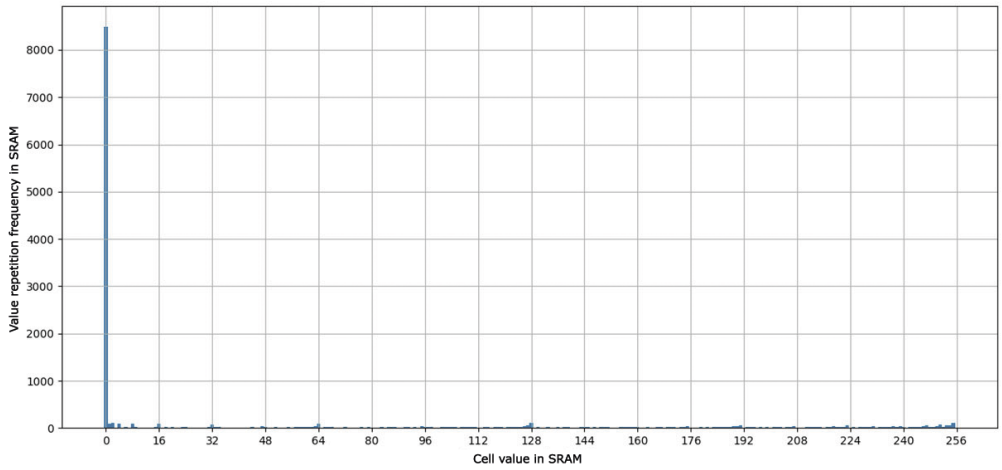


Figure 8a: Values frequency distribution in sample 2 cells.

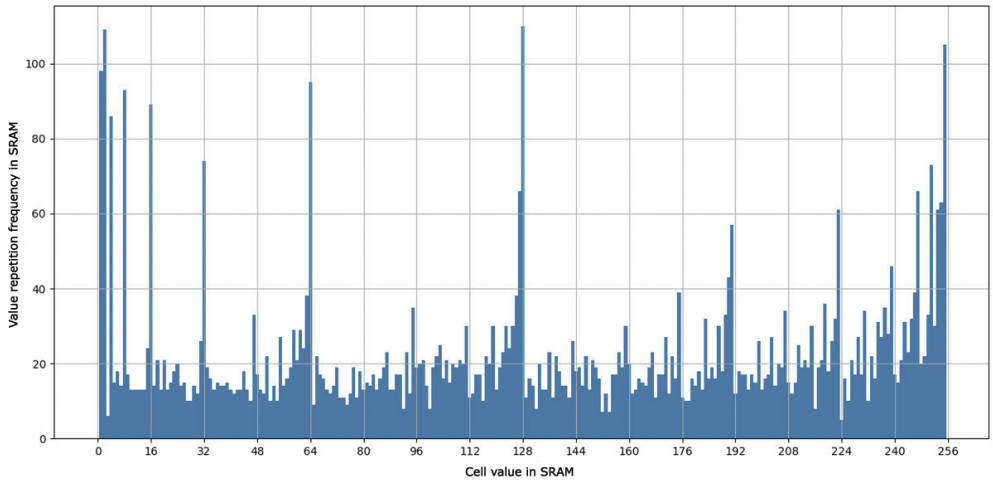


Figure 8b: Values frequency distribution in sample 2 cells after filtration of maximum values.

