Journal of Electronic Testing
https://doi.org/10.1007/s10836-018-5746-5

Exploiting Multi-Phase On-Chip Voltage Regulators as Strong PUF Primitives for Securing IoT

Weize Yu[1] · **Yiming Wen**[1] · **Selçuk Köse**[2] · **Jia Chen**[3]

Received: 5 July 2018 / Accepted: 14 August 2018

Abstract

The physical randomness of the flying capacitors in the multi-phase on-chip switched-capacitor (SC) voltage converter is exploited as a novel strong physical unclonable function (PUF) primitive for IoT authentication. Moreover, for the strong PUF we devised, an approximated constant input power is achieved against side-channel attacks and a non-linear transformation block is utilized to scramble the high linear relationship between the input challenges and output responses against machine-learning attacks. The results show that the novel strong PUF primitive we designed achieves a nearly 51.3% inter-Hamming distance (HD) and 98.5% reliability while maintaining a high security level against both side-channel and machine-learning attacks.

Keywords Multi-phase · Voltage converter · Strong physical unclonable function (PUF) primitive · Side-channel attacks · Machine-learning attacks

1 Introduction

With the advent of internet-of-things (IoT), a growing number of significant applications require low-cost and high-security IoT devices [2, 23]. Silicon strong physical unclonable functions (PUFs) are a type of hardware security primitives that can be efficiently utilized as authentication tools for securing the IoT devices [1, 2, 13]. The basic mechanism of silicon strong PUF is exploiting the internal physical randomness of identically designed IC modules induced by the fabrication process to build a unique math function to map the relationship between the input challenges and the output responses. To date, a variety of strong PUFs such as arbiter-PUF [1], lightweight-PUF [12], and clock-PUF [19] have been proposed as authentication tools for securing the IoT devices. Unfortunately, all of the existing strong PUFs [1, 12, 19] are vulnerable to non-invasive attacks.

Side-channel attacks (SCAs) are a sort of powerful non-invasive attacks that can extract the critical information of modern integrated circuits (ICs) through observing and analyzing the corresponding physical leakages, such as power consumption, electro-magnetic (EM) emanations, temperature, and timing information [8, 9, 21]. Accordingly, SCAs can be categorized as: power attacks, EM attacks, thermal attacks, and timing attacks. Power attacks are a type of SCAs that are widely used by attackers to leak the critical information of modern ICs by exploring the correlation between the processed data and the monitored

Responsible Editor: T. Xia

✉ Weize Yu
wyu@odu.edu

Yiming Wen
ywen001@odu.edu

Selçuk Köse
kose@usf.edu

Jia Chen
chen5625@umn.edu

[1] Department of Electrical and Computer Engineering, Old Dominion University, Norfolk, Virginia, USA

[2] Department of Electrical Engineering, University of South Florida, Tampa, Florida, USA

[3] Department of Electrical and Computer Engineering, University of Minnesota Twin Cities, Minneapolis, Minnesota, USA

power consumption [4, 5, 21]. When power attacks are implemented on conventional strong PUFs, like a 64-bit arbiter-PUF and a 64-bit lightweight-PUF, the prediction accuracy of the output response can be over 0.98 if only 26×10^3 items of data are analyzed [11].

Another security challenge of the present strong PUF primitives is the vulnerability against machine-learning attacks [1, 14, 20]. When machine-learning attacks are implemented on a strong PUF primitive, the attacker will input a number of challenges I to the PUF device and gather the corresponding responses R to estimate the math function F that can be used for mapping the relationship between I and R ($R = F(I)$) with advanced machine-learning algorithms. Once the math function F is uncovered by the attacker, the response of the strong PUF primitive can be accurately predicted by the attacker under any input challenge. As demonstrated in [10], if a machine-learning attack is performed on a 128-bit arbiter-PUF by executing the linear regression (LR) algorithm, the prediction accuracy of the output response is able to achieve 0.999 after training 39.2×10^3 number of challenge-to-response pairs (CRPs).

In order to protect modern ICs against power attacks, fully on-chip workload-aware multi-phase voltage regulators (WAMPVRs) such as converter-gating (CoGa) regulator [15] and converter-reshuffling (CoRe) regulator [21] were proposed to mitigate the power information leakage and improve the power conversion efficiency with negligible overhead. If a WAMPVR is utilized as a countermeasure for securing the PUF-embedded IoT devices against power attacks, the conventional design is shown in Fig. 1a. The WAMPVR-based power attack countermeasure thwarts the power information leakage of the conventional strong PUF primitive if an attacker performs a non-invasive power attack. Unfortunately, as shown in Fig. 1a, if the attacker combines a semi-invasive attack with a power attack, the power information leakage of the conventional strong PUF primitive still can be exposed to the attacker directly. The reason is that the attacker may implement a semi-invasive attack to bypass the power attack countermeasure at first, then leak the critical information of the unprotected strong PUF primitive by utilizing a power attack. Therefore, in order to secure the strong PUF primitive against the aforementioned combined attacks, the

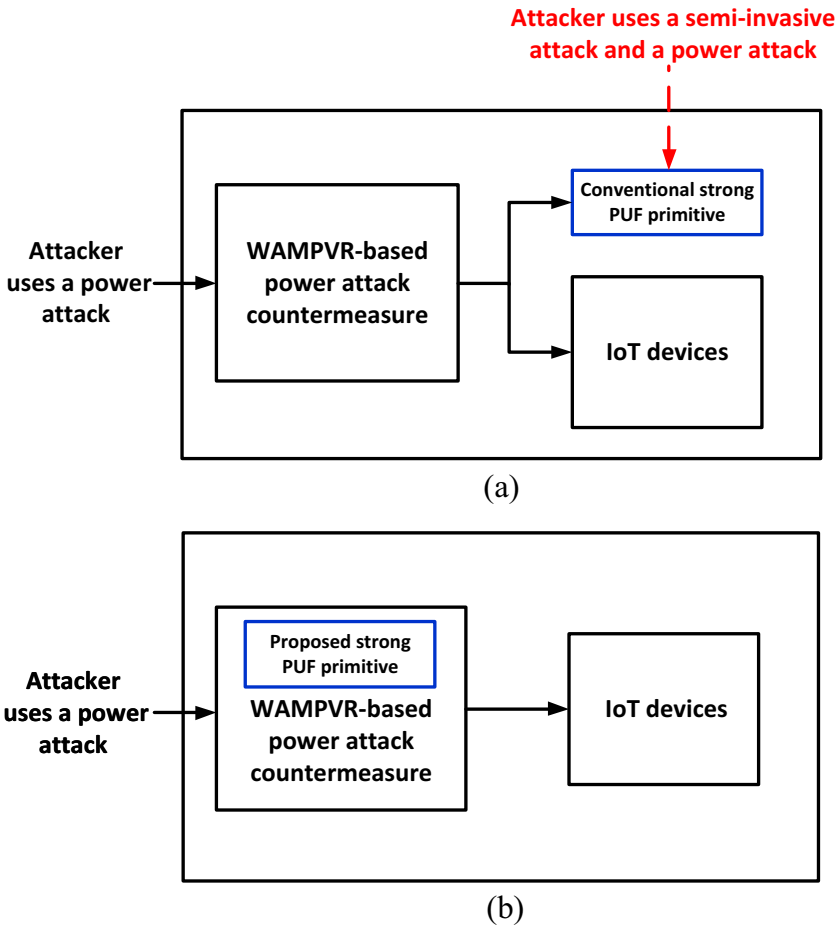


Fig. 1 Floorplans of the PUF-embedded IoT devices employ a power attack countermeasure. **a** Conventional design. **b** Our novel design

floorplan in our novel design is modified, as shown in Fig. 1b. The WAMPVR-based power attack countermeasure is exploited as a strong PUF architecture for authentication. In such a case, the power attack countermeasure thwarts the attacker from capturing the power information leakage of the strong PUF directly. Kindly note that when the authentication is in process, the IoT devices will be deactivated. The primary reason is that the WAMPVR is working as a strong PUF which is unable to deliver power to the IoT devices. However, once the authentication procedure ends, the IoT devices will be activated and the WAMPVR-based power attack countermeasure in Fig. 1b behaves normally to protect the active IoT devices against power attacks. Since the authentication is a one-time process, the overhead induced by turning off and on the IoT devices is negligible.

