Electromagnetic Side-Channel Analysis Against TERO-Based TRNG

Saki Osaka, Daisuke Fujimoto, Member, IEEE, Shinichi Kawamura, Senior Member, IEEE,
and Yuichi Hayashi, Senior Member, IEEE

Abstract—True random number generators (TRNGs) based on ring oscillators are employed in many devices because they can be constructed with logic gates only. Random numbers generated by TRNGs are used for various cryptographic systems as session keys, nonces, and masks. The randomness of a TRNG is characterized by uniformity, nonreproducibility, and unpredictability. Moreover, the quality of random numbers affects cryptographic systems. In particular, degradation of the unpredictability can reduce the security of the cryptographic system because random numbers can be easily estimated. Side-channel attacks, which exploit additional information leaked from a cryptographic module to reveal secret information, are well known. Some additional information reflecting the output bit can be measured from electromagnetic (EM) emission as a side-channel leakage against a TRNG, the unpredictability of the TRNG may decrease. Accordingly, this article introduces the leakage model that reflects an output bit generated by a transition effect ring oscillator (TERO) based TRNG, and an attack that estimates random number bits by measuring EM emission from an integrated circuit against TERO-based TRNG. We propose a leakage model against a TERO-based TRNG and demonstrate that the output bits of the TRNG can be estimated by analyzing the radiated emissions. We also consider a countermeasure against the proposed attack.

Index Terms—Electromagnetic (EM) information leakage, side-channel analysis, true random number generator.

I. INTRODUCTION

TRNG random number generators (TRNGs) generate random numbers based on a random physical phenomenon called an entropy source. Random numbers generated by TRNGs are used for various cryptographic systems as session keys, nonces, initialization vectors, and masks. The security of these applications relies on the uniformity and unpredictability of the utilized random numbers. In particular, failure in unpredictability can greatly reduce the security of the cryptographic device, should the random numbers be easily estimated. It has been reported that the use of random number generators (RNGs) with low unpredictability caused vulnerabilities in some cryptosystems and reduced confidentiality [1], [2].

An interesting theoretical analysis regarding the unpredictability of the RNGs implemented on hardware was proposed by Markus [3], who showed that the output of a certain RNG is predictable due to the following two factors.

1) The entropy source of the RNG provides low entropy.
2) The information that reduces the entropy of the output bit can be acquired.

These factors indicate that the entropy of the output can be significantly lower than the entropy assumed at the time of design, and thus, an attack against the unpredictability of the RNG is feasible. Thus, in recent years, there has been a demand to evaluate the entropy of TRNGs. The SP 800-90B [4], a special publication of the National Institute for Standards and Technology (NIST), contains the requirements for TRNG design. According to this document, a theoretical rationale for the unpredictable behavior of the entropy source is required to design a TRNG. AIS-20/31 [5], which contains the design recommendations of the German Federal Bureau for In-formation Security, requires a formal security analysis of the TRNG design based on a stochastic model of the entropy source. In accordance with these requirements, various TRNGs have been developed and evaluated for stochastic models of entropy sources. In particular, TRNGs based on ring oscillators (ROs) can be configured with logic gates only, and many designs have been proposed [6]–[8]. Among them, the transition effect ring oscillator (TERO) based TRNG, which uses metastability as the entropy source, is widely used because it can generate random numbers with a high entropy and bit rate [9]. A stochastic model that reflects the random physical process has also been proposed as an alternative to TERO-based TRNGs to ensure that the output of the TRNG has statistically sufficient entropy [10]. Therefore, TERO-based TRNGs are also considered to be unpredictable.

However, these design guidelines and stochastic model evaluations are intended to alleviate the issues caused by the first factor described previously. The second factor has not been fully evaluated as yet. To evaluate it, it is necessary to 1) construct and assess an information leakage model that reduces the entropy of the output bit, and 2) evaluate the output bit estimation method...
based on the leakage model. Hence, it is difficult to enumerate this factor, and so far, few studies have identified information leakage that reduces the entropy of TRNGs that use ROs as entropy sources [11].