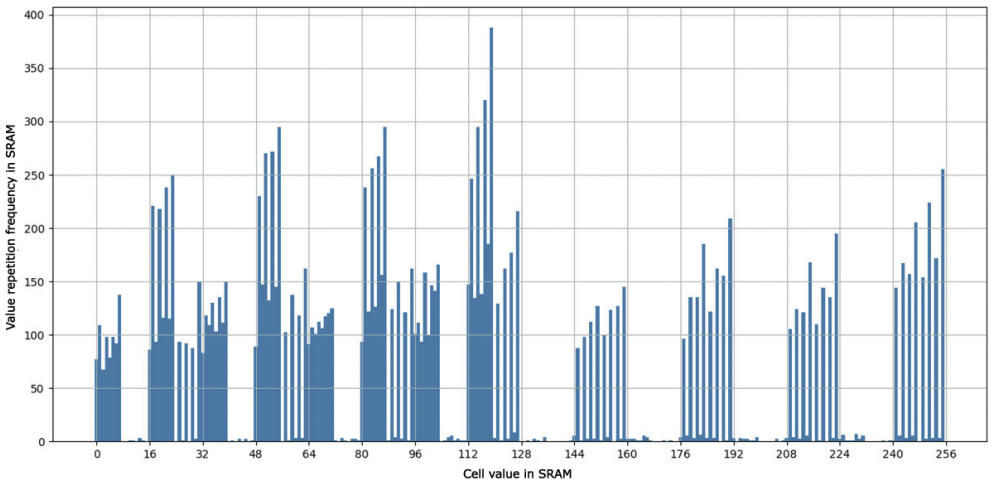


Figure 9: Values frequency distribution in sample 4 cells.

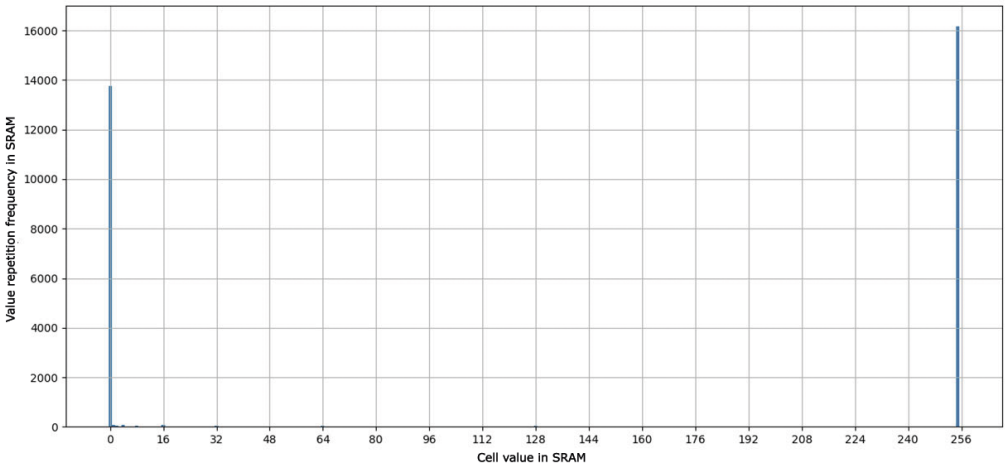


Figure 10a: Values frequency distribution in sample 6 cells.

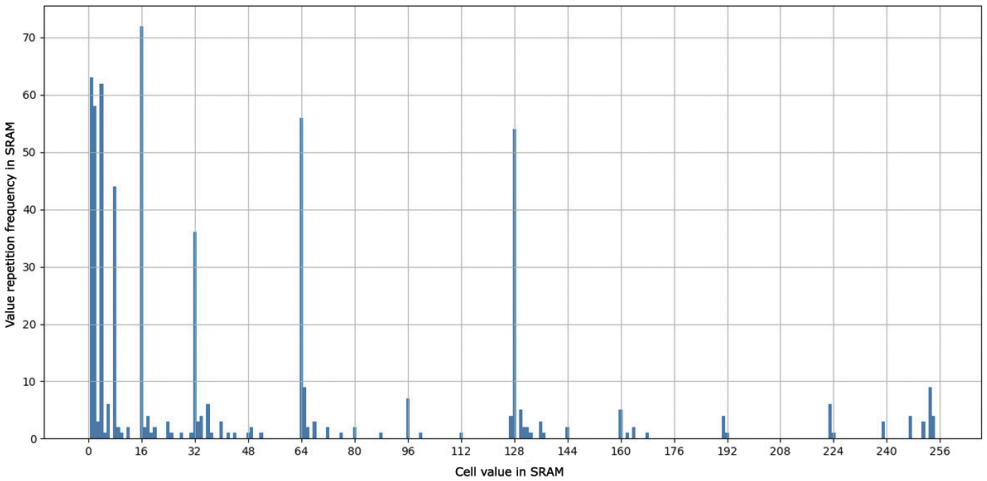


Figure 10b: Values frequency distribution in sample 6 cells after filtration of maximum values.