The primary reason why the existing PUFs [1, 12, 19] are vulnerable to machine-learning attacks is that the electrical signal that contains the high-linearity PUF physical randomness is used for generating the output responses, as shown in Fig. 2a. However, for our proposed WAMPVR-based strong PUF in Fig. 2b, the electrical signal that includes the high-linearity PUF physical randomness is scrambled by a non-linear transformation block for achieving the non-linear output responses against machine-learning attacks.

The rest of the paper is organized as follows. Background of the on-chip WAMPVRs is given in Section 2. The architecture design of WAMPVR-based strong PUF is fully introduced in Section 3. The performance and security of the proposed WAMPVR-based strong PUF are evaluated in Section 4 while the circuit level verification is provided in Section 5. Conclusions are offered in Section 6.

2 Background

The workload-aware multi-phase voltage regulators (WAMPVRs) like converter-gating (CoGa) voltage regulator [15] and converter-reshuffling (CoRe) voltage regulator [21] are designed based on multi-phase switched-capacitor (SC) voltage converters. Integrating WAMPVRs fully on-chip is an efficient solution for reducing the power conversion loss and strengthening the robustness of modern ICs against power attacks [15, 21]. As demonstrated in [15, 21], increasing the total number of phases for the WAMPVRs can result in significant improvements of the power conversion efficiency and the security against power attacks. Accordingly, the designs of on-chip voltage regulators with more than 120 phases have been frequently reported in the recent literatures [6, 7].

For a 2:1 (Input voltage/output voltage=2:1) 32-phase on-chip SC voltage converter, the simulated output voltage ripples are shown in Fig. 3. Case #1 (as shown in Fig. 3a) and Case #2 (as shown in Fig. 3b) indicate that different number of activated phases can generate different output voltage ripple signatures. Furthermore, when we compare Case #2 with Case #3 in Fig. 3b and c, under the same number of active phases, the output voltage ripples are also different if the sequences of activation pattern are different.

In a multi-phase SC voltage converter, the output voltage ripple is extremely sensitive to the flying capacitance in

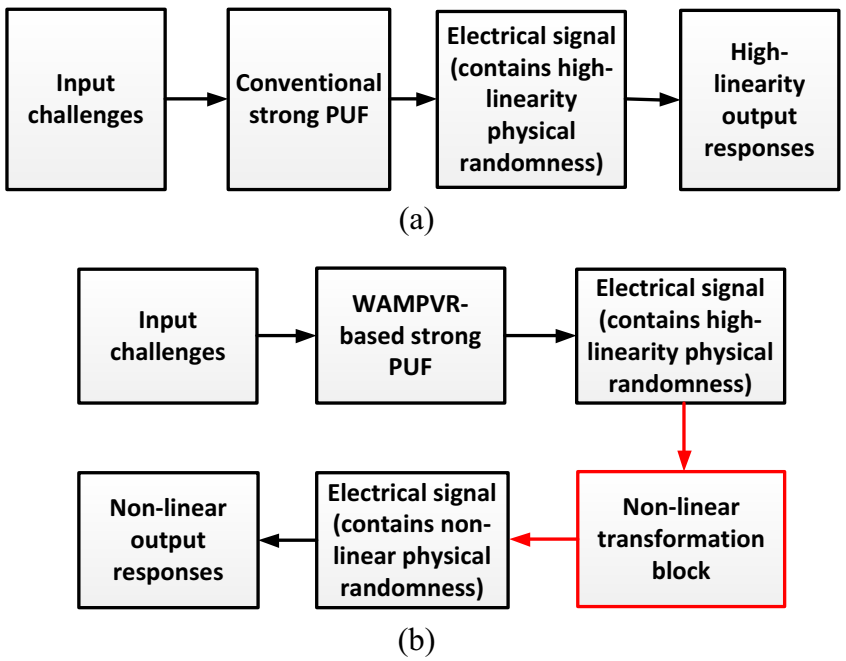


Fig. 2 Diagrams of strong PUFs under machine-learning attacks. **a** Conventional strong PUF. **b** Our novel strong PUF

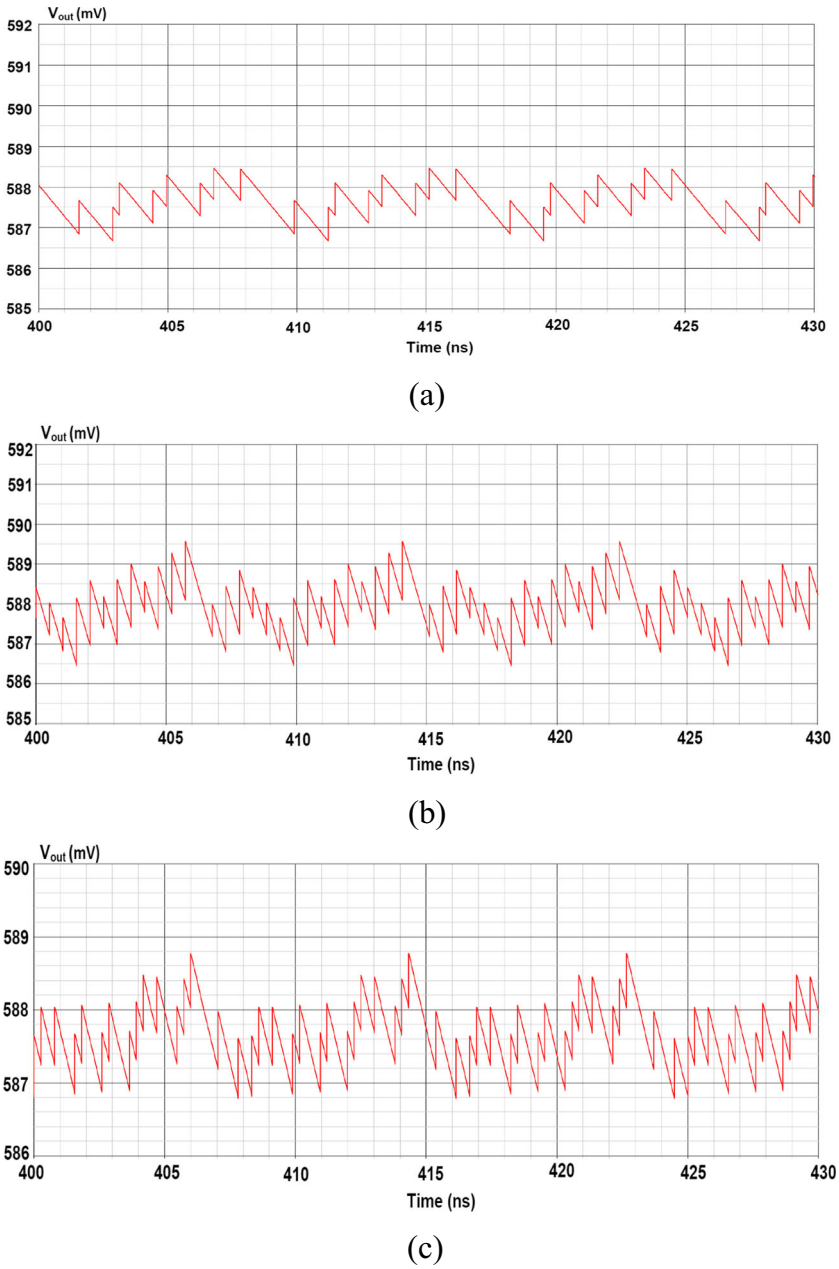


Fig. 3 Output voltage ripples of a 2:1 32-phase SC converter. **a** Case #1: Sequence of activation pattern (8 active phases): (7, 12, 13, 18, 20, 25, 27, 31). **b** Case #2: Sequence of activation pattern (16 active phases): (1, 2, 3, 4, 6, 8, 9, 14, 15, 16, 22, 23, 26, 28, 29, 30). **c** Case #3: Sequence of activation pattern (16 active phases): (2, 5, 6, 9, 10, 11, 14, 16, 19, 23, 24, 26, 28, 29, 30, 32)

each sub-phase [15]. Since the flying capacitor in each sub-phase is identically designed, the physical randomness of the flying capacitor induced by the fabrication process enables the multi-phase SC converter to be eligible for building PUF architectures.

