Physically Unclonable Function Using RTN-Induced Delay Fluctuation in Ring Oscillators

Motoki Yoshinaga, Hiromitsu Awano, Masayuki Hiromoto, and Takashi Sato
Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan
E-mail: paper@easter.kuee.kyoto-u.ac.jp

***Abstract*—This paper proposes *RTN-PUF*, a novel PUF that utilizes random telegraph noise (RTN) of transistors as the physical uniqueness of individual devices. Our proposed RTN-PUF generates a response from a pair of ring oscillators (ROs) by comparing the numbers of frequency changes, which depend on the time constants of RTN. Due to the log-uniform distribution of the time constants, our RTN-PUF provides more stable responses than the existing manufacturing-variation-based PUFs. The numerical experiments show that the RTN-PUF reduces false negative errors by about 60 times compared to the conventional RO-based PUF. This facilitates to implement PUF into security purposes.**

I. Introduction

Physically unclonable function (PUF) [1], often referred to as "chip's fingerprint", is attracting increasing attention in the field of security. A PUF receives challenges (inputs) and generates corresponding responses (outputs). The response generation utilizes physical device-characteristics determined during fabrication process. Thus, challenge-response pair (CRP) of a PUF is unique to each chip, making the chip resistant to counterfeiting.

In constructing a PUF, it is important to use the physical characteristics that have a high degree of variation. Considering the functionality of the PUFs as a fingerprint of a chip, the PUFs must return the same response whenever the same challenge is given. In general, the more greatly the physical characteristics vary, the more distinct the devices become, which facilitates accurate chip identification.

Utilizing the time constant of random telegraph noise (RTN) is a good option to design a PUF that generates stable responses. RTN, which is the temporal fluctuation in the threshold voltage ($V_{\rm th}$), is one of the most promising device characteristics. The origin of RTN is considered to be electrically active traps located inside the gate oxide films. These traps capture or emit carriers, and the can be observed as $V_{\rm th}$ fluctuation. The time constant of RTN, which is average interval of $V_{\rm th}$ change, is one of the representative device-intrinsic parameters and reported to spread uniformly in logarithmic time-scale [2] over many orders of magnitude. By utilizing this property, the PUF can be made more distinct than by using the conventional randomness source that follows a Gaussian distribution such as initial $V_{\rm th}$ variation.

A PUF circuit that utilizes RTN has been first proposed in [3]. However, the proposed PUF cannot fully utilize the property of RTN. This PUF uses a paired transistors which are first subjected to a short term stress, i.e., a high voltage is applied to the gate terminal to fill existing traps. Then, the gate voltages are lowered and the drain currents are compared using a sense amplifier to generate a 1-bit response. The PUF realized excellent resistance to deterioration over time utilizing the property that time constants of RTN is stable under electrical stressing. However, in [3], the response may be mostly determined by the initial $V_{\rm th}$ variation, which is still far larger than the RTN-induced $V_{\rm th}$ fluctuation in the current manufacturing process. Hence, a circuit structure whose responses rely only on the RTN-induced $V_{\rm th}$ fluctuations has to be developed. Moreover, no quantitative comparison was made with existing PUF structures.

In this paper, we propose a new PUF structure based on the ring-oscillator-based PUF (RO PUF), in which the RTN-induced temporal frequency fluctuation is utilized. The numerical experiment shows that the proposed PUF structure achieves 60 times smaller intra-chip variation than the existing RO PUF [4].

II. Preliminaries

A. Performance Metrics of a PUF

There are two important properties that PUFs must satisfy to identify chips: uniqueness and robustness. First, different PUFs should return different responses to the same challenge. We define this property as "uniqueness." Secondly, each PUF should always return the same response to the same challenge. We define this property as "robustness."

The uniqueness of PUFs can be improved by an elaborated response generation method regardless of the distribution that the device characteristics follow. For example, when two random numbers generated by the same random source are compared, the probability that one is larger than the other should be 0.5. By applying this method to response generation, each PUF can independently generate random responses and thus guarantee its uniqueness if sufficient number of bits are available.

