Proceedings of Joint Conference of
11th International Science, Social Sciences, Engineering and Energy Conference (I-SEEC 2022) and,
6th International Conference on Technology and Social Science 2022 (ICTSS 2022)

A Physical Unclonable Function Using Time-to-Digital Converter

Kentaroh Katoh[1, a], Shuhei Yamamoto[1,b], Zheming Zhao[1,c], Yujie Zhao[1,d], Shogo Katayama[1,e], Anna Kuwana[1,f], Keno Sato[2,g], Takashi Ishida[2,h], Toshiyuki Okamoto[2,i], Tamotsu Ichikawa[2,j], Takayuki Nakatani[1,k], Kazumi Hatayama[1,l] and Haruo Kobayashi[1,m *]

[1]Division of Electronics and Informatics, Faculty of Science and Technology, Gunma University, 1-5-1 Tenjin-cho, Kiryu Gunma 376-8515, Japan

[2]ROHM Semiconductor, 2-4-8 Shin-Yokohama, Kouhoku-Ku, Yokohama 222-8575, Japan

[a]kentarohkkkatoh@yahoo.co.jp, [b]t170d123@gunma-u.ac.jp, [c]t201d605@gunma-u.ac.jp, [d]t202d002@gunma-u.ac.jp, [e]t15304906@gunma-u.ac.jp, [f]kuwana.anna@gunma-u.ac.jp, [g]keno.sato@dsn.rohm.co.jp, [h]takashi.ishida@lsi.rohm.co.jp, [i]toshiyuki.okamoto@lsi.rohm.co.jp, [j]tamotsu.ichikawa@lsi.rohm.co.jp, [k]takayuki.nakatani1017@gmail.com, [l]hatayama@oak.gunma-u.ac.jp, [m]koba@gunma-u.ac.jp

Keywords: physical unclonable function, time-to-digital converter, linearity self-calibration, estimation of delay, FPGA

Abstract. This paper presents a physical unclonable function (PUF) using flash time-to-digital converter (TDC). The proposed PUF utilizes that the distribution of delay of delay elements of TDC is unique to the device and unclonable. The proposed PUF is based on the flash TDC with linearity self-calibration using histogram method. With the linearity self-calibration operation, variation of delay of delay elements is estimated. The response output of the PUF is calculated using the estimated variation and the challenge inputs. The proposed PUF is a simple digital circuit consisting of basic digital elements. It is easy to design and implement to both SoC and FPGA. Experiments have been carried out on Arix7 FPGA to assess the performance of the proposed PUF, such as reproducibility and uniqueness. Experimental results show that the intra-chip variation is 8.5 % and inter-chip variation is 42.5 %.

1. Introduction

In semiconductor industry, spread of counterfeit ICs is getting a serious problem. They say the background is globalization of the semiconductor design and fabrication industry, and today's shortage of IC chips by the supply chain broken [1]. Spread of counterfeit ICs causes theft of personal data and software data inside the chips and malicious attack. It gives serious damage to semiconductor companies.

One solution is device authentication based on unique chip ID. Conventionally, the chip ID was stored in non-volatile memory such as EEPROM and flash memory. However, this approach is vulnerable to side-channel attack and the chip ID as well as secret keys for secure communication stored in the memory are easily cloneable. Use of active tamper detection/prevention circuitry is an alternative. But it is costly.

Physical Unclonable Function (PUF) is a promising innovative primitive that is used for authentication and secret key storage to solve the drawbacks of the conventional approaches [2]. Process variation induces variation of gate delay, leakage current, initial state of memory and so on.

These physical parameters are unique to devices and unclonable. PUFs can generate bit strings unique to the device utilizing these parameters. These bit strings are reproducible and have correlation with the unique physical parameters induced by variation of devices. They are called fingerprints of chips. PUF is strong to tamper attack, unclonable, and cheap. There are various physical parameters available to construct PUFs. Various PUFs have been proposed in academia utilizing these parameters. SRAM-based PUFs and Butterfly PUF utilize variation of initial state of SRAM [3,4]. Current array PUF uses stochastic variability in operating in subthreshold region [5]. Arbiter PUF and ring oscillator PUF utilize variation of gate delay [6,7].

Time-to-Digital Converter (TDC) is on-chip delay measurement circuit. Time resolution of several picoseconds can be achieved when the TDC is implemented with an advanced CMOS process [8]. Therefore, it has various applications including phase comparators of all-digital PLLs, sensor interface circuits, modulation and demodulation circuits. Because TDC consists mostly of digital circuitry, it is easily implemented on SoC and FPGA [9]. However, the non-linearity of TDC increases as it is fabricated with fine CMOS process. In this case, the nonlinearity should be compensated with linearity calibration [10].