3 Architecture Design

The architecture of a workload-aware multi-phase voltage regulator (WAMPVR)-based strong PUF primitive is devised in Fig. 4. Two identically designed 32-phase switched-capacitor (SC) voltage converters: $Block_1$ and $Block_2$ are utilized to build the strong PUF architecture. The output port of the j^{th}, $(j = 1, 2, ..., 32)$ phase of the SC converter in $Block_i$, $(i = 1, 2)$ connects with the switch $W_{i,j}$. Moreover, a 32-bit phase number generator (PNG) is utilized to control the activation behaviors of the switches $W_{i,1}$, $W_{i,2}$, ..., $W_{i,32}$ to determine the sequences of active phases that are used for building the strong PUF. For example, if only the switches $W_{i,2}$, $W_{i,5}$, $W_{i,12}$, and $W_{i,18}$ are turned on by the PNG, the output voltage ripples of *phase #2*, *phase #5*, *phase #12*, and *phase #18* of the SC converters are selected for generating the PUF response. Since a 32-bit PNG can generate $\binom{32}{0} + \binom{32}{1} + \binom{32}{2} + ... + \binom{32}{32} = 2^{32}$ different activation patterns, therefore, the total

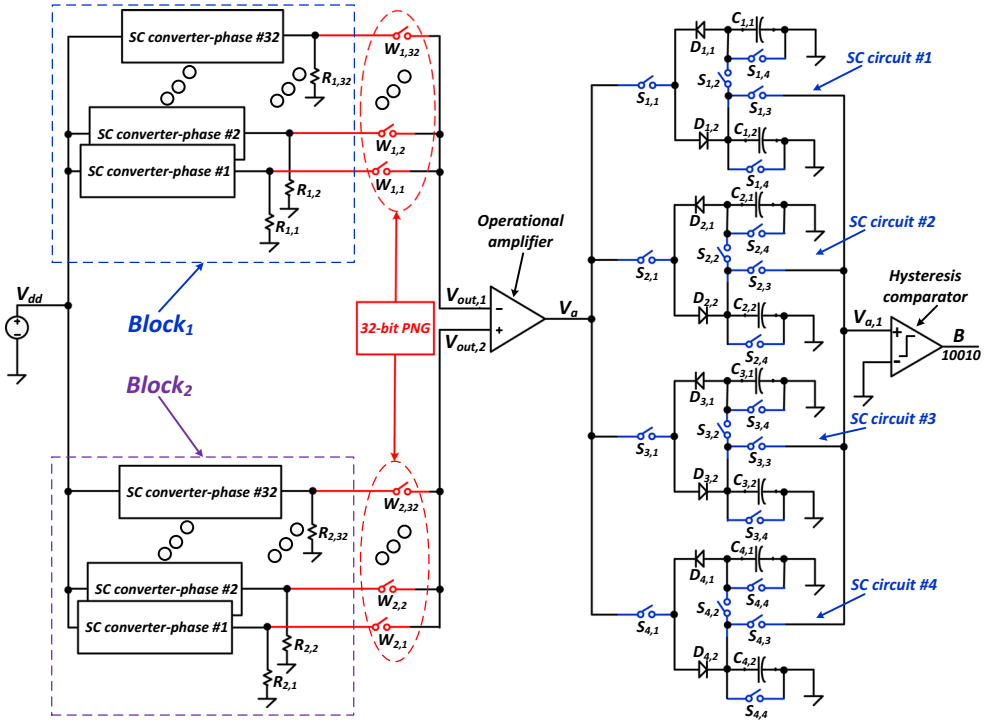


Fig. 4 Architecture of the WAMPVR-based strong PUF primitive (the total number X of phases in the original WAMPVR is 64, the resistors $R_{1,1}$, $R_{2,1}$, $R_{1,2}$, ..., and $R_{2,32}$ are designed with the same resistance R, and the capacitors $C_{1,1}$, $C_{1,2}$, $C_{2,1}$, ..., $C_{4,2}$ are also designed with the same capacitance C)

number of raw challenge-to-response pairs (CRPs) of the WAMPVR-based strong PUF primitive are 2^{32}.

As shown in Fig. 4, the mismatches of voltage ripple between $V_{out,1}$ and $V_{out,2}$ are magnified through employing an operational amplifier. Four pipelined SC circuits (*SC circuit #1*, ..., and *SC circuit #4*, as shown in Fig. 4) are utilized to convert the high-frequency voltage ripple mismatch V_a into the critical voltage $V_{a,1}$ for generating the secret authentication data B. Furthermore, each SC circuit has four independent working phases: *charging* phase, *charge-sharing* phase, *output* phase, and *discharging* phase. For example, as shown in Fig. 4, if *SC circuit #1* is in *charging* phase, the switch $S_{1,1}$ will be turned on. Then the positive component of V_a will charge the capacitor $C_{1,2}$ while the negative component of V_a will charge the capacitor $C_{1,1}$. Once the *charging* phase ends, the switch $S_{1,1}$ will be turned off while the switch $S_{1,2}$ will be activated to balance the charge of the capacitors $C_{1,1}$ and $C_{1,2}$. After the *charge-sharing* phase, the *SC circuit #1* will output the sampled critical voltage $V_{a,1}$ to generate the binary authentication data B by activating the switch $S_{1,3}$. If the voltage $V_{a,1} \geq 0$ V, the authentication data B output logic value "1". Otherwise, $B = 0$. In the final stage (*discharging* phase), the residual charge in the capacitors $C_{1,1}$ and $C_{1,2}$ will be cleared to initialize the next data sampling through turning on the $S_{1,4}$ switches. The main intention of employing *discharging* phase is to break the correlation between the current data and the history data against machine-learning attacks. Please note that in each SC circuit, the behaviors of the switches $S_{h,1}$, $(h = 1, 2, 3, 4)$, $S_{h,2}$, $S_{h,3}$, and $S_{h,4}$ are mutually exclusive. Additionally, as shown in Fig. 4, there are two different kinds of diodes: back-biased diode $D_{h,1}$ and forward-biased diode $D_{h,2}$ exist in each SC circuit. The main role of these diodes is working as a non-linear transformation block to generate the non-linear output response B against machine-learning attacks, which will be fully discussed in Section 4.

4 Evaluation

4.1 Performance Evaluation

Two most significant metrics that are selected to evaluate the PUF characterization are the inter-Hamming distance (HD) and the intra-HD (reliability) [3, 16, 18]. Inter-HD measures the distinctness between two different PUF devices while intra-HD (reliability) represents the stability of a single PUF device under different temperatures and supply voltages.