The robustness is strongly associated with how widely the characteristics vary. Considering the robustness, the use of manufacturing variation may not be a good option to construct a PUF. Most parameters suffering from manufacturing variation follow a Gaussian distribution [5]. At around the center of the bell-like curve, devices tend to have similar characteristics. This makes it difficult to distinguish between those devices because a slight measurement error can make the difference between the devices invisible. To realize a robust PUF structure, the device characteristics should be sufficiently distinct both within a PUF and between the PUFs. Hence, we focus on the variation of the RTN time constant in this paper.

B. Ring Oscillator PUF

Most of the existing PUFs, such as RO PUF [4], are based on *static* manufacturing variation of transistors [1], [6]. Fig. 1 shows the structure of an RO PUF. The PUF contains many ROs, and any two ROs (a, b), can be selected according to a challenge. The frequencies of the selected ROs ($f_{{\rm RO}_a}$ $f_{{\rm RO}_b}$) are compared to yield a single bit response, $f(a, b)$. Because the frequency of an RO depends on the $V_{\rm th}$ of the transistors, the results of the frequency comparisons are determined right at the time of chip fabrication. Thus, the CRP of the PUF is chip-intrinsic and unduplicatable.

According to [4], RO PUF is reported to achieve sufficiently good uniqueness, which is owed to the response

978-1-4799-5341-7/16/$31.00 ©2016 IEEE

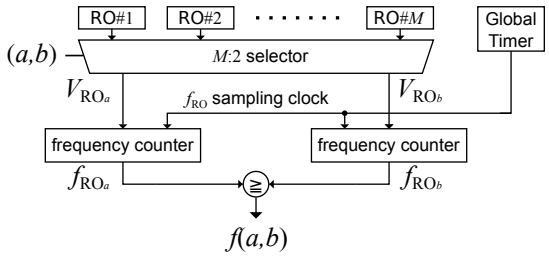
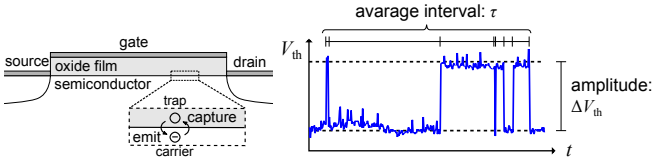


Fig. 1. RO PUF generates a single bit response by comparing frequencies of two ROs.



(a) Physical RTN model. (b) An example of measured $V_{\rm th}$ fluctuation.

Fig. 2. RTN is caused by carriers' probabilistic behaviors.

generation procedure. In RO PUF, the responses are generated by comparing the characteristics of two devices. The comparison result will be random no matter what distribution the characteristics follow, contributing the good uniqueness performance of RO PUFs. On the other hand, the robustness of the RO PUF is not as good as its uniqueness. The oscillation frequencies of a pair of ROs can be too close to obtain stable comparison results because they are determined by the sum of gate delays which follows a Gaussian distribution.

C. RTN and Time Constant Variation

RTN is associated with a probabilistic behavior of the carriers at the Si-SiO_2 interface. Fig. 2(a) shows a physical RTN model. Carriers are captured at the Si-SiO_2 interface, which contributes to the $V_{\rm th}$ increase. When the captured carrier is emitted from the trap, $V_{\rm th}$ returns to its original value. Fig. 2(b) shows a measured $V_{\rm th}$ fluctuation containing a trap that causes large $V_{\rm th}$ change. The carrier trap and emission occurs probabilistically, producing two major $V_{\rm th}$ levels (states). Although the accurate timing of state transitions is unpredictable, the carrier behavior can be modeled by using a time constant τ, the average interval of the state transitions.

The proposed PUF utilizes the extremely wide distribution of τ to improve robustness. RTN parameters including τ and the amplitude of $V_{\rm th}$ shift ($\Delta V_{\rm th}$) depend on the location of traps in the gate oxide films. Hence, these parameters are transistor-intrinsic and thus suitable for the device characteristics used in a PUF. The time constants are log-uniformly distributed at least in the range of 10^{-7}–10^{1} s [2].

