Unclonable Identification and True Random Number Generation Based on CRO PUF

Alexander Ivaniuk
Faculty of Computer Systems and Networks
Belarusian State University of Informatics
and Radioelectronics
Minsk, Belarus
ivaniuk@bsuir.by

Liana Burko
Faculty of Computer Systems and Networks
Belarusian State University of Informatics
and Radioelectronics
Minsk, Belarus
burkoliana@gmail.com

Abstract. **The problem of generating true random numbers and unique identifiers is more relevant than ever in the modern digital world. This paper analyzes the bits of a binary counter acting as a number's recorder of impulses generated by the physically unclonable functions (PUF) based on a configurable ring oscillator (CRO). The results of the conducted experiments using FPGA chips and an analytical study of the PUF CRO model show the possibility of generating unique stable identifiers and true random numbers at the same time.**

Keywords: **physical unclonable functions, configurable ring oscillator, identification, true random numbers, mathematical model, binary counter**

I. INTRODUCTION

Security is paramount in nowadays interconnected world, innovative solutions are constantly evolving. Robust methods of protection are highly desirable for sensitive data and systems. Physical Unclonable Functions (PUFs) offer a unique approach to security. PUFs based on extracting and measuring unique physical characteristics of semiconductor crystals of digital devices are the basic elements of physical cryptography [1]. Their unpredictable nature makes them incredibly difficult to clone or replicate, cause fake and manipulated PUFs are not able to generate the true IDs. This technology has great potential for improving security in various applications, as it has a simple structure and is capable of solving two problems at the same time. According to various rattling sounds (jitters), caused by various factors, which include instability of the supply voltage, thermal noise of the environment and the semiconductor devices, imperfection of the measuring equipment, etc. PUF-circuits can also, in addition to identification, solve the problem of generating true random numbers.

PUF generates an output bit sequence as response to an input (challenge): R_n = PUF(CH_n), where $n \in [0, 2^L - 1]$. The response of a PUF to a given challenge should show uniqueness, reliability, and unpredictability [2]. The PUF scheme is represented in Fig. 1.

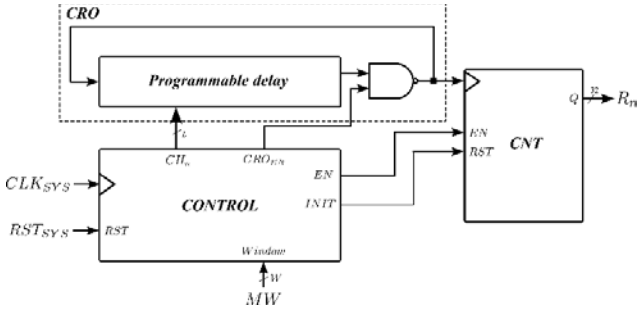


Fig. 1. Scheme of the CRO PUF

This is a reduced circuit scheme of the CRO PUF for the counter, full scheme is in [4]. The general scheme of the CRO can be represented as a programmable delay circuit and a controlled inverter, implemented, as a rule, using a NAND2 gate, which are united by a feedback loop [3, 4]. To build a PUF circuit based on the CRO, it is necessary to have a counter CNT (Measure phase) and a control unit CONTROL, which generates the necessary sequence of signals. In addition, CONTROL generates the response value of the CRO based on the supplied request value CH_n (Select/Switch phase) in the determined measuring window.

II. EXPERIMENT DESCRIPTION

A. Time parameters of ring oscillator

The frequencies of CRO circuits are inherently unpredictable and random. To measure the frequency (or period) of signals generated by the CRO, the sampling frequency must, according to the Kotelnikov theorem, exceed at least twice the frequency of the signal under investigation. Measurements were carried out on FPGA rapid prototyping boards with a system frequency of 50 MHz. Accordingly, CRO frequencies up to 25 MHz can be measured with confidence. If the signal period (the time interval between two rising edges of a periodic digital signal) must be determined, the signal can be applied to the synchronization input of a binary counter implemented on the FPGA. On the selected FPGA family, a 32-bit counter can reliably

operate at up to 180 MHz; therefore, CRO frequencies up to 180 MHz can be measured using such devices.