In Fig. 4, assume the resistors $R_{1,1}$, $R_{2,1}$, $R_{1,2}$, ..., and $R_{2,32}$ are designed with a high resistance R to reduce the overall power consumption of the WAMPVR-based strong PUF primitive. As a result, under the same process variation, the mismatch rate of these resistors $R_{1,1}$, ..., and $R_{2,32}$ will be negligible as compared to the mismatch rate of the flying capacitors in the SC converters. Hence, in Fig. 4, the output voltage $V_{out,i,j}$ of the j^{th}, $(j = 1, 2, ..., 32)$ phase of the SC

converter in $Block_i$, $(i = 1, 2)$ can be denoted by a function F, as shown below

$$V_{out,i,j} = F\left(C^s_{i,j}, V_{dd}, T_c, t + (j-1)\frac{T_s}{32}\right) \quad (1)$$

where $C^s_{i,j}$ is the flying capacitance of the j^{th} phase of the SC converter in $Block_i$. V_{dd}, T_c, T_s, and t, respectively, are the supply voltage, the environmental temperature, the switching period of the SC converters, and the timing of the 1^{st} phase of the SC converters. Let us assume the supply voltage V_{dd} and the environmental temperature T_c are time-invariant. As a result, the critical parameters: $C^s_{i,j}$, V_{dd}, T_c, and t are mutually independent. Then the output voltage $V_{out,i,j}$ can be approximated as[1]

$$\begin{aligned} V_{out,i,j} &= F(C^s_{i,j}, V_{dd}, T_c, t + \left(j-1\right)\frac{T_s}{32}\Big) \\ &= F_1(C^s_{i,j}) \times F_2(V_{dd}) \times F_3(T_c) \times F_4\left(t + (j-1)\frac{T_s}{32}\right) \\ &\approx \left(\sum_{i_1=0}^{m_1} a_{i_1}(C_{i,j})^{i_1}\right) \times \left(\sum_{i_2=0}^{m_2} b_{i_2}(V_{dd})^{i_2}\right) \times \left(\sum_{i_3=0}^{m_3} c_{i_3}(T_c)^{i_3}\right) \\ &\quad \times \left(\frac{d_0}{2} + \sum_{i_4=1}^{m_4} d_{i_4} cos\left(\frac{2\pi i_4}{T_s}\left(t + (j-1)\frac{T_s}{32}\right)\right)\right. \\ &\quad \left. + \sum_{i_4=1}^{m_4} e_{i_4} sin\left(\frac{2\pi i_4}{T_s}\left(t + (j-1)\frac{T_s}{32}\right)\right)\right) \end{aligned} \quad (2)$$

where $F_1(C^s_{i,j})$, $F_2(V_{dd})$, $F_3(T_c)$, and $F_4\left(t + (j-1)\frac{T_s}{32}\right)$, respectively, are the voltage components of $V_{out,i,j}$ that are determined by $C^s_{i,j}$, V_{dd}, T_c, and $t + (j-1)\frac{T_s}{32}$. $\sum_{i_1=0}^{m_1} a_{i_1}(C_{i,j})^{i_1}$, $\sum_{i_2=0}^{m_2} b_{i_2}(V_{dd})^{i_2}$, and $\sum_{i_3=0}^{m_3} c_{i_3}(T_c)^{i_3}$ are the approximated polynomial expansions of $F_1(C^s_{i,j})$, $F_2(V_{dd})$, and $F_3(T_c)$, respectively. $a_{i_1}, (i_1 = 0, 1, ..., m_1)$, $b_{i_2}, (i_2 = 0, 1, ..., m_2)$, and $c_{i_3}, (i_3 = 0, 1, ..., m_3)$, respectively, are the coefficients of $(C_{i,j})^{i_1}$, $(V_{dd})^{i_2}$, and $(T_c)^{i_3}$. m_1, m_2, and m_3 are the degrees of the approximated polynomials of $F_1(C^s_{i,j})$, $F_2(V_{dd})$, and $F_3(T_c)$, respectively. $d_0, d_1, ..., d_{m_4}, e_1, e_2, ..., e_{m_4}$ (m_4) are the coefficients (degree) of the approximated Fourier series of $F_4(t + (j-1)\frac{T_s}{32})$. If the supply voltage V_{dd}, the environmental temperature T_c , and the timing t are fixed, through matching the relationship curve between the capacitance $C^s_{i,j}$ and the output voltage $V_{out,i,j}$, the coefficients a_0, a_1, ... and the degree m_1 for $F_1(C^s_{i,j})$ can be unriddled. The coefficients and the degrees of $F_2(V_{dd})$, $F_3(T_c)$, and $F_4\left(t + (j-1)\frac{T_s}{32}\right)$ can also be estimated in a similar way.

Once the complete expression of the output voltage $V_{out,i,j}$ is obtained, the following step is to model the mismatches of output voltage ripple between $Block_1$ and $Block_2$ in Fig. 4. Assume the 32-bit PNG in Fig. 4 generates the 32-bit binary data $W = (w_1, w_2, ..., w_{32})_2$ to select a certain number of active phases of the SC converters for building a strong PUF for authentication by controlling the activation patterns of the corresponding switches.[2] As a result, by using the Kirchhoff's law, the voltages $V_{out,1}$ and $V_{out,2}$ in Fig. 4 can, respectively, be derived as

$$\begin{aligned} V_{out,1} &= \frac{\sum_{j=1}^{32} w_j V_{out,1,j}}{R} \times \frac{R}{\sum_{j=1}^{32} w_j} \\ &= \frac{\sum_{j=1}^{32} w_j V_{out,1,j}}{\sum_{j=1}^{32} w_j}, \end{aligned} \quad (3)$$

$$\begin{aligned} V_{out,2} &= \frac{\sum_{j=1}^{32} w_j V_{out,2,j}}{R} \times \frac{R}{\sum_{j=1}^{32} w_j} \\ &= \frac{\sum_{j=1}^{32} w_j V_{out,2,j}}{\sum_{j=1}^{32} w_j}. \end{aligned} \quad (4)$$

Then the voltage ripple mismatch V_a in Fig. 4 is

$$V_a = A_v(V_{out,2} - V_{out,1}) = A_v \frac{\sum_{j=1}^{32} w_j (V_{out,2,j} - V_{out,1,j})}{\sum_{j=1}^{32} w_j} \quad (5)$$

where A_v is the differential gain of the operational amplifier.

For the WAMPVR-based strong PUF primitive in Fig. 4, assume the switching period of the SC circuits is designed equal to four times of the switching period of the SC converters and the pulse width of all the switches $S_{1,1}$, $S_{1,2}$, ..., $S_{4,4}$ in SC circuits is 25%. If *SC circuit #1* is in *charging* phase, the switch $S_{1,1}$ is in on-state. The voltages V_a^* and V_a^{**} of the capacitors $C_{1,1}$ and $C_{1,2}$ in Fig. 4, respectively, are

$$V_a^* = \begin{cases} V_a - V_b & , V_a \geq V_b \\ 0 & , V_a < V_b, \end{cases} \quad (6)$$

$$V_a^{**} = \begin{cases} V_a + V_b & , V_a \leq -V_b \\ 0 & , V_a > -V_b \end{cases} \quad (7)$$

where V_b is the forward-biased threshold voltage of the diodes $D_{1,1}$ and $D_{1,2}$ in Fig. 4. When *SC circuit #1* enters into *output* phase, since the capacitors $C_{1,1}$ and $C_{1,2}$ are designed with the same capacitance C, the critical voltage $V_{c,1}$ in Fig. 4 can be denoted as

$$\begin{aligned} V_{a,1} &= \frac{\int_t^{t+T_s} C_{1,1}\frac{dV_a^*}{dt}dt + \int_t^{t+T_s} C_{1,2}\frac{dV_a^{**}}{dt}dt}{C_{1,2} + C_{1,2}} \\ &= \frac{\int_t^{t+T_s}\left(\frac{dV_a^*}{dt} + \frac{dV_a^{**}}{dt}\right)dt}{2}. \end{aligned} \quad (8)$$

[1] As demonstrated in Fig. 3, the output voltage of an SC converter is a periodical signal. Therefore, the voltage component of $V_{out,i,j}$ related with the timing t can be unfolded with Fourier series.

[2] w_1, w_2, ..., w_{32} control the activation behaviors of the switches $W_{i,1}$, $W_{i,2}$, ... $W_{i,32}$, respectively. If $w_j = 1$, the switches $W_{1,j}$ and $W_{2,j}$ are turned on, and vice versa.

Therefore, if the critical voltage $V_{a,1} \geq 0$ V, the output binary data $B = 1$. Otherwise, $B = 0$.