III. RTN-Based PUF

The proposed PUF (RTN-PUF) utilizes the RTN-induced fluctuations in oscillation frequency of ROs. Specifically, time constants extracted from two ROs are compared to generate a response signal. Because the direct observation of the $V_{\rm th}$ requires a large amount of hardware resources, we propose to indirectly measure the change of $V_{\rm th}$ as the frequency fluctuations of ROs. Fig. 3 illustrates an example timing chart showing the detection of frequency fluctuations. RTN-induced $V_{\rm th}$ fluctuation in a transistor forming the RO causes the temporal changes of the oscillation frequency. The oscillation frequency is repeatedly sampled with a $f_{\rm RO}$ sampling clock. When the change of the oscillation frequency is larger than the pre-defined threshold value $\Delta f_{\rm ref}$, a detection signal is asserted. The number of detection bit assertions is counted to generate responses.

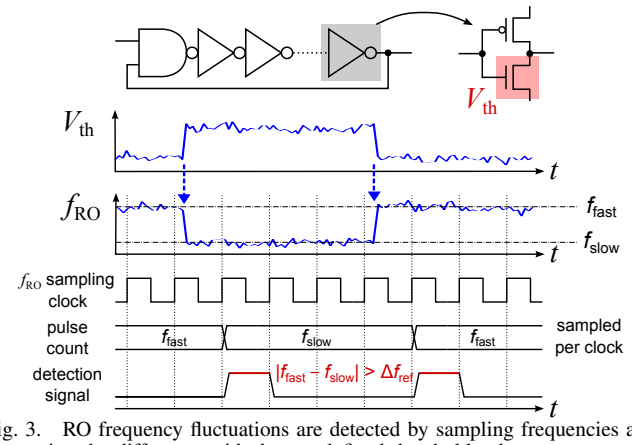


Fig. 3. RO frequency fluctuations are detected by sampling frequencies and comparing the difference with the pre-defined threshold value.

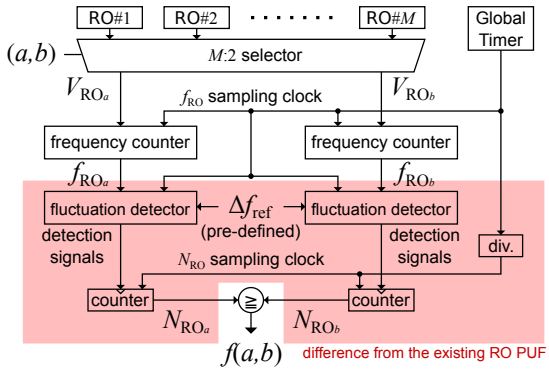
The use of frequency fluctuation instead of the initial frequency variation improves the PUF's robustness without deteriorating its uniqueness. Since RTN-PUFs generate responses by comparing two devices in the similar way as RO PUFs, RTN-PUF is expected to realize as good uniqueness as the existing RO PUF. In terms of the robustness, RTN-PUF compares the number of frequency fluctuations per unit time between two ROs to generate a single bit response whereas the existing RO PUF directly compares the frequency. This means that RTN-PUF utilizes the time constant τ, which has much greater variation than that of the manufacturing variation. Hence, RTN-PUFs can realize greater robustness than RO PUFs.

Note again that at the current manufacturing process, the initial $V_{\rm th}$ variation is larger than the RTN-induced $V_{\rm th}$ fluctuation and hence the oscillation frequency is mostly determined by the initial $V_{\rm th}$ variation. In the proposed RTN-PUF, the static effect of initial $V_{\rm th}$ variation is canceled by utilizing the temporal differentiation of the oscillation frequency.