The nonlinearity occurs due to process variation. It is unique to implemented device and unclonable. Therefore, the nonlinearity of TDC can be used for PUF.

This paper presents a PUF using flash TDC (TDC PUF). The proposed PUF utilizes that the distribution of delay of delay elements of TDC is unique to the device and unclonable. The proposed PUF is based on the flash TDC with linearity self-calibration using histogram method. With the linearity self-calibration operation, variation of delay of delay elements is estimated. The response output of the PUF is calculated using the estimated variation and the challenge inputs. Because the delay variation is unique to the device and unclonable, the output response is unique and unclonable, too. The proposed PUF is a simple digital circuit consisting of basic digital elements. It is easy to design and implement to both SoC and FPGA. Furthermore, because the challenge input space is larger than other PUFs utilizing delay variation, the proposed PUF can realize better device authentication. As long as we know, this is the first proposal of PUF using TDC with linearity self-calibration.

The rest of the paper is organized as follows. Section 2 explains the proposed TDC PUF. Section 3 shows the experimental results. Finally, section 4 concludes the paper.

2. Proposed TDC PUF

This section explains the proposed TDC PUF. First, 2.1 reviews the basic functions of PUF. The proposed PUF is based on the flash TDC with linearity self-calibration using histogram method. 2.2 and 2.3 give the explanation of the flash TDC and the linearity calibration using histogram method, respectively. Finally, 2.4 describes the proposed TDC PUF.

2.1 Basics of PUF

PUF can generate unique bits to the device which is used for device authentication and secure communication without requirement of secure EEPROMs and other expensive hardware. As mentioned above, there are various implementations of PUF. However, the function is same.

Fig. 1 gives the system-level description of PUF. As shown in this figure, PUF is a challenge-response system. It has challenge input *c* and its response output *r*. The relation between *r* and *c* is described as $r = f(c)$. Unlike usual function, the function f has hidden parameters representing internal manufacturing variability such as variation of delay or leakage current as well as the explicit input *c*. With the implicit and explicit parameters, it generates a unique response output *r*. Gathering the multiple challenge-response pairs, we can construct a bit string. As the response output *r* of the challenge input *c* is unique, the constructed bit string is unique, too.

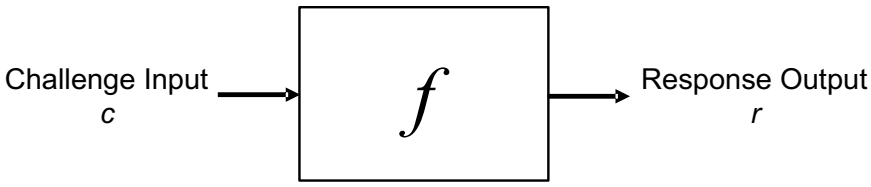


Fig. 1. System level description of a PUF.

2.2 Flash TDC

Flash TDC measures the time interval between two edges [10]. Fig. 2 shows the configuration of a flash TDC: the reference CLK passes through a buffer delay line, which consists of a chain of inverters, and the delayed reference CLK signals are used as the data input for some flip-flop (DFF) circuits. The measured signal is used as the clock signal of the flip-flops. We obtain the outputs of the flip-flops as a thermometer code, according to the rise-edge-timing interval between the reference START edge and STOP edge, and the encoder transforms the results into a binary code. The time resolution is determined by gate delay τ.

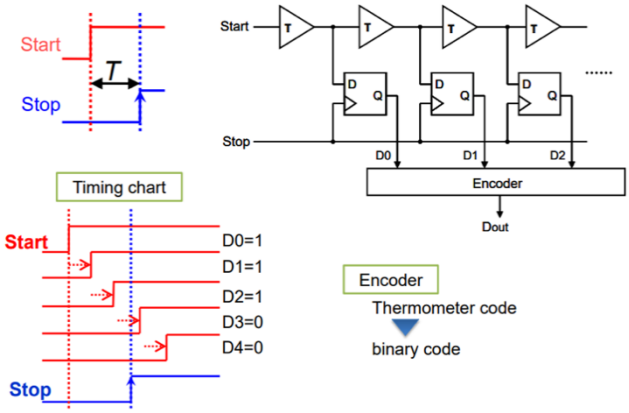


Fig. 2. A flash TDC architecture and its operation.