Moreover, side-channel attacks, which exploit additional information leaked from a cryptographic module to reveal secret information, are well known [12]–[17]. In such attacks, the secret key is analyzed by modeling changes in power consumption or electromagnetic (EM) radiation during cryptographic processing as information leakage sources. These side-channel leakages due to changes of power consumption or electromagnetic (EM) emission can also occur during the TRNG operation. If the output of a TRNG can be estimated using side-channel attacks, the security of the entire cryptographic system may be greatly reduced.

In this article, we aim to mitigate these problems by investigating the possibility of degrading the unpredictability of TRNGs by noninvasive side-channel attacks against TERO-based TRNGs, which are widely used in cryptographic hardware. Specifically, we propose an information leakage model indicating the output bits of a TERO-based TRNG and measure the EM emission with a near-field magnetic probe. Then, we propose an analysis method for estimating output bits from the EM emission. Simultaneously, since the proposed attack may significantly reduce the security of cryptographic hardware that implements TERO-based TRNGs, we also propose circuit-level countermeasures against such attacks.

The rest of this article is organized as follows. In Section II, the leakage model that reflects an output bit is proposed, and the output bit estimation method using EM emission is described. In Section III, we evaluate the leakage model, and then demonstrate the feasibility of the proposed attack by practically estimating a random sequence. In Section IV, the countermeasure against the proposed attack is investigated and evaluated. Finally, Section V concludes this article.

II. PROPOSAL FOR THE OUTPUT BIT ESTIMATION METHOD USING A SIDE-CHANNEL ATTACK AGAINST A TERO-BASED TRNG

In Section II-A, we describe the structure of the TERO-based TRNG and the principle of random number generation. In Section II-B, a leakage model of side-channel information indicating the output bits of TERO-based TRNGs and its measurement technique are proposed. Next, we devise an analysis method for estimating output bits from a single side-channel trace.

A. TERO-Based TRNG Architecture

The TERO-based TRNG was proposed in [8] and its stochastic model appears in [10]. The TERO is a multi-event ring oscillator that oscillates temporarily. It is composed of an even number of inverters and a couple of NAND gates that restart temporary oscillations (see Fig. 1). Following the rising edge of the $V_{\text{ctrl}}$ input, the outputs $V_{\text{out1}}$ and $V_{\text{out2}}$ start to oscillate (see Fig. 2). This state is called the metastable state. These signals circulate inside the loop until a collision occurs, during which the edge that moves faster reaches the slower one. The difference in the speed of these signals is caused by differences in delays between inverters in loop branches and by the analog phenomena that occur in the inverters. After the collision, these signals are stabilized, and this state is called the stable state. The number of oscillations before the outputs stabilize is not constant but varies due to the electronic noises. The number of oscillations is counted by a T flip-flop, and the output signal of the T flip-flop after TERO stabilization is a 1-bit random number. If the output signal of the T flip-flop is low when the TERO becomes stable, the output bit is 0 [see Fig. 2(c)]. On the other hand, if the output signal of the T flip-flop is high when the TERO becomes stable, the output bit is 1. In order to harvest sufficient entropy, the TERO has to stabilize before $V_{\text{ctrl}}$ falls. In [9], the conditions for the number of oscillations of the TERO to obtain sufficient entropy are described. As a general configuration, every time an output bit is generated, the T flip-flop that counts the number of oscillations of the TERO is kept stable. As a result, the output of the TERO is reset [8]–[10]. The reset signal is input after generating an output bit. This signal is generated by the clock, and the T flip-flop is reset after a certain period from the rising edge of $V_{\text{ctrl}}$.

B. Leakage Model That Reflects an Output Bit

This section outlines the leakage model of side-channel information reflecting an output bit of the TERO-based TRNG.