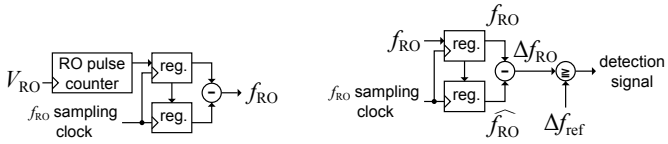
A. Challenges and Response Generation Procedure

In general, the relationship between a challenge $\boldsymbol{c}_i$ and the response r_i can be represented as $r_i = f(\boldsymbol{c}_i)$, where $f(\cdot)$ is a function that maps a challenge to a response. In most cases, the function $f(\cdot)$ utilizes randomness of the device parameter to obtain a unique response. In RTN-PUF, the challenge $\boldsymbol{c}_i$ is composed of a pair of bit sequences $\boldsymbol{a}_i$ and $\boldsymbol{b}_i$ that are used for selecting a pair of ROs. Temporal frequency fluctuation counts are compared, and a single-bit response r_i is output. Typically, a sequence of challenges $\boldsymbol{C} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \cdots, \boldsymbol{c}_L)$ is used to obtain a multi-bit response $\boldsymbol{R} = (r_1, r_2, \cdots, r_L)$ to enhance the uniqueness of the response.

Fig. 4 shows the block diagram of RTN-PUF. It generates a response to a challenge (a, b) in four steps: RO selection, frequency measurement, fluctuation detection, and count comparison. First of all, two of the M ROs are selected and activated by the challenge signal. Let the outputs of the selected ROs be $V_{\rm RO_a}$ and $V_{\rm RO_b}$. Next, the frequencies ($f_{\rm RO_a}$ and $f_{\rm RO_b}$) are measured by counting RO pulses in $f_{\rm RO}$ clock period. This clock counting is repeated for a number of times. Each count in the repetitive counting is compared with that in the previous counting period ($\widehat{f_{\rm RO_a}}$ and $\widehat{f_{\rm RO_b}}$) to find the difference between successive two countings. If the difference is larger than the pre-defined threshold, $\Delta f_{\rm ref}$, the fluctuation-detection logic asserts the detection signal. The numbers of fluctuations over the pre-defined duration are counted for two ROs and stored in the respective registers, $N_{\rm RO_a}$ and $N_{\rm RO_b}$. Finally, $N_{\rm RO_a}$ and $N_{\rm RO_b}$ are compared to generate a response



(a) Entire structure of the proposed PUF.



(b) Frequency counter. (c) Fluctuation detector.

Fig. 4. Block diagram of the proposed RTN-PUF.

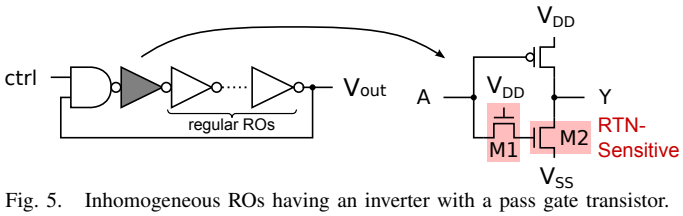


Fig. 5. Inhomogeneous ROs having an inverter with a pass gate transistor.

bit, $f(a,b)$. This procedure will be repeated for L times for a challenge input of length L.

B. Design Consideration

In RTN-PUF, we adopt the topology of inhomogeneous RO [7] to amplify the sensitivity to RTN. Detection of the frequency fluctuation in a regular RO is not an easy task, because the frequency fluctuation due to RTN is too small to observe reliably. The inhomogeneous ring oscillator is utilized as well as the proposed circuit structure in Fig. 4, which facilitates to detect frequency fluctuations using purely digital circuits and in a small area.

The topology of an inhomogeneous RO in Fig. 5 amplifies the sensitivity to RTN by making $V_{\rm th}$ of particular transistors significantly affect the frequency of the RO. One of the inverters composing the RO is replaced with the one having a pass gate transistor in series. The two transistors, M1 and M2, have higher sensitivity to RTN than the others.