2.3 Linearity Calibration of Flash TDC Using Histogram Method

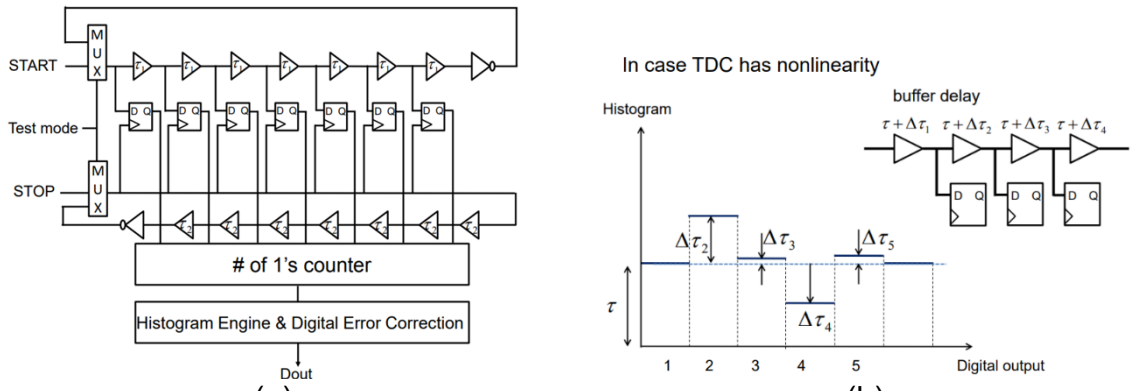
The flash TDC may show nonlinearity characteristics due to delay-time mismatch among delay buffers.

Fig. 3 (a) shows the basic TDC with linearity self-calibration using two ring oscillators to compensate nonlinearity [11]. During linearity calibration, the two MUXs choose feed-back lines to construct ring oscillators to generate a random delay sequence. TDC measures each random delay one by one and the histogram engine constructs a histogram that counts the measured results.

If the delay sequence is sufficiently random and the number of sampled delays is sufficiently large, the histogram reflects the characteristics of the nonlinearity among buffers (Fig. 3 (b)).

The distribution of the histogram constructed in the histogram engine follows the distribution of the delay of buffers. For example, when the buffers have uniform delay, the distribution of the bins of the constructed histogram is also uniform.

With the obtained histogram, TDC can compensate for linear operation in normal operation.



(a) (b)

Fig. 3. Flash TDC with linearity self-calibration (a) and its estimation of variation of buffer delays (b).

2.4 TDC PUF

The proposed TDC PUF utilizes the variation of the delay of the buffers of the flash TDC. The response output of the challenge input is unique affected by the variation of the delay of the buffers.

Fig. 4 depicts the 8-stage TDC PUF. This is made by modifying the flash TDC with linearity self-calibration function explained in the previous subsection. The buffers are replaced with the 2-to-1 multiplexers. The output of a multiplexer of a stage is fan-out to the 2 inputs of the 2-to-1 multiplexer of the next stage. The ideal delay of the fan-out paths should be same. The 1-bit control input of the ith stage 2-to-1 multiplexer is CI[i] ($0 \leq i \leq 7$). The outputs of the flip flops of TDC are connected to the 8-to-1 multiplexer. The output of the multiplexer is connected to a counter. It has 3-bit control inputs, CI[10], CI[9], and CI[8]. They connect the output of the selected flip flop to the counter. When the measurement result of the TDC is equal to the 3-bit control inputs value, the counter is incremented.