In side-channel attacks against cryptographic hardware, a secret key is analyzed by measuring the change in power consumption at the complementary metal-oxide-semiconductor (CMOS) gate as the side-channel information [12], [13], [17]. The mechanism behind the leakage is discussed in [19] and [20] based on the switching behavior of the CMOS gates. Therefore,
if a leakage model that relates the output bit of the TRNG and the switching of the CMOS gates can be established, the output bit can be estimated from the side-channel leakage.

As shown in Fig. 3, when the reset signal is input to a T flip-flop, the circuit operation changes depending on the previous state. If the output of the T flip-flop is low before the reset signal (i.e., the output bit is 0), the output does not change when the reset signal is input [see Fig. 3(a)]. This phenomenon indicates that the power consumption is low because the CMOS gates do not switch. On the other hand, if the output of the T flip-flop is high before the reset signal (i.e., the output bit is 1), the output changes when the reset signal is input [see Fig. 3(b)]. At this time, the reset signal is input to switch from high to low at the CMOS gates, and discharge occurs. This phenomenon indicates that when the output bit is 1, the power consumption increases temporarily. Therefore, it is considered that the power consumption of a T flip-flop when the reset signal is input becomes a leakage source of side-channel information reflecting an output bit.

There is a possibility that such a steep change in power consumption can be observed from outside the device by measuring the near field above the chip. Changes in power consumption are observed as differential signals in EM emission, which is used as a side-channel information. Here, the side-channel information is described as follows: when the output bit is 0, the CMOS gates do not switch, and thus, a peak is not observed in the side-channel information [see the red arrow in Fig. 3(a)]. In contrast, when the output bit is 1, a peak is observed in the side-channel information due to a steep change caused by the switching of the CMOS gates [see the red arrow in Fig. 3(b)]. The amplitude of such a peak in the EM field depends on the sharpness of the rising edge of the original signal. Therefore, there is a possibility that the side-channel information corresponding to the TRNG output bits can be acquired by EM measurements even in a noisy environment.

C. Output Bits Estimation Method by Analyzing Side-Channel Leakage

The side-channel information that reflects the output bits of the TRNG appears as a change in amplitude value when a reset signal is input to the T flip-flop. Hence, we need an analysis method for estimating the exact timing at which the reset signal is input solely from the measured side-channel information. Accordingly, we propose such a method by analyzing the side-channel information, and then, we estimate the output bits by using the amplitude value.

By measuring EM emission, the switching of the counter during TERO oscillation can also be observed together with the peak or nonpeak at a reset signal timing shown in Fig. 3. In [18], even the number of oscillations of a TERO were estimated by analyzing the side-channel information. As shown in Fig. 2, when the TERO oscillates [see Fig. 2(b)], the output signal of the T flip-flop fluctuates due to the switching of the CMOS gates [see Fig. 2(c)]. Thus, a large amplitude change is also observed in the side-channel information graphs in Fig. 3. Thereafter, the TERO reaches the stable state in Fig. 2(b), and the oscillation of the output signal of the T flip-flop stops [see Fig. 2(c)]. Thus, the amplitude of the side-channel information decreases in Fig. 3. The changes in the side-channel information during TERO oscillation are not temporary peaks; rather, we note a continuous change in the amplitude value (in a blue box in Fig. 3). Therefore, the start of the TERO oscillation, i.e., the rising timing of $V_{\text{ctrl}}$, can be estimated easily by the start of continuous change in the side-channel information. Next, the input timing of the reset signal is described. As shown in Section II-A, the reset signal is generated by the clock, and the T flip-flop is reset after a certain period from the rising edge of the $V_{\text{ctrl}}$. Therefore, by preprofiling the side-channel information from the target device and acquiring time from the start of a continuous change in the amplitude value to the final peak at a reset signal timing in Fig. 3(b), we can estimate the period from the rising edge of $V_{\text{ctrl}}$ to the input of the reset signal. As shown in Section II-B, the output bit appears as a change in the amplitude value of the side-channel information when the reset signal is input. Hence, the output bit can be distinguished by comparison to a threshold for the change in the analyzed amplitude value, i.e., the amplitude value of the side-channel information at the time of resetting the signal input. When the analyzed amplitude value exceeds a threshold, the output bit is estimated as 1, and when the threshold is not exceeded, the output bit is estimated as 0.