The width of the measurement window (multiplier k_{factor}) and the bit depth of the registering counter affect the accuracy of measuring the frequency of the CRO signal. With repeated M measurements on the same window MW, different values of the registering counter are observed, caused by various factors, which can include instability of the voltage supply, temperature noise of the environment and the FPGA crystal, imperfection of the measuring equipment, etc.

To increase the resolution of the measurement circuit, let us estimate the period (frequency) of the CRO signal by feeding it to the synchronization input of the binary synchronous counter in the measurement time window $MW = k_{factor} \cdot P_{sys}$, $k_{factor} = 2^i$, $i \in \mathbb{Z}$, which is a factor of the stationary period P_{sys} of the system synchronization signal. Such a measurement method will allow us to estimate the frequencies of $F_{cro} \leq 180$ MHz. The measurement accuracy of P_{cro} depends on the window size: $P_{cro\_i} = MW / R_n^m = 2^i \cdot P_{sys} / R_n^m$, or value $\lambda_i = P_{sys} \cdot P_{cro}^{-1} = R_n^m \cdot 2^{-i}$, where R_n^m is value registered by the counter in m-th measurement with $k_{factor} = 2^i$, $m \in [0, M - 1]$.

The number of clock signals in a certain time window is used as a quantitative measure. When converting the values R_n^m into binary form, the division between the stable (signal) and unstable (noise) parts is visible. The registered values in repeated measurements can be represented by the probabilities of the appearance of a single symbol in each digit of the counter. $P_j^1 = M^{-1} \cdot \sum_{m=0}^{M-1} B_j^m$, $P_j^0 = 1 - P_j^1$, where B_j^m is the value of the j-th digit of the counter in the m-th measurement in a fixed window. The counter length affects the group size, also let us denote $P_j = \max(P_j^0, P_j^1)$.

As can be seen in Fig. 2, the values of all significant digits can be divided into three groups (subsets):

- The group of stable digits G_0, which includes digits for which $P_j = 1$.
- The group of conditionally stable digits G_1, which includes all B_j, for which either $1 > P_j > 0{,}5+\varepsilon$, where ε is a small value characterizing the deviation from the value of 0,5.
- The group of highly unstable digits G_2, for which $P_j < 0{,}5 + \varepsilon$.

Due to the 32-bit counter (see Fig. 1) the values of $i \in [0,30]$ and $M = 1000$ were used in all experiments. The maximum value of $i = 30$ is used because next equation:

$$|G_0| + |G_1| + |G_2| = \lceil \log_2 R_n^m \rceil = \lceil \log_2 (\lambda_i \cdot 2^i) \rceil = \lceil \log_2 \lambda_i \rceil + i = N_i,$$

where $\lceil \log_2 \lambda_{30} \rceil + 30 = 32$.

B. Tests for normal distribution

It was hypothesized that the data from the CRO PUF counter form a normal discrete distribution. To test the hypothesis of normality there are graphical and statistical tests. Visually, there are histograms with an overlaid normal curve and Q–Q [6] plot to see if data quantiles line up with theoretical normal quantiles.

Combining both approaches give a quantitative decision and an intuitive sense of how and where any deviations occur. All data sets under study passed visual tests. The Q-Q test shows deviations at the ends, as already mentioned in the previous study on the assessment of the unstable part. Normality also was tested using the Shapiro–Wilk [6], Anderson–Darling [6], and Pearson tests [6], which compare set's distribution with the ideal normal. In static tests there are already deviations from the normal distribution, but the aim is to show the similarity of the digit-wise probabilities with the ideal model of the normal