As can be seen from the above dependencies, for the majority of the samples involved the frequency distribution graph is significantly different from uniform distribution. This means that in most cases stable cells differ from cells containing all zeros or all ones in one or two bits. Filtered from the maximum values, the graphs (Fig. 8b and 10b) show prominent bursts at values that are multiples of $2^n$ (4, 8, 16, 32, 64, 128, 192, 224, 240, 252, 254). Closer to the uniform distribution are the repetition frequency values for sample 4. For the same sample, there was the minimum autocorrelation function value observed. In addition, the Hamming distance was determined for unstable cells in all the samples under investigation. For samples 1,2,4,5, the average distance was 2-3 bits; for sample 3 the distance was 5-8 bits, for samples 6-10 1-2 bits. The indicated distances show the number of bits in the unstable cells, which changed their value through repeated measurements.

## 5 Conclusions

An analysis of the study outcomes indicates the need for further testing of microcircuits or crystals of static RAM when using them as PUFs, since the choice of a short initialization vector in mutual authentication systems implies a high collision value probability for different areas of SRAMs.

As a criterion for possible use of SRAMs as PUFs, the autocorrelation functions can be used for values in memory cells. In this case, the criterion for potential use will be the autocorrelation function minimum value (00.25) in the whole range at the maximum similarity period. Additionally, in view of comprehensive examination, there can be certain interest taken in studying changes in the number of stable and unstable cells in the SARM silicone through the life cycle of the microcircuit.

## References


[Yarm11] Yarmolik V.N., Vashinko Yu.G. Physically uclonable functions // Informatica. 2011. # 2. P. 92103.

[Papp02] R. Pappu Physical One-Way Functions / R. Pappu [et al.] // Science. 2002. Vol. 297. P. 20262030.

[Papp01] R. Pappu, Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu //Massachusetts Institute of Technology (MIT). Cambridge, 2001. 154 p.

[Gass02] Controlled physical random functions / B. Gassend [et al.] // Proc. of 18th Annual ComputerSecurity Applications Conf. (ACSAC), Las Vegas, Nevada, USA, 2002. Las Vegas, 2002. P. 149160.

[Gass03] Gassend, B. Physical Random Functions: MSc Thesis / B. Gassend // Massachusetts Institute of Technology (MIT). Cambridge, 2003. 89 p.

[Eker91] Ekert, A.K. Quantum cryptography based on Bell's theorem / A.K. Ekert // Physical Review Letters. 1991. Vol. 67, # 6. P. 661663.

[Benn92] Bennett, C.H. Quantum cryptography using any two nonorthogonal states / C.H. Bennett //Physical Review Letters. 1992. Vol. 68, # 21. P. 31212124.

[Koca01] Kocarev, L. Chaos-based cryptography: a brief overview / L. Kocarev // Circuits and Systems Magazine. 2001. Vol. 1, # 3. P. 621.

[Shan49] Shannon, C.E. Communication theory of secrecy systems / C.E. Shannon // Bell System Tech. J. 1949. P. 656715.

[Oztu08] Ozturk, E. Physical unclonable function with tristate buffers / E. Ozturk, G. Hammouri, B. Sunar // Proc. of IEEE International Symposium on Circuits and Systems (ISCAS 2008). Seattle, WA, USA, 2008. P. 31943197.

[Holo08] Holocomb, D. Power-up SRAM State as an Identifying Fingerprint and Source of TrueRandom Numbers / D. Holocomb, W. Burleson // IEEE Transactions on Computers. 2008. Vol. 57, # 11. P. 11981210.

[Guaj07] FPGA Intrinsic PUFs and Their Use for IP Protection / J. Guajardo [et al.] // Lecture Notes in Computer Science. 2007. Vol. 4727. P. 6380.

[Maes08] Maes, R. Intrinsic PUFs from Flip-flops on Reconfigurable Devices / R. Maes, P. Tuyls, I. Verbauwhede // Proc. of 3rd Benelux Workshop on Information and System Security (WISSec 2008). Eindhoven, The Netherlands, 2008. P. 320.

[Bohm10] Bohm, C., Hofer, M. An alternative to error correction for SRAM-like PUFs. In Cryptographic Hardware and Embedded Systems (CHES). Berlin, Heidelberg (Germany), 2010, p. 335350.

[Blah86] Blahut R. Theory and Practice of Error Control Codes. M.: Mir, 1986. 576 p.