In this method, random bit is estimated by using the changes in EM emission that accompany the output of TRNG. Therefore, it is considered that an attack could be established in an environment or implementation where the EM emission generated from the TRNG are easy to measure. Therefore, it is considered that the proposed attack could succeed at least on devices with limited functionality (e.g., smart card, sim card).

III. Experiment

This section demonstrates that TERO-based TRNGs are vulnerable to noninvasive side-channel attacks. Section III-A shows the experimental setup. Section III-B evaluates the leakage model by comparing the T flip-flop output signal measured
from the I/O pin with the side-channel information measured by the near-field magnetic probe. In Section III-C, we demonstrate that the proposed attack is feasible against a TERO-based TRNG in a general configuration that simulates actual devices where the T flip-flop output signal is not output from the I/O pin.

A. Experimental Setup

The experimental setup is described in terms of the implementation of the target device and the required measurement.

A target TERO-based TRNG was implemented in a field programmable gate array (FPGA), as shown in the Fig. 4. TRNG is enabled when the FPGA received a command from a personal computer (PC) via the Universal Asynchronous Receiver Transmitter (UART) module. After generating a continuous 512-bit random number, the output bitstream was transmitted from the UART module to the PC. The TERO-based TRNG under attack was designed with reference to [9]. The clock signal that controls the TERO (i.e., $V_{\text{ctrl}}$) signal) was generated by an 11-stage RO and an 8-bit asynchronous counter. When the rising edge of the clock was input, the TERO started oscillating and stabilized before the clock fell. A reset signal was input to the T flip-flop at the falling edge of the clock pulse. The TERO consisted of two NAND gates and 20 inverters. The number of oscillations of the TERO was counted with the T flip-flop, and the T flip-flop output at the fall of $V_{\text{ctrl}}$ was a 1-bit random number. A trigger signal indicating the start of random number generation was output from the I/O pin.

Fig. 5 shows the experimental setup. The target TERO-based TRNG was implemented on the FPGA (Spartan6 LX9 Microboard). The FPGA under attack was powered from a PC via a USB cable. Side-channel information was measured with a near-field magnetic probe (Langer EMV, RF-U 5-2), which was used to measure the magnetic field of surface currents within conducting paths. The measured side-channel information was amplified with a low noise amplifier (COSMOWAVE, LNA270WS) and then observed with an oscilloscope (Keysight, DSOS204A).

B. Evaluation of the Leakage Model

In this section, we show that the operation of the T flip-flop changes corresponding to the output bit of the TRNG when the signal input is reset, and these changes can also be observed in the side-channel information. The oscillation frequency of the TERO was 127.56 MHz, and the frequency of the clock controlling the TERO was 434.30 kHz. In this experiment, the output signal of the T flip-flop was output from the I/O pin.

Figs. 6 and 7 show the output signal of the T flip-flop and side-channel information when the output bit is 0 or 1, respectively. In either case, the following phenomena are observed: when the TERO becomes stable, the fluctuation of the side-channel information increases. On the other hand, when the output signal of the T flip-flop is stabilized, the fluctuation of the side-channel information is reduced.

If the output signal of the T flip-flop is low when the TERO becomes stable, the output bit is 0 [see Fig. 6(a)]. At this time, even if a reset signal is input, the output signal of the T flip-flop does not change. Therefore, it is confirmed that the amplitude value does not change in the side-channel information [see the red arrow in Fig. 7(a)]. On the other hand, if the output signal of the T flip-flop is high when the TERO becomes stable, the output bit is 1 [see Fig. 6(b)]. At this time, the output signal of the T flip-flop reduces due to the input of the reset signal, and the switching of the CMOS gates occurs. Therefore, the peak of
the amplitude value reflecting the switching of the CMOS gate in the side-channel information is observed [see the red arrow in Fig. 7(b)]. These results indicate that the amplitude value of the side-channel information changes depending on the output bit of the TRNG. Hence, it was considered that the proposed leakage model can be used for attacks.