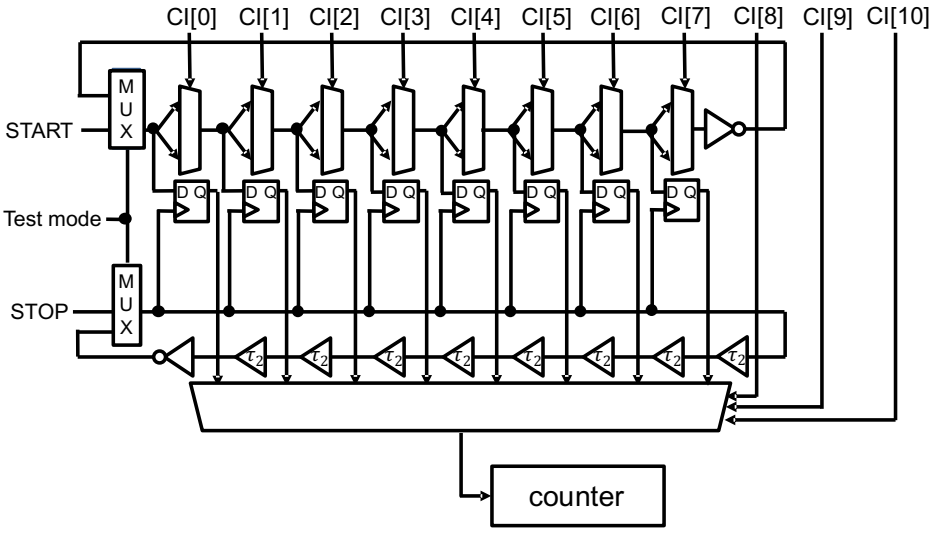


Fig. 4. 8-stage TDC PUF.

We explain how to calculate the response output R of a challenge input C. The challenge input is applied to CI of the PUF. In this example, CI is 11 bits. Then C is 22 bits. First, the former 11 bits are applied to CI. After that, the 1st calibration is performed. After the calibration, the bin length of the histogram of measurement result assigned by the control inputs, CI[10], CI[9], and CI[8] are stored to the counter. The bin length depends on CI and the variation of delay of the multiplexers. Second, the

latter 11 bits are applied to CI. After that, the 2nd calibration is performed. After the calibration, the bin length of the histogram of measurement result assigned by the control inputs, CI[10], CI[9], and CI[8] are stored to the counter. When the former counter value is larger than the latter counter value, R is 0, otherwise 1.

The distribution of histogram obtained by the calibration follows the distribution of the delay of the multiplexers. Because the distribution of delay of the multiplexer is unique to the device, the counter value is unique to the device, too. Accordingly, the response output R decided by the difference of the counter values is also unique to the device.

However, the bin length of the maximum measurement result (in this case, CI[10]CI[9]CI[8]=111) depends on not only the delay of multiplexer but also the delay of inverter, feed-back wire, and multiplexer MUX which decides the mode of the PUF. It is not used to decide the response output.

In general, the challenge input C consists of the former sub-input C_0 and the latter sub-input C_1. When the number of stages of the TDC PUF is 2^n, where n is an integer, the width of the sub-inputs is 2^n+n bits, and thus, the width of C is $2(2^n+n)$ bits. When variation of delay among stages is not negligible, the coefficients COEF[i] for bin of ith stage ($0 \leq i \leq 2^n - 2$)) is introduced to compensate the variation. Let $COUNT_0$ and $COUNT_1$ be the counter values after the 1st and the 2nd calibration, respectively. Let $COEF_0$ and $COEF_1$ be the coefficients for $COUNT_0$ and $COUNT_0$, respectively. Then the calculation of R is described as following steps.

Step1. Apply C_0 and perform the 1st calibration, then $COUNT_0$ is obtained.

Step2. Apply C_1 and perform the 2nd calibration, then $COUNT_1$ is obtained.

Step3. When $COEF_0 \times COUNT_0 > COEF_1 \times COUNT_1$, R = 0, otherwise R=1.

3. Experimental Results

This section evaluates the proposed TDC PUF implemented with FPGA. A PUF is required reproducibility and uniqueness as its basic functions [7]. A PUF is needed to generate same bit string even under different environment or external noises. It is reproducibility. Because a PUF is used for identification of devices, the bit string generated by a PUF must be unique to the device. It is uniqueness. Reproducibility is important to guarantee the reliability, uniqueness is important to realize security.

Intra-chip variation is a quantitative metric of reproducibility. It is defined as the number of bits in bit strings generated by a PUF that vary when a set of identical challenge inputs is repeatedly queried [2]. The intra-chip variation v_{intra} is calculated by the following formula.

$$v_{intra} = \frac{1}{N_q}\frac{1}{N_{PUF}}\sum_{i=1}^{N_{PUF}}\sum_{j=1}^{N_q}\frac{HD(B_i,B_{i,j})}{N_B} \times 100 \ \ (\%), \tag{1}$$

where N_q is the number of query to a PUF, N_{PUF} is the number of PUFs, B_i is the unique bit string of the ith PUF, $B_{i,j}$ is the bit string generated by the jth query of the ith PUF, N_B is the length of the generated bit strings, and $HD(B_i, B_{i,j})$ is the hamming distance between B_i and $B_{i,j}$.