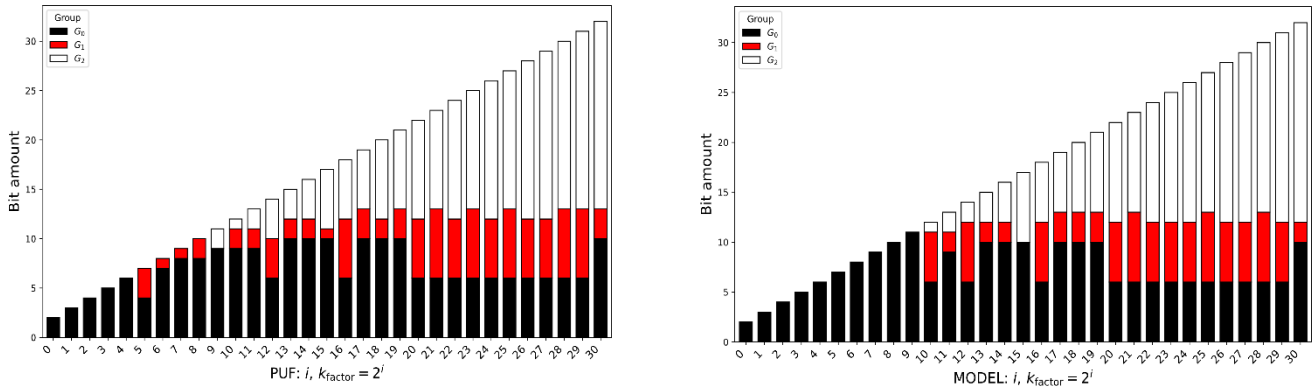
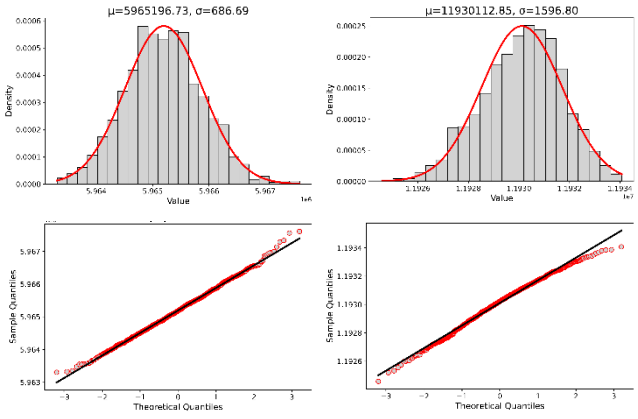


Fig. 2. Devision on groups in PUF and Model data

distribution.

In Fig. 3 there are examples of graphic tests for i = {21,22}.



a b

Fig. 3. Graphical tests for datasets, i=21 (*a*), i=22 (*b*)

III. Program Model of Normal Distribution

Since the data has similarities with a normal distribution, there is need to construct a mathematical model of the ideal normal distribution to predict theoretically the functionality of the selected CRO PUF with known mean and variance. There is need to make sure that the bitwise probabilities of model data P_j^{Model} and of experimental data P_j^{PUF} will be almost the same.

A. Software Model description

To confirm this hypothesis, a software mathematical model of the CRO PUF scheme with a counter was built based on the *numpy* library of the Python language, which generates a discrete set U_{model} of a given size with fixed values of the mean μ_{model} and variance σ^2_{model}.

Model is based on *np.random.normal* function with rounding to the nearest integer.

B. Comparison of PUF and model data

In Fig. 3 comparison with groups of U_{model} and U_{PUF} for different i (k_{factor}) is represented.

First, it is necessary to determine the deviation of model estimates from experimental ones using the Euclidean distance. Let us V_i^{PUF} to be a vector of *PUF* data, V_i^{Model} to be vector with the same size of modeled data. Each component of vector represents the value P_j, then the maximum Euclid distance between V_i^{PUF} and V_i^{Model} can be estimated as $D_{em}^{\max}(i) = \sqrt{\lceil \log_2 \lambda_i \rceil + i} = \sqrt{N_i}$.