C. Estimating Output Bits Using a Single Side-Channel Trace

In this section, we demonstrate that output bit estimation is feasible in a general device simulating an actual device.

First, we show that the leakage model can be observed even in such a device. Subsequently, we prove that the distribution of the amplitude value of the side-channel information changes corresponding to the output bit. Finally, we demonstrate the estimation results for continuous 512-bit random sequences generated by the TERO-based TRNG.

In order to simulate actual devices, the FPGA under attack did not output signals related to the TRNG (i.e., the output of the TERO, output of the T flip-flop, and clock signal) outside the chip, except for the UART module. Only the trigger signal indicating the start of random number generation was output from the I/O pin. Therefore, under this experimental environment, it is considered only a few leakages of side-channel information due to I/O output, which can be regarded as a leakage source, will occur. In addition, since the UART module that transmitted the generated output bitstream to the PC started operation after the TRNG was disabled, the information leakage from the UART module and its communication are considered not to occur during the EM measurement.

Fig. 8 shows the side-channel information during the generation of the output bits. The output bits corresponding to the side-channel information waveform are also shown. Similar to the side-channel information shown in Fig. 7, it was observed that the changes in the side-channel information reflect the oscillation of the TERO and the output signal of the T flip-flop. Therefore, the interval indicated by the blue arrow in Fig. 8 is estimated to be one cycle of the clock that controls the TERO, and it is considered that the TRNG generated a 1-bit random number during this period. In the TRNG configuration used in this experiment, the reset signal was input at the falling edge of the clock pulse. Thus, it was considered that the reset signal was input at the time indicated by the red arrow. In Fig. 8, when the output bit acquired from the UART module is 1, a peak is observed. On the other hand, when the output bit is 0, no peak is observed. These results indicate that the leakage model evaluated in the previous section applies even to an actual device.

Subsequently, the distribution of amplitude values corresponding to the output bits was evaluated. Continuous 512-bit random sequence generation was repeated 100 times while measuring side-channel information. We acquired the side-channel information and the 51200-bit random numbers acquired via the UART module. As can be seen in Fig. 8, the side-channel information fluctuates in both positive and negative directions with respect to the average value of the waveform. Thus, the preprocessing was performed as follows: The waveform was subtracted from the average value of the waveform and the absolute value was taken. Subsequently, after detecting the start of the oscillation of the TERO \((t = t_0)\), the period during which a reset signal was expected to be input was extracted. In this experiment, the time period \([t_0+1.42, t_0+1.46 \text{us}]\) was used for the analysis. The maximum amplitude value in this period was used as a feature value. The distribution of feature values corresponding to output bits acquired via the UART module is shown in Fig. 9. The figure shows histograms, with the horizontal axis representing the feature values and the vertical axis representing the proportion. It can be confirmed that when the output bit is 0, the feature value is distributed to less than 0.08 V, whereas when the output bit is 1, the feature value is distributed to 0.08 V or more. These results indicate that the amplitude value of the side-channel information changes greatly corresponding to the output bit, and we consider that the output bit can be estimated by using this feature value.

Finally, in order to demonstrate that the TRNG output bits can be predicted using side-channel information, we estimated continuous 512-bit random sequences. Continuous 512-bit random number generation was repeated 100 times while measuring side-channel information and acquiring output bits via the UART module. Then, preprocessing and feature value calculation were performed on the side-channel information, as described previously. The threshold value was set to 0.082 V for the feature value. The output bit was estimated to be 1 if feature value was greater than or equal to the threshold, and 0 if it was less than the threshold. We succeeded in fully estimating 512-bit random numbers for all the random sequences that were considered.