IV. Numerical Experiment and Evaluation

A. Evaluation Criteria

In order to evaluate the performance of the proposed RTN-PUF, we adopt two quantitative criteria introduced in [4], where inter-chip variation ($p_{\rm inter}$) and intra-chip variation ($p_{\rm intra}$) correspond to uniqueness and robustness respectively. Firstly, $p_{\rm inter}$ is the probability that the response bits from two PUF instances differ from each other when the same challenge is given to the both instances. In the ideal case when the responses of each instance are truly random, $p_{\rm inter}$ becomes 0.5. Secondly, $p_{\rm intra}$ represents the reproducibility of the response. Specifically, it is the probability that a PUF instance returns the same response when the same challenge is given to the instance. When $p_{\rm intra}$ is large, it is difficult to determine whether the response comes from the same instance or not, and hence $p_{\rm intra}$ should be close to zero.

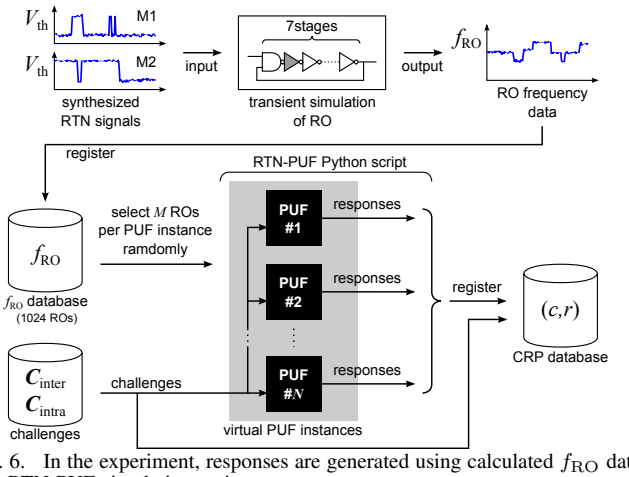


Fig. 6. In the experiment, responses are generated using calculated $f_{\rm RO}$ data and RTN-PUF simulation script.

B. Numerical Experiment

Fig. 6 shows the flow chart of the numerical experiment. We first construct a collection of the RTN-induced frequency fluctuations through Monte Carlo simulations. Seven-stage inhomogeneous ROs are designed using a 65-nm commercial CMOS process. In this experiment, only the RTN of the two transistors, i.e. M1 and M2 in Fig. 5, are considered. This assumption is reasonable because $V_{\rm th}$ of these transistors have 100 times higher impact on the oscillation frequency [7] than the others. In order to simulate the RTN-induced $V_{\rm th}$ fluctuation, voltage sources are connected to gate terminals of these transistors and they are controlled according to the synthesized RTN signals whose parameters and their distributions are based on the measurement results in [2], [8]. RTN-induced frequency fluctuations of 1024 ROs are obtained by transient transistor-level circuit simulations. Then, among these ROs, 256 ROs are randomly selected to compose a single virtual RTN-PUF instance. In this experiment, 128 RTN-PUF instances are constructed. Here, let M be the number of ROs included in a single RTN-PUF instance and N be the number of RTN-PUF instances for later references. The response generation procedure in Fig. 4 is simulated using Python scripting language.

For the estimation of $p_{\rm inter}$, we first generate a sequence of challenges $\boldsymbol{C}_{\rm inter}$. Then, a pair of RTN-PUF instances is randomly selected from the N instances. Using the same sequence of challenges ($\boldsymbol{C}_{\rm inter}$), the sequences of responses from two instances ($\boldsymbol{R}$ and $\widehat{\boldsymbol{R}}$) are simulated and the Hamming distance ($d_{\rm inter}$) between $\boldsymbol{R}$ and $\widehat{\boldsymbol{R}}$ is calculated. The above procedures from the selection of an RO pair to the calculation of Hamming distance are repeated to obtain a statistical distribution of $d_{\rm inter}$. According to [4], the distribution of $d_{\rm inter}$ follows the binomial distribution $B(L, p_{\rm inter})$, where L is the response bit length. Hence, $p_{\rm inter}$ is calculated by finding x of $B(L,x)$ that best fit to the distribution.