Distance of similarity between vectors V_i^{PUF} и V_i^{Model} is estimated through their normalized Euclidean distance $D_{em}^{norm}(i)$. In Fig. 4, it shown that $D_{em}^{norm}(i)$ is close to 0,01:

$$D_{em}^{norm}(i) = \frac{1}{D_{em}^{max}(i)} \cdot \sqrt{\sum_{j=0}^{N_i-1} \left(V_i^{PUF}(j) - V_i^{Model}(j)\right)^2}.$$

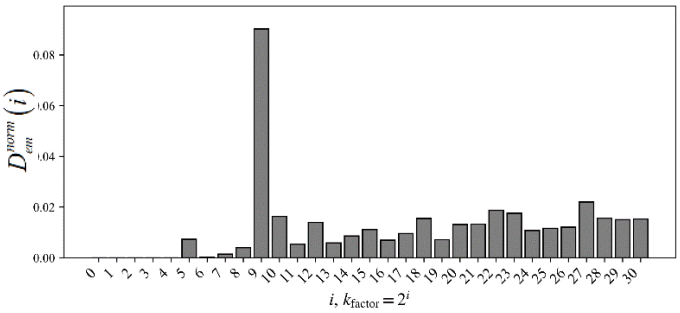


Fig. 4. The plot of $D_{em}^{norm}(i)$

The Fig. 3 shows that the groups sizes are almost the same. This proves that the mathematical model can indeed be used to replicate the work of the CRO PUF.

IV. Experiments with different CRO PUFs on different FPGAs

Experimental results are illustrated with datasets from four similar FPGAs (instances *F*0, *F*1, *F*2, *F*3) with four similar CRO PUFs (instances *C*0, *C*1, *C*2, *C*3). In each FPGA four PUFs were located in different places. In figure 6 there is heatmap of P_j values from 16 combinations.

It was shown that the counter values can indeed be divided into three groups, and the bits of the stable groups G_0 and G_1 can be used as identifiers, cutting off the highly unstable part of G_2. The hypothesis is that all identifiers will be different. For the experiment i = 21 and M = 500 were chosen.

As it is shown in Fig. 5, $|G_0|$, $|G_1|$ are different for all instances, and $|G_2|$, is almost the same.

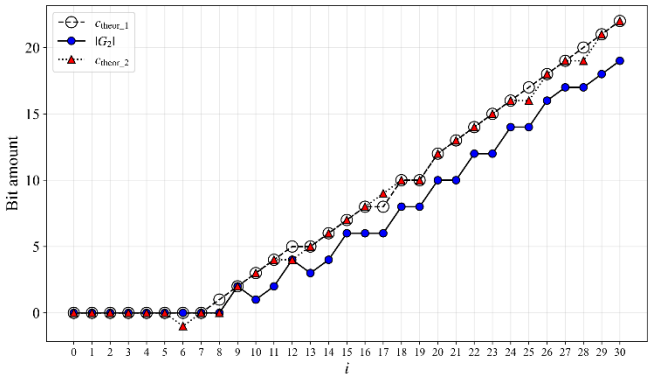


Fig. 5. $|G_2|$ estimation for data with different i

A. *Estimation of highly unstable group G_2*

The length $c = |G_2|$ of highly unstable group G_2 can be estimated with metrics, based on min/max (c^1_{theor}):

$$c^1_{theor} = \lceil \log_2(\max(U) - \min(U)) \rceil,$$

where $U = \{U_{model}, U_{PUF}\}$) values and σ ($c^2_{theor}$ = = $\lceil \log_2(6\sigma) \rceil$).

In theoretical normal distribution 99,7 % values are in range of (-3σ, 3σ), but as *PUF* distribution has deviations at the ends, as it was shown in Fig. 5, the metrics, c^2_{theor} is more accurate, than c^1_{theor}.

Size of group G_2 can be estimated in Fig. 6 with expression $c \le c^2_{theor} \le c^1_{theor}$.

B. *Identification with stable groups G_0, G_1*

Like in many articles [7], the metrics most usually employed to evaluate PUF performance are based on the average Hamming distances (*HD*) evaluated on PUF responses of different PUF instances (HD_{inter}) or different measurements of the same PUF response (HD_{intra}). $ID_{x:y}$ is identifier for each instance F_x:C_y, for the experiment x, $y \in [0,3]$. The Hamming distance between the identifiers of two instances is the number of distinct characters divided by its length.