Assume N number of WAMPVRs are utilized for building a strong PUF primitive to generate the N-bit binary authentication data $\overline{B}$. As a result, if K strong PUF primitives are selected for evaluating the uniqueness, the inter-HD E is written as [16]

$$E = \frac{2}{K(K-1)} \sum_{k_1=1}^{K-1} \sum_{k2=k_1+1}^{K} \frac{\overline{B}_{k_1} \oplus \overline{B}_{k_2}}{N} \times 100\% \tag{9}$$

where $\overline{B}_{k_1}, (k_1 = 1, 2, ..., K-1)$ and $\overline{B}_{k_2}, (k_2 = k_1 + 1, ..., K)$, respectively, are the N-bit binary authentication data generated by the k_1^{th} and k_2^{th} strong PUF primitives.

Similarly, for a single PUF primitive, if M number of different environmental settings are considered, the reliability of the strong PUF primitive G can be expressed as [16]

$$G = \left(1 - \frac{1}{M} \sum_{l=1}^{M} \frac{\overline{B}_0^* \oplus \overline{B}_l^*}{N}\right) \times 100\% \tag{10}$$

where $\overline{B}_0^*$ and $\overline{B}_l^*$ are the N-bit binary authentication data generated by the single PUF primitive under the ideal and $l^{th}, (l = 1, 2, ..., M)$ environmental setting, respectively.

All of the aforementioned parameters in the mathematical model of the designed WAMPVR-based strong PUF primitive are extracted from the 130 nm CMOS technology kits in Cadence. As shown in Fig. 5a, by applying the Monte Carlo simulation into the aforementioned mathematical model, the inter-HD E of the WAMPVR-based strong PUF primitive is about 51.3% (L_g =130 nm). Furthermore, if the scaling of CMOS technology is considered, through utilizing the mismatch rates of capacitors under different CMOS technologies from [23], the inter-HD E of the technology-scaled WAMPVR-based strong PUF primitive can also be predicted. As shown in Fig. 5a, when the CMOS technology is scaled from 130 nm to 14 nm, the inter-HD E is improved from 51.3% to 50.1%. That indicates a larger capacitance mismatch rate induced by a shorter gate length enables the WAMPVR-based strong PUF primitive to achieve a better uniqueness. Additionally, the reliability G of the designed WAMPVR-based strong PUF primitive is assessed in Fig. 5b. The ideal environmental setting for the strong PUF primitive is: the ambient temperature T_c =27 °C and the supply voltage V_{dd} =2.4 V. As shown in Fig. 5b, the worst reliability of the designed WAMPVR-based strong PUF primitive is 98.5% when V_{dd} =2.9 V.

4.2 Security Against Side-Channel Attacks

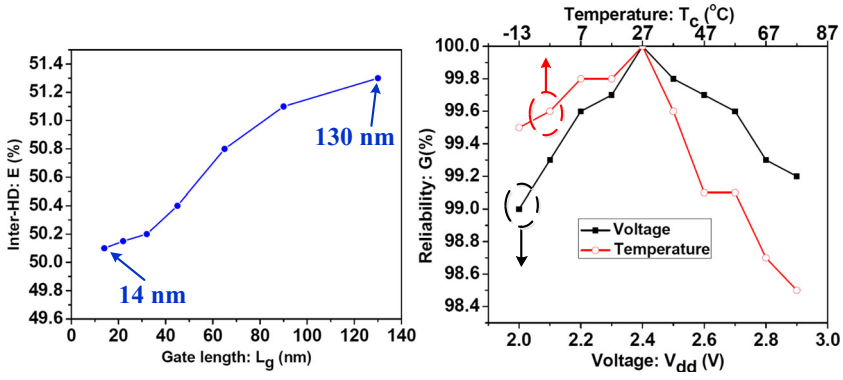
4.2.1 Side-Channel Leakage Analysis

If an X-phase (assume X is even) WAMPVR is utilized for devising a strong PUF architecture, the number of phases in $Block_1$ and $Block_2$ in Fig. 4 is $X/2$. Since all the phases in $Block_1$ and $Block_2$ are active all the time, the input power of the WAMPVR-based strong PUF primitive is a constant within a switching period T_s regardless the variations of process, voltage, and temperature (PVT). However, if the mismatches of the flying capacitors in the SC converters induced by the random fabrication process are considered, the total input power P_{in} of the WAMPVR-based strong PUF primitive within a switching period T_s can be expressed as

$$P_{in} = \sum_{i=1}^{2} \sum_{j=1}^{X/2} C_{i,j}^{s} f_s V_{dd}^2 \tag{11}$$

where f_s is the switching frequency of the SC converters.

Since the attacker may leak the mismatches of the flying capacitors in the SC converters through analyzing the input power P_{in}, the absolute value r of correlation coefficient between the input power P_{in} and the capacitance mismatch $\Delta C = C_{2,j}^{s} - C_{1,j}^{s}$ is studied against side-channel attacks. As shown in Fig. 6, the correlation coefficient between P_{in} and ΔC is about 0.0037 when the phase number X = 64, which indicates a good robustness against side-channel attacks. Moreover, if the phase number X increases, the



(a) (b)

Fig. 5 Performance evaluation for the designed strong PUF primitive. **a** Inter-HD E versus gate length L_g (K = 100 and N = 32). **b** Reliability G versus supply voltage V_{dd} and environmental temperature T_c (M = 50 and N = 32)

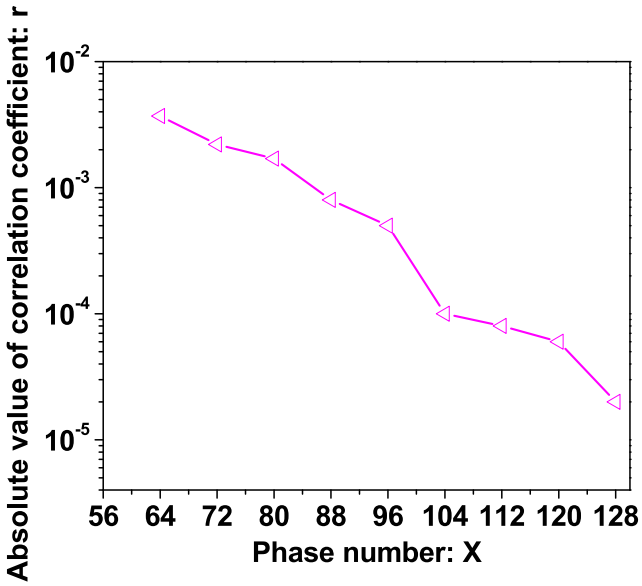


Fig. 6 Absolute value r of correlation coefficient between P_{in} and ΔC versus phase number X against side-channel attacks

correlation coefficient between P_{in} and ΔC will be further reduced against side-channel attacks.

4.2.2 Implementation of Side-Channel Attacks

The main intention of implementing side-channel attacks on the WAMPVR-based strong PUF primitive is unriddling the output response B by analyzing the critical side-channel leakage. If the input power P_{in} of the proposed strong PUF device is tailored as the critical side-channel leakage, the relationship between the input power P_{in} and the output response B needs to be studied when side-channel attacks are executed. Since the random fabrication process and circuit noise conform to normal distributions [16, 22], if the variations of PVT are considered, the input power P_{in} can be further derived as

$$\begin{aligned} P_{in} &= \sum_{i=1}^{2}\sum_{j=1}^{X/2} C_{i,j}^{s} f_s V_{dd}^2 \\ &= \frac{1}{\sqrt{2\pi X}\sigma_c} exp\left(-\frac{(\sum_{i=1}^{2}\sum_{j=1}^{X/2} C_{i,j}^{s} - X\mu_c)^2}{2X\sigma_c^2}\right) \\ &\quad \times \frac{1}{\sqrt{2\pi}\sigma_f} exp\left(-\frac{(f_s-\mu_f)^2}{2\sigma_f^2}\right) \\ &\quad \times \left(\frac{1}{\sqrt{2\pi}\sigma_v} exp\left(-\frac{(V_{dd}-\mu_v)^2}{2\sigma_v^2}\right)\right)^2 \end{aligned} \tag{12}$$

where μ_c (σ_c), μ_f (σ_f), and μ_v (σ_v) are the means (standard deviations) of the flying capacitance, switching frequency, and supply voltage of the proposed strong PUF device, respectively.