The estimation of $p_{\rm intra}$ proceeds in the same way except that the same sequence of challenges $\boldsymbol{C}_{\rm intra}$ is repeatedly applied to the same PUF instance to characterize the stability of the generated responses. Among generated CRPs, the one that was most frequently observed is considered as "correct" CRP and the Hamming distance from the correct response is calculated to be $d_{\rm intra}$. In [4], it is reported that $d_{\rm intra}$ again follows the binomial distribution $B(L, p_{\rm intra})$, which means that $p_{\rm intra}$ can be estimated using the fitting as well as $p_{\rm inter}$. However, $p_{\rm intra}$ may be too small to estimate precisely. Thus, we obtain $p_{\rm intra}$ by calculating the average of $d_{\rm intra}/L$ by

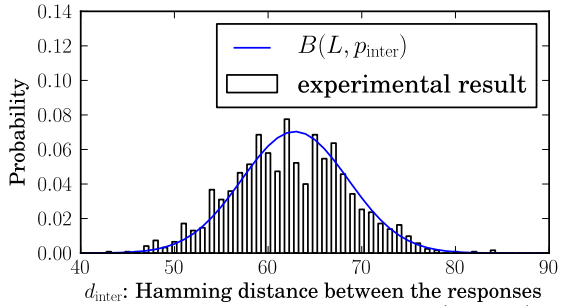


Fig. 7. The probability distribution of $d_{\rm inter}$ and $B(L, p_{\rm inter})$, $p_{\rm inter} = 0.48$.

repeating the above procedures.

The length of response used in a single device authentication, L, is set to 128 by considering the number of ROs embedded in a single PUF instance, M=256. When L is more than a half of the number of ROs, some ROs should be reused for the response generation, which deteriorates the uniqueness of the response. In order to avoid this deterioration in the uniqueness, a single PUF should contain twice or more number of ROs than the number of bits in response.

C. RTN Parameters and PUF Settings

The synthetic RTN signals are obtained from a Markov model with 2^n states, where n is the number of traps in a transistor that is typically in the range of 1–3 [9]. The expected number of $V_{\rm th}$ changes during Δt is $\Delta t/\tau$, where τ is the time constant of RTN. $\Delta V_{\rm th}$ is reported to follow an exponential distribution [8], and τ is distributed uniformly on a logarithmic scale in the range of 10^{-7}–10^{1} s [2].

The sampling clock frequencies for $f_{\rm RO}$ and $N_{\rm RO}$ are set to 1 kHz and 100 kHz respectively, which means that the frequencies of ROs are measured every 10 μs and the fluctuation counts are compared every 1 ms. RTN with time constants except for 10^{-5}–10^{-3} s are dismissed. The threshold for detecting the stair-like fluctuation in oscillation frequency ($\Delta f_{\rm ref}$) is set to 150 kHz, which is approximately 0.1% of the average frequency of the ROs.

In order to enhance the reliability, RO PUF [4] employs a 1-out-of-8 scheme, in which eight pairs of ROs are selected according to a challenge and the pair with the maximum frequency difference is used to generate a response. In this paper, we also employ the 1-out-of-8 scheme in order to compare RTN-PUF and RO PUF under the same conditions. Note that, in the case of RTN-PUF, the pair of ROs that has the largest difference in the number of fluctuation counts is selected.

D. Experimental Results

Fig. 7 shows the histogram of $d_{\rm inter}$, the Hamming distance of the two responses, and the model distribution $B(L, p_{\rm inter})$. The model distribution well approximates the distribution of $d_{\rm inter}$ obtained in the simulation experiment. By fitting the model to the distribution using the least square method, we calculate the average of $p_{\rm inter}$ to be 0.48.

On the other hand, $p_{\rm intra}$ of RTN-PUF was calculated to be 8.0×10^{-5}. We confirmed that the same value is obtained by estimating $p_{\rm intra}$ using the obtained distribution of $d_{\rm intra}$ and the model distribution $B(L, p_{\rm intra})$.