HD_{intra} is the arithmetic (HD_a) or geometric (HD_g) mean between all pairs $\{y_1, y_2\}$ for fixed x.

HD_{inter} is the arithmetic (HD_a) or geometric (HD_g) mean between all pairs $\{x_1, x_2\}$ for fixed y.

First identifier was built with length $|ID| = \min(|G_0|) = 6$ (Fig. 7) for all observed sets. Results of HD_{intra} and HD_{inter} are in the Tabl. I.

TABLE I. INTRA- AND INTER- UNIQUENESS FOR $|ID| = 6$

HD_{intra}			HD_{inter}		
	HD_a	HD_g		HD_a	HD_g
*F*0	0,250	0,236	*C*0	0,194	0,000
*F*1	0,361	0,340	*C*1	0,389	0,340
*F*2	0,333	0,333	*C*2	0,278	0,252
*F*3	0,333	0,303	*C*3	0,252	0,236

A key advantage of the geometric mean is its immediate identification of identical values, as observed in *C*0. In this case the uniqueness is weak, since there are repeating examples. The length of fully stable group not enough for good uniqueness.

According to the maximum likelihood estimation, the length of unique identifier can be expanded up with values, where $P_j > 0{,}5 + \varepsilon$, $|ID| = \min(|G_0| + |G_1|) = 12$ (Fig. 7).

TABLE II. INTRA- AND INTER- UNIQUENESS FOR $|ID| = 12$

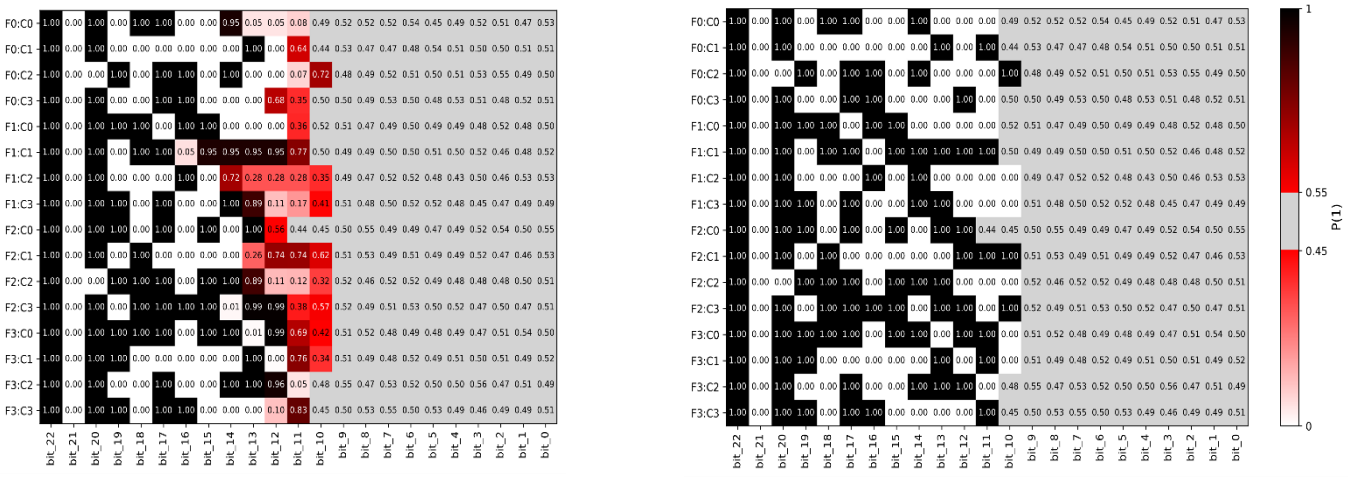
HD_{intra}			HD_{inter}		
	HD_a	HD_g		HD_a	HD_g
*F*0	0,417	0,407	*C*0	0,375	0,360
*F*1	0,431	0,411	*C*1	0,389	0,376
*F*2	0,458	0,446	*C*2	0,319	0,280
*F*3	0,403	0,394	*C*3	0,403	0,394

As can be seen in Fig. 6 red group has gone. Now there are only two groups, stable and highly unstable. It can be seen that the identifiers are different and have good intra- and inter-uniqueness.