Therefore, we demonstrated that a noninvasive side-channel attack against a TERO-based TRNG is a feasible attack that greatly reduces the unpredictability of the TRNG.
IV. COUNTERMEASURE AGAINST THE PROPOSED ATTACK

In this section, we investigate a countermeasure to ward off a proposed attack against a TERO-based TRNG. First, we examine the feasibility of the proposed method in a general TRNG configuration. Next, countermeasure technology at the circuit-level is proposed, and then, the resistance against the proposed attacks is evaluated.

Fig. 10 shows a TRNG general structure recommended by NIST SP800-90B [4] and AIS-20/31 [5]. This configuration recommends implementation of a health test that verifies the randomness of the TRNG and a postprocessing module that improves the randomness of the raw bits.

Until now, various health tests have been proposed, such as a health test that evaluates the entropy of analog noise source and another that assesses the raw bits of a TRNG [21], [22]. However, since the proposed attack obtains side-channel information noninvasively, it is considered that the attack does not affect the randomness of the analog noise source or the output bits. Hence, it is difficult to detect the attack even when using health test modules, and thus, the proposed attack could be effective even for a device that implements a health test.

As shown in the previous section, the proposed method can successfully estimate the whole random sequence. This result shows that if the attacker knows the design of the implemented postprocessing modules, the postprocessed output bits can also be estimated. Therefore, the output bit estimation by the proposed method may be realized even for a general TRNG configuration, and thus, implementing countermeasures is essential.

A. Circuit-Level Countermeasure

Since the proposed method performs side-channel attacks by EM measurements, suppressing leakage of side-channel information that reflects output bits by means of algorithms or gate-level countermeasures is effective. In this section, we propose a circuit-level countermeasure that suppresses the proposed leakage model of side-channel information.

The leakage model based on the attack uses switching of the CMOS gate according to the output bit when the reset signal is input. As a simple countermeasure, a circuit configuration in which power consumption does not change by switching according to the output bit can be considered. Specifically, by eliminating the reset of the T flip-flop, we consider that the difference in power consumption due to switching depending on the output bit does not occur. Therefore, the side-channel information reflecting the output bit based on this leakage model cannot be observed. Even if the T flip-flop is not reset, the stochastic model of TERO will not change. Therefore, the implementation of this countermeasure is not expected to reduce the randomness of the TRNG.

B. Evaluation of the Countermeasure

In this section, side-channel leakage is evaluated for the TERO-based TRNG that implements the countermeasure proposed in Section IV-A.

The TERO-based TRNG used in the evaluation is the same as that applied in the implementation in Section III-B. Here, the operation of the reset signal is controlled by an AND gate and the physical switch on the FPGA. The output bits in this implementation, where the reset signal is fixed, were evaluated by NIST’s randomness test suite [21], and then it was confirmed that there was no statistical difference in randomness compared to the original implementation. The experimental setup is the same as that in Section III. The oscillation frequency of the TERO was 127.56 MHz, and the frequency of the clock controlling the TERO was 434.30 kHz. The output signal of the T flip-flop and the trigger signal indicating the start of random number generation were output from the I/O pin and measured with an oscilloscope. The side-channel information was measured by a near-field magnetic probe.

Figs. 11 and 12 show the output signal of the T flip-flop and side-channel information when the output bit is 0 or 1, respectively. Since the T flip-flop was not reset, the output signal of the T flip-flop changes only when the TERO was oscillating. In Fig. 12, the fluctuation in the amplitude value reflecting the oscillation of the TERO and the T flip-flop in the side-channel information is observed. Changes in the amplitude
we confirmed that the side-channel leakage is suppressed by the countermeasure. When the output bit is 1 and 0 have approximately the same amplitude value as the feature value was the same as that in Fig. 9(b), and the feature value is smaller than that shown in Fig. 9(b), and it is difficult even if an arbitrary threshold value is used. In addition, the feature value reflecting the output bit due to the reset signal are not observed. Therefore, we confirmed that it is difficult to conduct an attack when the countermeasure is in place.