So as to model the relationship between the input power P_{in} and the output response B, let us define a function $F^*(P_{in})$ and approximate the function $F^*(P_{in})$ with a polynomial expansion $F^{**}(P_{in})$ as shown below

$$F^*(P_{in}) \approx \sum_{k=0}^{K^*} f_k^* \times (P_{in})^k = F^{**}(P_{in}) \tag{13}$$

where K^* is the degree of the approximated polynomial and f_k^* is the coefficient of $(P_{in})^k$. Assume that Z is the number of input power and output response pairs: ($P_{in,1}$, B_1), ($P_{in,2}$, B_2), ..., and ($P_{in,Z}$, B_Z) of the proposed strong PUF primitive are selected for analysis, then the matching error ΔL between the input power P_{in} and the output response B with the polynomial expansion $F^{**}(P_{in})$ can be expressed as

$$\Delta L = \sum_{z=1}^{Z}\left(\sum_{k=0}^{K^*} f_k^* \times (P_{in,z})^k - B_z\right)^2 \tag{14}$$

By minimizing the matching error ΔL with

$$\frac{\partial \Delta L}{\partial f_k^*} = \left(2\sum_{z=1}^{Z}\left(\sum_{k=0}^{K^*} f_k^* \times (P_{in,z})^k - B_z\right)\right) \times \sum_{k=0}^{K^*} (P_{in,z})^k = 0, \tag{15}$$

the optimal K^*, f_0^*, f_1^*, ..., $f_{K^*}^*$ can be determined.

The Z number of input power and output response pairs: ($P_{in,1}$, B_1), ($P_{in,2}$, B_2), ..., and ($P_{in,z}$, B_z) of the WAMPVR-based strong PUF primitive with the 130 nm CMOS technology under the standard deviations σ_f and σ_v is simulated in Cadence. As shown in Fig. 7, if power attacks are implemented on the WAMPVR-based strong PUF primitive by exploring the input power P_{in} as the critical side-channel leakage, the maximum prediction accuracy of the power attacks is about 0.52 even if 1 million input power and output response pairs are analyzed. That indicates the proposed strong PUF primitive is adequately secure against the advanced power attacks.

4.3 Security Against Machine-learning (ML) Attacks

4.3.1 Non-Linearity Analysis

The degree of the non-linearity between the input challenges and the output responses is a critical parameter that affects the robustness of a strong PUF against machine-learning (ML) attacks [1]. For the WAMPVR-based strong PUF primitive in Fig. 4, the relationship between the average capacitance mismatch Q and the critical voltage $V_{a,1}$ is

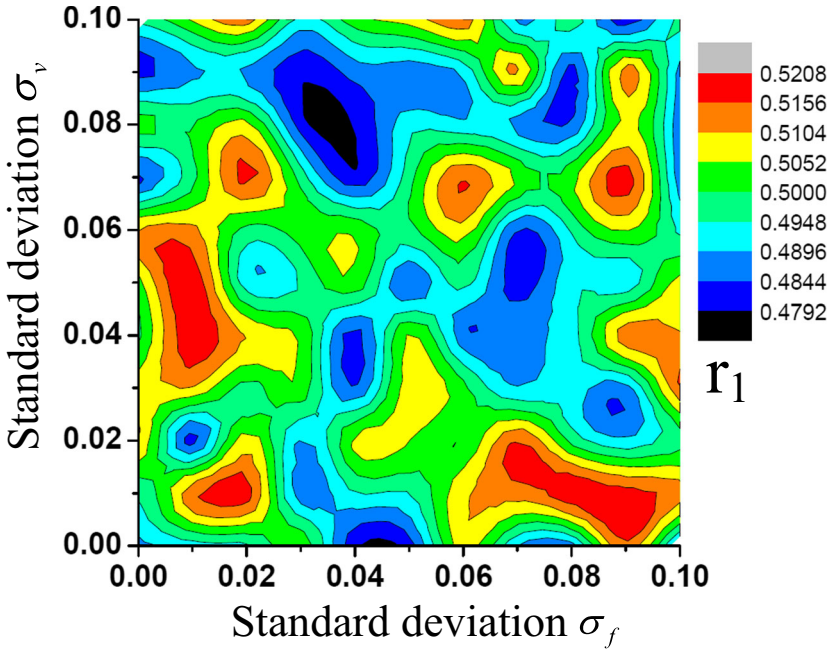


Fig. 7 Prediction accuracy r_1 of power attacks versus standard deviations σ_f and σ_v after analyzing 1 million input power and output response pairs (The colors and contours represent the variation values of the prediction accuracy r_1. Since the variation values of the prediction accuracy r_1 are around 0.5 and random, that reflects power attacks are unable to leak critical information on the proposed PUF)

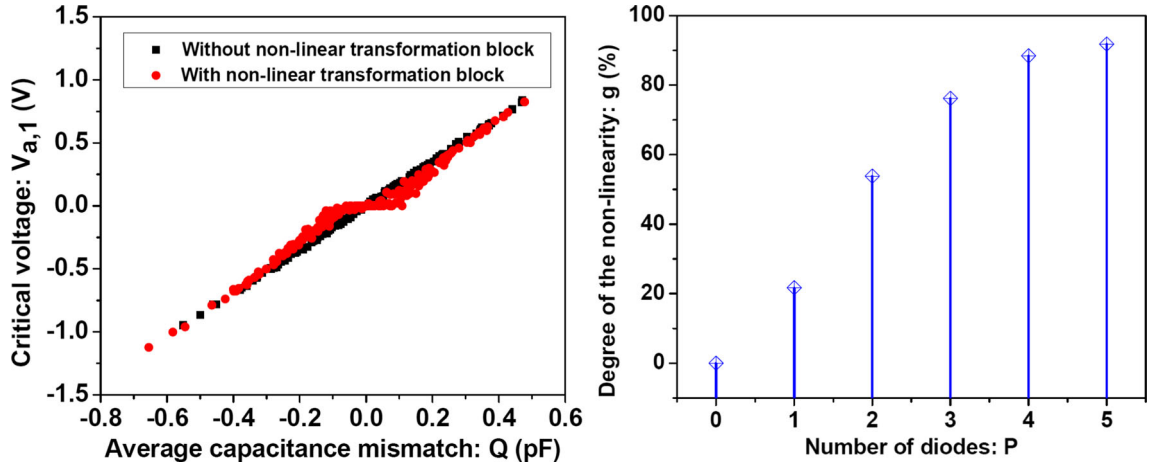
studied. The definition of the average capacitance mismatch Q in Fig. 4 is

$$Q = \sum_{j=1}^{32} w_j (C^s_{2,j} - C^s_{1,j}). \tag{16}$$

The non-linear relationship between Q and $V_{a,1}$ can be observed in Fig. 8a when the non-linear transformation block that is consist of diodes $D_{1,1}$, $D_{1,2}$, $D_{2,1}$, ..., $D_{4,2}$ (as shown in Fig. 4) is enabled. By contrast, a strong linear relationship exists between Q and $V_{a,1}$ if the non-linear transformation block is removed.

If Y number of different Q values: Q_1, Q_2, ..., Q_Y are studied, assume the corresponding value of the critical voltage $V_{a,1}$ is: $V_{a,1,1}$, $V_{a,2,1}$, ..., $V_{a,2,Y}$ ($V'_{a,1,1}$, $V'_{a,2,1}$, ..., $V'_{a,2,Y}$) for the strong PUF with (without) the non-linear transformation block. As a result, the degree g of the non-linearity of the designed WAMPVR-based strong PUF primitive can be estimated as [17]

$$g = \frac{\frac{1}{2Y}\sum_{j_1=1}^{Y}(V_{a,1,j_1} - V'_{a,1,j_1})^2}{\left(\frac{\sum_{j_1=1}^{Y} V'_{a,1,j_1}}{Y}\right)^2} \times 100\%. \tag{17}$$



(a) (b)

Fig. 8 **a** Critical voltage $V_{a,1}$ versus average capacitance mismatch Q against ML attacks. **b** Number of diodes P between the switch $S_{h,1}$ and the capacitor $C_{h,x}$ in Fig. 4 versus degree g of the non-linearity of the WAMPVR-based strong PUF primitive

To enhance the degree of the non-linearity of the proposed strong PUF device, we can increase the number of diodes in the non-linear transformation block. For instance, in Fig. 4, only one diode $D_{h,x}$, ($h = 1, 2, 3, 4$ and $x = 1, 2$) exists between the switch $S_{h,1}$ and the capacitor $C_{h,x}$. If larger number of diodes can be inserted, the degree g of the non-linearity of the WAMPVR-based strong PUF primitive will be improved ($g = 91.79\%$ when $P = 5$), as shown in Fig. 8b.