Inter-chip variation is a quantitative metric of uniqueness. It is defined as the number of different bits in bit strings generated by different PUFs with a shared set of identical challenge inputs [2]. Inter-chip variation v_{inter} is calculated by the following formula.

$$v_{inter} = \frac{2}{N_{PUF}\cdot(N_{PUF}-1)}\sum_{i=1}^{N_{PUF}-1}\sum_{j=i+1}^{N_{PUF}}\left(\frac{HD(B_i,B_j)}{N_B}\right) \times 100 \ \ (\%). \tag{2}$$

For the application of secure authentication, intra-chip variation should be low (ideally 0%). On the other hand, inter-chip variation should be high (ideally 50% on average) [2].

Here, we evaluate the intra-chip variation and inter-chip variation of the proposed PUF. We implement the 15 proposed TDC PUFs and a MicroBlaze, a soft processor core of Xilinx, on a Xilinx Arix7 FPGA board [12]. The TDC PUF has 11-bit input. The number of stages of the internal TDC is 8. The length of the counter to count the bin length is 16 bits. The number of sampling in a

calibration operation is 2^{17}. A set of common 128 challenge inputs are constructed from the 11-bit pseudo-random patterns. The 11-bit pseudo-random patterns are generated with emulation of 11-bit linear feed-back shift register on MicroBlaze. The challenge inputs are sent to arbitrary TDC PUF and receive the output 128-bit bit string. The intra-chip variation and inter-chip variation are calculated with Eq. (1) and Eq. (2). The number of queries to a PUF N_q is 128. According to the results, the intra-chip variation is 8.5 %. It is less than 10%. It meets the need for strong PUF, which is mainly used for device authentication [13]. The inter-chip variation is 42.5 %. It is 7.5 % less than the ideal value 50 %. Fig. 5 shows the probability distribution of $HD(B_i, B_{i,j})$ of intra-chip variation of Eq. (1) and $HD(B_i, B_j)$ of inter-chip variation of Eq. (2). The vertical axis is the occurrence probability. The color bars are the raw data. The dotted lines are Gaussian distributions with parameters fitted to the raw data. With the fitted Gaussian distributions, we calculate misclassification rate. The misclassification rate is the probability that a PUF is mistook as another PUF or another PUF is mistook as the PUF. It is 0.80 %.

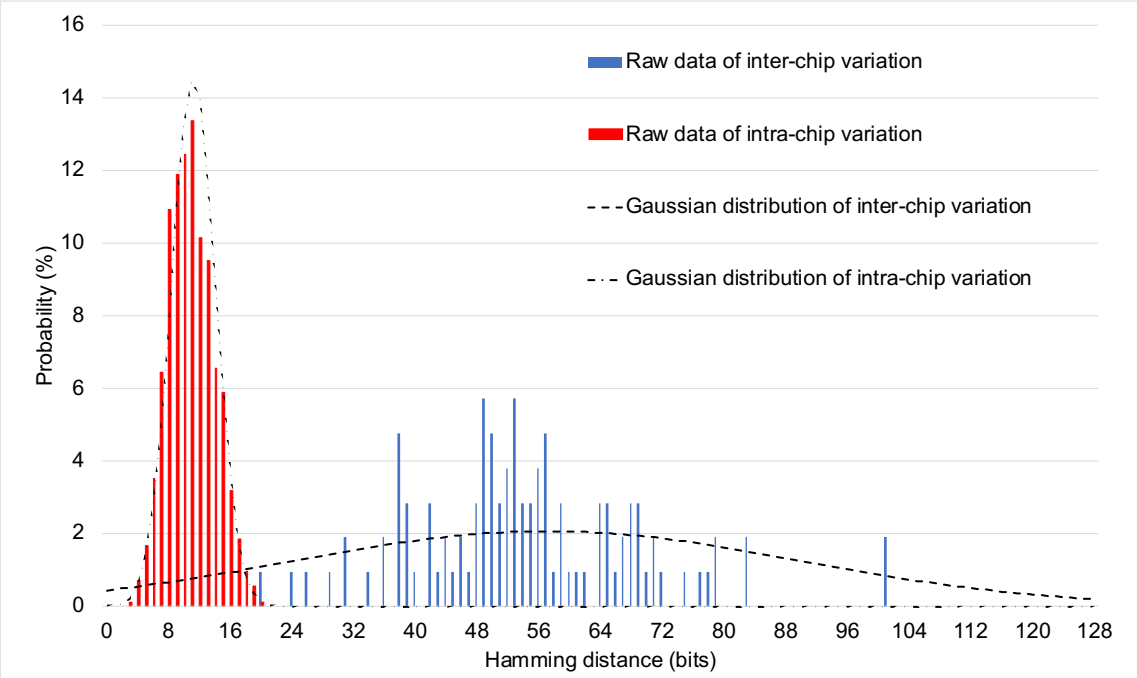


Fig. 5. Probability distribution of hamming distance.