Next, we investigated whether the output bits could be estimated by observing the side-channel leakage. Fig. 13 shows the side-channel information while the output bits were generated. The output bits corresponding to the side-channel information waveform are also shown. Similar to the side-channel information shown in Fig. 8, changes in side-channel information indicating the oscillation of the TERO and the T flip-flop were observed. On the other hand, the change in the amplitude value of the side-channel information at the falling edge of the clock pulse for controlling the TERO (i.e., the input of the reset signal) was not observed.

Subsequently, the distribution of amplitude values corresponding to the output bits was evaluated. Continuous 512-bit random sequence generation was repeated 100 times while measuring the side-channel information. We acquired the side-channel information, and the 51200-bit random numbers were acquired via the UART module. The method for analyzing the amplitude value as the feature value was the same as that in Section III-C. The distribution of the feature values corresponding to the output bits acquired via the UART module is shown in Fig. 14. It can be confirmed that the feature distributions when the output bit is 1 and 0 have approximately the same shape. According to this result, distinguishing the output bit is difficult even if an arbitrary threshold value is used. In addition, the feature value is smaller than that shown in Fig. 9(b), and we confirmed that the side-channel leakage is suppressed by the countermeasure.

Hence, we showed that the proposed countermeasure reduces the side-channel leakage reflecting the output bits.

V. CONCLUSION

In this article, we proposed a leakage model that reflects an output bit generated by a TERO-based TRNG and a method to estimate the output bits of a TRNG using a noninvasive side-channel attack. It was demonstrated that this estimation is possible by using a proposed leakage model and measuring and analyzing EM emission as a side-channel information. Since the implementation of a TRNG used for evaluation is a general configuration that simulates actual devices, the proposed attack may affect many devices that implement a TERO-based TRNG. In addition, the proposed method demonstrated high predictive performance; thus, the unpredictability could decrease even for TRNGs that implement postprocessing modules.

We conducted an experiment wherein the side-channel information was measured by using a near-field magnetic probe. In the EMC field, it is known that common-mode current propagates through cables [23]–[28]; it has already been shown that EM emission caused by common-mode currents causes unintentional information leakage via a power cable of a cryptographic device [16], [17], [28]. Therefore, as well as the cryptographic module, there is a possibility the side-channel leakage of TERO-based TRNGs is observed outside the device through the common-mode current using the same principle. Hence, the attack may be possible from a distance.

The goal of this article is to point out the new potential vulnerabilities against a TERO-based TRNG and to provide its countermeasure. In the security field, the discovery of new vulnerabilities often can be applied to attacks on other cryptographic techniques. The scope of this attack can be extended to other TRNGs and cryptographic processing, because the implementation of T flip-flops causes information leakage of output bits. In addition, clarifying the security boundaries of the proposed vulnerability will lead to the examination of practical scenarios, and will be an issue for the future.

REFERENCES

[1] M. Bellare, S. Goldwasser, and D. Micciancio, “‘Pseudo-random’ number generation within cryptographic algorithms: The DSS case,” in CRYPTO’97, LNCS, vol. 1294, B. S. Kaliski, Jr. Ed. Heidelberg, Germany: Springer, 1997, pp. 277–291.
[2] L. Bello, “DSA-1571-1 openssl–predictable random number generator,” Debian Security Advisory, 2008. [Online]. Available: http://www.debian.org/security/2008/dsa-1571
[3] D. Markus, “How to predict the output of a hardware random number generator,” in Proc. Int. Workshop Cryptographic Hardware Embedded Syst., 2003, pp. 181–188.
[4] M. S. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, “Recommendation for the entropy sources used for random bit generation,” National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. SP800-90B, 2018.
[5] W. Killmann and W. Schindler, "A proposal for: Functionality classes for random number generators," in Proc. ACM/SIGDA 12th Int. Symp. Field Programmable Gate Arrays., 2004, pp. 71–78.
X. Hayashi et al., “Analysis of electromagnetic information leakage from cryptographic devices with different physical structures,” IEEE Trans. Electromagn. Compat., vol. 55, no. 3, pp. 571–580, Jun. 2013.