4.3.2 Linear Regression (LR) Attacks

Linear regression (LR) algorithm [17, 24] is a kind of popular machine-learning (ML) algorithms that can be explored to uncover the confidential information of a strong PUF device. For the WAMPVR-based strong PUF primitive as shown in Fig. 4, there is a 32-bit phase number generator (PNG) $W = (w_1, w_2, ..., w_{32})_2$ that is working as the input challenge. Accordingly, the main intention of performing ML attacks on the proposed strong PUF primitive is estimating the relationship between the input challenge W and output response B. When the LR algorithm is considered for training the challenge-to-response pairs (CRPs), the predicted output response B^* of the proposed strong PUF device under the input challenge W can be written as

$$B^* = \sum_{j=1}^{32} w_j \theta_j + \theta_0 \tag{18}$$

where θ_0, θ_1, ..., θ_{32} are the linear coefficients of the LR algorithm.

If n number of CRPs: (W_1, B_1), (W_2, B_2), ..., and (W_n, B_n) are selected as the training data sets, by considering the least-squares fit rule, the cost function $S(\theta)$ of the LR algorithm can be obtained as

$$S(\theta) = \frac{1}{2n} \sum_{j_1=1}^{n} \left(\sum_{j=1}^{32} w_{j,j_1} \theta_j + \theta_0 - B_{j_1} \right)^2 \tag{19}$$

where w_{j,j_1} is the j^{th} bit of the j_1^{th} input challenge W_{j_1}. After repeating the gradient descent algorithm as shown below

$$\begin{aligned} \theta_j &:= \theta_j - \beta \frac{\partial S(\theta)}{\partial \theta_j} \\ &= \theta_j - \beta \frac{1}{n} \left(\sum_{j_1=1}^{n} \left(\sum_{j=1}^{32} w_{j,j_1} \theta_j + \theta_0 - B_{j_1} \right)^2 \right) \sum_{j=1}^{32} w_{j,j_1} \end{aligned} \tag{20}$$

where β is the learning coefficient of the LR algorithm, the critical parameters: θ_0, θ_1, ..., θ_{32} can be estimated.

Figure 9 shows the variations of the cost function value $S(\theta)$ and prediction accuracy r_2 of the WAMPVR-based strong PUF primitive with n number of CRPs. Even if 100,000 number of CRPs are used for training with the LR algorithm, the variation of the cost function $S(\theta)$ is negligible. Furthermore, the maximum value of prediction accuracy r_2 of the LR algorithm is below 0.53 after enabling 100,000 number of training CRPs, as shown in Fig. 9. Consequently, the proposed strong PUF primitive is sufficiently robust against ML attacks.

5 Circuit Level Simulation

A WAMPVR-based strong PUF architecture is designed and simulated. The waveforms of the voltages $V_{out,1}$ and $V_{out,2}$ in Fig. 4 that contain the voltage ripple information are

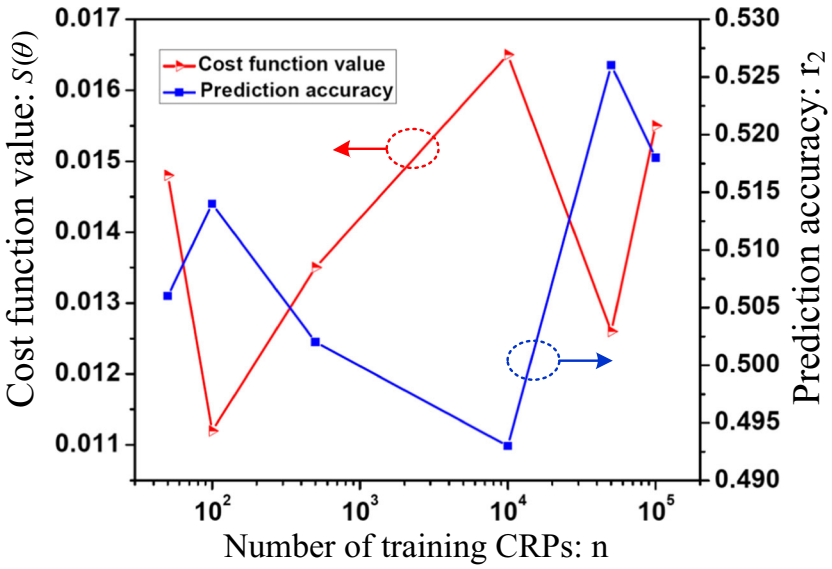


Fig. 9 Cost function value $S(\theta)$ and prediction accuracy r_2 versus number of training CRPs n for the WAMPVR-based strong PUF primitive under LR attacks (number of diodes $P = 3$)

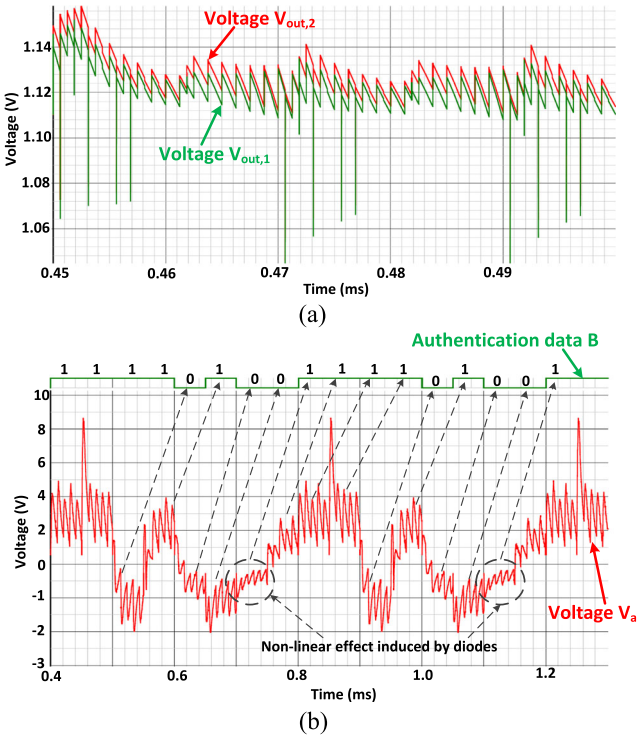


Fig. 10 Simulated waveforms of the WAMPVR-based stong PUF primitive ($X = 32$). **a** Voltages $V_{out,1}$ and $V_{out,2}$ versus time. **b** Voltage $V_{a,1}$ and binary authentication data B versus time

shown in Fig. 10a. By using Monte Carlo simulation, the mismatches of voltage ripple of $Block_1$ and $Block_2$ in Fig. 4 induced by the random mismatches of the flying capacitors in the SC converters can be observed in Fig. 10a obviously. Additionally, as shown in Fig. 10b, if the voltage V_a (as shown in Fig. 4) exhibits a high negative amplitude, the authentication data B (as shown in Fig. 4) output logic value "0". Moreover, the non-linear effect induced by the diodes can also be observed in Fig. 10b if the voltage V_a exhibits a small negative amplitude.