4. Conclusion

This paper has presented a PUF using flash TDC. The proposed PUF utilizes that the distribution of delay of delay elements of TDC is unique to the device and unclonable. The proposed PUF is based on the flash TDC with linearity self-calibration using histogram method. With the linearity self-calibration operation, variation of delay of delay elements is estimated. The response output of the PUF is calculated using the estimated variation and the challenge inputs. The proposed PUF is a simple digital circuit consisting of basic digital elements. It is easy to design and implement to both SoC and FPGA. Experiments have been carried out on Arix7 FPGA to assess the performance of the proposed PUF, such as reproducibility and uniqueness. Experimental results show that the intra-chip variation is 8.5 % and inter-chip variation is 42.5 %.

References

[1] M.T. Rahman, D. Forte, Q. Shi, G.K. Contreras, and M. Tehranipoor, "CSST: preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly", ***Proceedings of DFT2014*** (Amsterdam, Netherlands) Oct. 2014.

[2] C. Herder, M.-D. Yu, F. Koushanfar and S. Devadas, "Physical unclonable functions and applications: a tutorial", ***Proceedings of the IEEE***, Vol.102, No.8, pp.1126-1141, 2014.

[3] S. Taneja, V.K. Rajanna and M. Alioto, "In-memory unified TRNG and multi-bit PUF for ubiquitous hardware security", ***IEEE Journal of Solid-State Circuits***, Vol.57, No.1, pp. 153 - 166, 2022.

[4] S.S. Kumar, J. Guajardo, R. Maes, G.J. Schrijen and P. Tuyls, "The butterfly PUF: protecting IP on every FPGA", ***Extended Abstract of HOST2008*** (Anaheim, CA, USA) Jun. 2008.

[5] X. Xi, H. Zhuang, N. Sun and M. Orshansky, "Strong subthreshold current array PUF with 2^{65} challenge-response pairs resilient to machine learning attacks in 130nm CMOS", ***Proceedings of Symposium on VLSI Circuits 2017*** (Kyoto, Japan) Aug. 2017.

[6] J.W. Lee, D. Lim, B. Gassend, G.E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication application", ***Digest of Symposium on VLSI Circuits 2004*** (Honolulu, HI, USA) Jun. 2004.

[7] E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation", ***Proceedings of DAC2007*** (San Diego, CA, USA) Jun. 2007.

[8] Y. Tu, R. Xu, D. Ye, L. Lyu and C.-J. Richard Shi, "A 400 MHz, 8-bit, 1.75-ps resolution pipelined-two-step time-to-digital converter with dynamic time amplification", ***Proceedings of ISCAS2020*** (Virtual) Oct. 2020.

[9] N. Lusardi, F. Garzetti, N. Corna, S. Salgaro, N. Bachetti and A. Geraci, " Plug-and-play tunable and high-performance time-to-digital converter as IP-core for Xilinx FPGAs", ***Proceedings of NSS/MIC2020*** (Boston, MA, USA) Nov. 2020.

[10] S. Yamamoto, Y. Sasaki, Y. Zhao, A. Kuwana, K. Katoh, Z. Zhang, J. Wei, T.M. Tran, S. Katayama, K. Sato, T. Ishida, T. Okamoto, T. Ichikawa, T. Nakatani, K. Hatayama and H. Kobayashi, "Metallic ratio equivalent-time sampling and application to TDC linearity calibration", ***IEEE Transactions on Device and Materials Reliability***, Vol.22, No.2, pp.142-153, 2022.

[11] S. Ito, S. Nishimura, H. Kobayashi, S. Uemori, Y. Tan, N. Takai, T. J. Yamaguchi and K. Niitsu, "Stochastic TDC architecture with self-calibration", ***Proceedings of APCCAS2010*** (Kuala Lumpur, Malaysia) Dec. 2010.

[12] MicroBlaze Soft Processor Core (website), https://www.xilinx.com/products/design-tools/microblaze.html

[13] S. Taneja, "Energy-efficient and low-cost hardware security primitives for secure ubiquitous computing", ***Proceedings of MWSCAS2022*** (Fukuoka, Japan) Aug. 2022.