K. Ikobe, T. Amano, K. Okamoto, and Y. Toyot, “Equivalent circuit modeling of cryptographic integrated circuit for information security design,” IEEE Trans. Electromagn. Compat., vol. 55, no. 3, pp. 581–588, Jun. 2013.

K. Ikobe, T. Kan, and Y. Toyota, “A study on evaluation board requirements for assessing vulnerability of cryptographic modules to side-channel attacks,” in Proc. IEEE Int. Symp. Electromagn. Compat. Signal/Power Integrity, 2020, pp. 528–531.

K. Nakamura, Y.-I. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, “Method for estimating fault injection time on cryptographic devices from EM leakage,” in Proc. IEEE Int. Symp. Electromagn. Compat., 2015, pp. 225–240.

S. Osuka et al., “EM information security threats against RO-based TRNGs: The frequency injection attack based on IEMI and EM information leakage,” IEEE Trans. Electromagn. Compat., vol. 61, no. 4, pp. 1122–1128, Aug. 2019.

L. Tebembel, M. Pehl, and V. Immel, “Side-channel analysis of the TERO PUF,” in Proc. Int. Workshop Constructive Side-Channel Anal. Secure Des., 2019, pp. 43–60.

E. Peeters, F. X. Standaert, and J. J. Quisquater, “Power and electromagnetic analysis: Improved model, consequences and comparisons,” Integration, VLSI J., vol. 40, no. 1, pp. 52–60, 2007.

S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, vol. 31. New York, NY, USA: Springer Science & Business Media, 2008.

V. B. Suresh, D. Antonioli, and W. P. Burleson, “On-chip lightweight implementation of reduced NIST randomness test suite,” in Proc. IEEE Int. Symp. Hardware-Oriented Secure. Trust, 2013, pp. 93–98.

B. Yang, V. Rožič, M. Grujić, N. Mentens, and I. Verbauwhede, “On-chip jitter measurement for true random number generators,” in Proc. Asian Hardware-Oriented Secure. Trust, 2017, pp. 91–96.

T. H. Hubing, “Printed circuit board EMI source mechanisms,” in Proc. IEEE Symp. Electromagn. Compat., 2003, vol. 1, pp. 1–3.

M. Vuagnoux and S. Pasini, “An improved technique to discover compromising electromagnetic emanations,” in Proc. IEEE Int. Symp. Electromagn. Compat., 2010, pp. 121–126.

J. DREWNIAK, F. SHA, T. VAN DOREN, T. HUBING, AND J. SHAW, “Diagnosing and modeling common-mode radiation from printed circuit boards with attached cables,” in Proc. IEEE Symp. Electromagn. Compat., 1995, pp. 465–470.

D. Hockanson, J. Drewniak, T. Hu Bing, T. Van Doren, F. Sha, and M. Wilhelm, “Investigation of fundamental EMI source mechanisms driving common-mode radiation from printed circuit boards with attached cables,” IEEE Trans. Electromagn. Compat., vol. 38, no. 4, pp. 557–566, Nov. 1996.

S. Wada, Y. Hayashi, D. Fujimoto, N. Homma, and Y. Kim, “Measurement and analysis of electromagnetic information leakage from printed circuit board power delivery network of cryptographic devices,” IEEE Trans. Electromagn. Compat., vol. 63, no. 5, pp. 1322–1332, Oct. 2021.

Y. Hayashi et al., “Analysis of information leakage from a cryptographic hardware via common-mode current,” in Proc. IEEE Int. Symp. Electromagn. Compat., 2009, pp. 17–20.