6 Conclusion

A novel strong PUF architecture is designed based on the on-chip workload-aware multi-phase voltage regulators (WAMPVRs). Through exploiting the physical randomness of the flying capacitors in the multi-phase switched-capacitor (SC) voltage converter, the strong PUF primitive we designed achieves a nearly 51.3% inter-HD and 98.5% reliability. Furthermore, in the WAMPVR-based strong PUF architecture we proposed, an approximated constant input power is achieved against side-channel attacks while a non-linear transformation block is utilized to add non-linearity against machine-learning attacks. As demonstrated in the results, for the designed strong PUF primitive, after enabling 1×10^6 (1×10^5) items of data to execute power (machine-learning) attacks, the prediction accuracy is about 0.52 (0.53). By contrast, the prediction accuracy is about 0.98 (0.999) when power (machine-learning) attacks are performed on the conventional PUF design under the assistance of 26×10^3 (39.2×10^3) items of data.

References

1. Alkatheiri MS, Zhuang Y (2017) Towards fast and accurate machine learning attacks of feed-forward arbiter PUFs. In: Proceedings of Dependable and Secure Computing, Taipei, Taiwan, pp 181–187
2. Gao Y, Ma H, Abbott D, Al-Sarawi SF (2017) PUF Sensor: Exploiting PUF unreliability for secure wireless sensing. IEEE Trans Circuits Syst Regul Pap 64(9):2532–2543
3. He Z, Wan M, Deng J, Bai C, Dai K (2018) A reliable strong PUF based on switched-capacitor circuit. IEEE Trans Very Large Scale Integr VLSI Syst 26(6):1073–1083
4. Khedkar G, Kudithipudi D, Rose GS (2015) Power profile obfuscation using nanoscale memristive devices to counter DPA attacks. IEEE Trans Nanotechnol 14(1):26–35
5. Levi I, Keren O, Fish A (2015) Data-dependent delays as a barrier against power attacks. IEEE Trans Circuits Syst Regul Pap 62(8):2069–2078
6. Liu Y, Jiang J, Ki WH (2017) A multiphase switched-capacitor DC-DC converter ring with fast transient response and small ripple. IEEE J Solid State Circuits 52(2):579–591
7. Liu Y, Jiang J, Ki WH, Yue CP, Sin SW, SP U, Martins RP (2015) 20.4 A 123-phase DC-DC converter-ring with fast-DVS for microprocessors. In: Proceedings of International Solid-State Circuits Conference (ISSCC), San Francisco, United States, pp 1–3
8. Luo Y, Cui A, Qu G, Li H (2016) A new countermeasure against scan-based side-channel sttacks. In: Proceedings of International Symposium on Circuits and Systems (ISCAS), Montreal, Canada, pp 1722–1725
9. Qu M, Chang Y (2016) Irradiation side-channel attack on cyptographic chip. In: Proceedings of International Conference on Integrated Circuits and Microsystems (ICICM), Chengdu, China, pp 41–45
10. Rührmair U, Sehnke F, Sölter J, Dror G, Devadas S, Schmidhuber J (2010) Modeling attacks on physical unclonable functions. In: Proceedings of conference on Computer and communications security (CCS), Chicago, Illinois, USA, pp 237–249
11. Rührmair U, Xu X, Sölter J, Mahmoud A, Majzoob M, Koushanfar F, Burleson W (2014) Efficient power and timing side channels for physical unclonable functions. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Busan, Korea, pp 476–492
12. Sahoo DP, Nguyen PH, Mukhopadhyay D, Chakraborty RS (2015) A case of lightweight PUF constructions: Cryptanalysis and machine learning attacks. IEEE Trans Comput Aided Des Integr Circuits Syst 34(8):1334–1343
13. Santiago L, Patil VC, Prado CB, Alves TAO, Marzulo LAJ, Franca FMG, Kundu S (2017) Realizing strong PUF from weak PUF via neural computing. In: Proceedings of Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Cambridge, United Kingdom, pp 1–6
14. Tanaka Y, Bian S, Hiromoto M, Sato T (2018) Coin flipping PUF: a novel PUF with improved resistance against machine learning attacks. IEEE Trans Circuits Syst Express Briefs 65(5):602–606

15. Uzun O, Köse S (2014) Converter-gating: a power efficient and secure on-chip power delivery system. IEEE J Emerging Sel Top Circuits Syst 4(2):169–179
16. Wan M, He Z, Han S, Dai K, Zou X (2015) An invasive-attack-resistant PUF based on switched-capacitor circuit. IEEE Trans Circuits Syst Regul Pap 62(8):2024–2034
17. Xu X, Rahmati A, Holcomb DE, Fu K, Burleson W (2015) Reliable physical unclonable functions using data retention voltage of SRAM cells. IEEE Trans Comput Aided Des Integr Circuits Syst 34(6):903–914
18. Yanambaka VP, Mohanty SP, Kougianos E (2018) Making use of manufacturing process variations: A dopingless transistor based-PUF for hardware-assisted security. IEEE Trans Semicond Manuf 31(2):285–294
19. Yao Y, Kim M, Li J, Markov IL, Koushanfar F (2013) ClockPUF: Physical unclonable functions based on clock networks. In: Proceedings of Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, pp 422–427
20. Yu W, Chen J (2018) Masked AES PUF: a new PUF against hybrid SCA/MLAs. IET Electron Lett 54(10):618–620
21. Yu W, Köse S (2016) A voltage regulator-assisted lightweight AES implementation against DPA attacks. IEEE Trans Circuits Syst Regul Pap 63(8):1152–1163
22. Yu W, Köse S (2017) Implications of noise insertion mechanisms of different countermeasures against side-channel attacks. In: Proceedings of International Symposium on Circuits and Systems (ISCAS), Baltimore, United States, pp 1–4
23. Yu W, Köse S (2017) A lightweight masked AES implementation for securing IoT against CPA attacks. IEEE Trans Circuits Syst Regul Pap 64(11):2934–2944
24. Zhou C, Parhi KK, Kim CH (2017) Secure and reliable XOR arbiter PUF design: An experimental study based on 1 trillion challenge response pair measurements. In: Proceedings of Design Automation Conference (DAC), Austin, Texas, pp 1–6

Weize Yu received the B.S. degree in electrical engineering from University of Electronic Science and Technology of China, Chengdu, in 2009, and the M.S. and Ph.D. degrees in electrical engineering from Chinese Academy of Sciences, Beijing, and University of South Florida, Florida, in 2012 and 2017, respectively. Currently, he is an Assistant Professor in the department of electrical and computer engineering at the Old Dominion University. Weize Yu is an Associate Editor of the Elsevier Microelectronics Journal. His current research interests are mainly focused on power management IC, hardware security, and Internet of things (IoT).

Yiming Wen received the B.S. degree in safety engineering from the Central South University, Changsha, China, in 2013, and the M.S. degree in electrical engineering from University of South Florida, Florida, in 2016. He is currently pursuing the Ph.D. degree with the Old Dominion University. His current research interests include on-chip power management and hardware security.

Selçuk Köse received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from the University of Rochester, Rochester, NY, in 2008 and 2012, respectively. He was with the VLSI Design Center of the Scientific and Technological Research Council, Ankara, Turkey, the Central Technology and Special Circuits Team in the enterprise microprocessor division of Intel Corporation, Santa Clara, CA, USA, and the RF, Analog, and Sensor Group, Freescale Semiconductor, Tempe, AZ, USA. He is currently an Assistant Professor with the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA. His current research interests include the analysis and design of high-performance integrated circuits, on-chip dc–dc converters, and hardware security. Prof. Köse has served on the Technical Program and Organization Committees of various conferences. He is a recipient of the NSF CAREER Award, the Cisco Research Award, the USF College of Engineering Outstanding Junior Researcher Award, and the USF Outstanding Faculty Award. He is an Associate Editor of the Journal of Circuits, Systems, and Computers and Microelectronics Journal.

Jia Chen received the B.S. degree from Southwest Jiaotong University, China, in 2009 and the M.S. degree from University of Electronic Science and Technology of China in 2012, both in electrical engineering. In 2016, she received the Ph.D. degree in electrical engineering from the University of Texas at Arlington, Arlington, TX, USA. She is currently a Postdoctoral Associate in the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN, USA. Her research interests include machine learning, IoT, data analytics, and signal processing.