Also, the *ID* length can be estimated with metrics c^2_{theor}:

$$|G_0| + |G_1| > N - \lceil \log_2(6\sigma) \rceil.$$

This metrics can help to draw a boundary between unstable and stable group. For example, in experiment $\log_2(6\sigma_{exp}) = \lceil 11{,}9 \rceil = 12$, $N = 23$.



a b

Fig. 6. Distribution of bit probabilities before the maximum likelihood estimation of group (G_2 (a), gray zone is $P_j < 0{,}55$) and after (b)

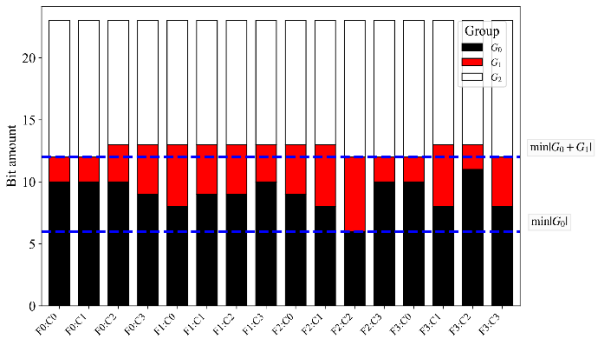


Fig. 7. Group's sizes distribution for experimental data

Without any checking of length groups, only with σ the *ID* length can be chosen. For experimental data the *ID* length is $|ID| = 23 - 12 = 11$.

TABLE III. INTRA- AND INTER- UNIQUENESS FOR $|ID| = 11$

HD_{intra}			HD_{inter}		
	HD_a	HD_g		HD_a	HD_g
*F*0	0,409	0,399	*C*0	0,364	0,339
*F*1	0,424	0,410	*C*1	0,424	0,410
*F*2	0,455	0,445	*C*2	0,303	0,272
*F*3	0,394	0,389	*C*3	0,394	0,381

The scores are slightly lower than those for $|ID| = 12$, but still satisfy the conditions of uniqueness and difference.

CONCLUSUON

CRO PUF is a simple design that exploits the same hardware to generate TRNG response and unique identifier without the need of changing it.

An estimation of a highly unstable group was given, suggesting that so many channels could be used as a source of randomness. To ensure greater randomness, various manipulations can be made with these data. Ways to expand the unique identifier were also provided. It was shown that identifiers from CRO PUF are indeed distinct and unique, and have good intra- and inter-uniqueness.

REFERENCES

[1] Ch. H. Chang, M. Potkonjak (eds.), "Secure System Design and Trustable Computing", Switzerland, Springer, 2016, 549 p. DOI:10.1007/978-3-319-14971-4.

[2] Y. Gao, S. F. Al-Sarawi and D. Abbott, "Physical unclonable functions", Nature Electronics, vol. 3, Feb. 2020, pp. 81-91.

[3] A. A. Ivanyuk, V. N. Yarmolik, "Configurable ring oscillator with controlled interconnections", Security of Information Technologies, vol. 31, no. 2, pp. 121–133. DOI:10.26583/bit.2024.2.08.

[4] A. A. Ivaniuk, "Investigation of the physically unclonable function of a configurable ring oscillator", Informatics, vol. 22(1), 2025, pp. 73-89. (In Russ.). DOI:10.37661/1816-0301-2025-22-1-73-89.

[5] A. A. Ivaniuk, V. N. Yarmolik, "Physically unclonable functions based on a controlled ring oscillator", vol. 30, no. 3, 2023, pp. 90–103 (In Russ.). DOI:10.26583/bit.2023.3.06.

[6] A. Ghasemi, S. Zahediasl, "Normality tests for statistical analysis: a guide for non-statisticians", Int. J. Endocrinol Metab., vol. 10(2), Spring, Apr 20. 2012, pp. 486-9. DOI:10.5812/ijem.3505.

[7] A Unified Multibit PUF and TRNG Based on Ring Oscillators for Secure IoT Devices, IEEE Internet of Things Journal, 2023.