TABLE I shows the $p_{\rm inter}$ and $p_{\rm intra}$ of RTN-PUF and RO PUF. $p_{\rm inter}$ of the proposed RTN-PUF is a little closer to 0.5 than that of the RO PUF [4]. This means that the proposed RTN-PUF achieves better uniqueness than the existing RO PUF, but the both of them achieve the sufficient uniqueness.

TABLE I. COMPARISON OF $p_{\rm inter}$ AND $p_{\rm intra}$ BETWEEN RTN-PUF AND RO PUF

	$p_{\rm inter}$	$p_{\rm intra}$
RTN-PUF	0.48	8.0×10^{-5}
RO PUF	0.46	4.8×10^{-3}

$p_{\rm intra}$ of RTN-PUF is 60 times smaller than that of the RO PUF. In [4], an example of PUF-generated cryptographic keys using BCH (127, 64, 21) code is given to estimate robustness of RO PUF. The PUF response is used as a seed to generate and re-generate cryptographic keys. If the PUF returns a different response to the same challenge, the two keys will not correspond, which makes it impossible to authenticate devices. RO PUF fails to re-generate the same key with the probability 4.5×10^{-11} if 10 errors in a 127-bit response can be corrected. In the case of RTN-PUF, the smaller failure probability can be realized even if the number of allowed errors is reduced to 4, which simplifies error correction hardware. After all, we can conclude that the time constant variation of RTN can make PUFs more robust than the existing ones that use static transistor parameter variation.

V. CONCLUSION

This paper proposed an RTN-based PUF that generates responses by comparing the number of frequency fluctuations in ROs. Through numerical experiments, the proposed PUF proved to be superior to the existing RO PUF, especially in terms of its robustness. This indicates that RTN time constant variation is useful to improve PUF's robustness. The future work is experimental validation of the proposed PUF.

ACKNOWLEDGMENT

This work is partially supported by JSPS KAKENHI Grant Number 26280014. This work is also supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Synopsys, Inc.

REFERENCES

[1] B. Gassend, D. Clarke, M. van Dijky, and S. Devadas, "Silicon physical random functions," in *Proc. Computer and Communication Security Conf.*, 2002, pp. 148–160.

[2] T. Nagumo, K. Takeuchi, T. Hase, and Y. Hayashi, "Statistical characterization of trap position, energy, amplitude and time constants by RTN measurement of multiple individual traps," in *Proc. International Electron Devices Meeting*, 2010, pp. 28.3.1–28.3.4.

[3] J. Chen, T. Tanamoto, H. Noguchi, and Y. Mitani, "Further investigations on traps stabilities in random telegraph signal noise and the application to a novel concept physical unclonable function (PUF) with robust reliabilities," in *Dig. Tech. papers VLST Tech. Symp.*, 2015, pp. T40–T41.

[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. Design Automation Conf.*, 2007, pp. 9–14.

[5] T. Mizutani, A. Kumar, and T. Hiramoto, "Analysis of transistor characteristics in distribution tails beyond $\pm 5.4\sigma$ of 11 billion transistors," in *Proc. IEEE Int. Electron Devices Meeting*, 2013, pp. 33.3.1–33.3.4.

[6] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," *Cryptographic Hardware and Embedded Systems*, pp. 63–80, 2007.

[7] S. Fujimoto, I. Mahfzul, T. Matsumoto, and H. Onodera, "Inhomogeneous ring oscillator for within-die variability and RTN characterization," *IEEE Trans. Semicond. Manuf.*, vol. 26, pp. 296–305, 2013.

[8] N. Tega, H. Miki, F. Pagette, D.J. Frank, A. Ray, M.J. Rooks, W. Haensch and K. Torii, "Increasing threshold voltage variation due to random telegraph noise in FETs as gate lengths scale to 20 nm," in *Proc. Symp. VLSI Technology*, 2009, pp. 50–51.

[9] T. Obara, A. Teramoto, A. Yonezawa, R. Kuroda, S. Sugawa and T. Ohmi, "Analyzing correlation between multiple traps in RTN characteristics," in *Proc. Reliability Physics*, 2014, pp. 4A.6.1–4A.6.7.