Design and Evaluation of Fluctuating Power Logic to Mitigate Power Analysis at the Cell Level

Fan Zhang, Bolin Yang, *Student Member, IEEE*, Bojie Yang, Yiran Zhang, *Student Member, IEEE*, Xuanle Ren, Shivam Bhasin, *Member, IEEE*, and Kui Ren, *Fellow, IEEE*

***Abstract*—In this article, we design a novel cell-level power-analysis countermeasure, named fluctuating power logic (FPL), which diffuses the correlation between the real power consumption and the fixed data transitions by employing a *cascade voltage logic*. The countermeasure further acts as a cell-level V_{DD} randomizer, making it a strong candidate for implementing algorithmic countermeasure and exploiting its noise generation capabilities. This proposed scheme is illustrated by a standard flip-flop (FF). HSPICE-based simulation results show that the modified FF is resistant against power analysis (PA) at the cost of doubled power dissipation. Two illustrative case studies of PRESENT and AES substitutions have been explored. Furthermore, our proposal can be combined with other cell-level countermeasures against PA, such as wave dynamic differential logic. The resistance is evaluated by the correlation PA and the test vector leakage assessment. The new logic outperforms other counterparts in consideration of both security and cost, which renders it as a practical solution for resource-constrained systems. The proposed cell-level countermeasure can naturally mitigate other side-channel analysis such as electromagnetic analysis.**

***Index Terms*—Dual-rail precharge (DRP), flip-flop (FF), fluctuating power logic (FPL), side-channel analysis, wave dynamic differential logic (WDDL).**

I. Introduction

CRYPTOGRAPHIC technologies and secure implementations of cryptographic algorithms have been developed and widely used in electronic banking, virtual private networks, online payment, and so on. The Internet of Things (IoT) and cyber-physical systems (CPS) are the primary contributors to the revolution of the way that humans and intelligent systems interact. With the rapid development, the security and privacy of sensitive information handled by such systems are emerging as a serious concern [1], [2]. While these technologies offer a lot of new possibilities, the increasing complexities of hardware and software also increase the vulnerability to security attacks.

One severe security vulnerability of embedded devices is side-channel analysis (SCA) [3], which aims to extract the secrets using unintentional physical leakages from underlying logic elements. Power analysis (PA) is one of the most classical attack approaches, which includes simple PA (SPA), differential PA (DPA) [3], correlation PA (CPA) [4], and more. These attacks exploit the fact that the power dissipation of the implemented cryptographic modules inherently correlates to their switching operations.

The CMOS is the basic building block of modern circuits. Its dynamic power consumption is caused by charging and discharging the capacitive loads when internal and output nodes perform transitions, which accounts for a large portion of the total power in the circuits [5], [6]. Variant data transitions ($0 \rightarrow 1$ and $1 \rightarrow 0$) consume more distinguishable power than invariant ones ($0 \rightarrow 0$ and $1 \rightarrow 1$). Such power activity is consequently associated with the key-dependent variables being processed by the algorithm in a noninvasive manner [7]. The dependency can be approximately described by a power model, such as the Hamming weight (HW) or the Hamming distance (HD) model.

Since the PA brings severe security threats to modern circuits, effective SCA countermeasures are in high demand. The two mainstream SCA countermeasures are hiding and masking [8]. Both techniques make it difficult to deduce the key-dependent data from observable power dissipations,

Manuscript received March 24, 2020; revised July 23, 2020; accepted August 24, 2020. Date of publication September 14, 2020; date of current version May 20, 2021. This work was supported in part by the Open Fund of State Key Laboratory of Cryptology; in part by the Fundamental Research Funds for the Central Universities under Grant 2020QNA5021; in part by the Alibaba-Zhejiang University Joint Institute of Frontier Technologies; in part by the Zhejiang Key Research and Development Plan under Grant 2019C03133; in part by the Major Scientific Research Project of Zhejiang Lab under Grant 2018FD0ZX01; in part by the Young Elite Scientists Sponsorship Program by CAST under Grant 17-JCJQ-QT-045; in part by the National Natural Science Foundation of China under Grant 61772236 and Grant 62072398; in part by the Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang under Grant 2018R01005; and in part by the Research Institute of Cyberspace Governance in Zhejiang University. This article was recommended by Associate Editor R. Gupta. *(Corresponding author: Bolin Yang.)*

Fan Zhang is with the School of Cyber Science and Technology, College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China, also with the State Key Laboratory of Cryptology, Beijing 100878, China, and also with the Alibaba-Zhejiang University Joint Institute of Frontier Technologies, Zhejiang University, Hangzhou 310027, China (e-mail: fanzhang@zju.edu.cn).

Bojie Yang and Kui Ren are with the School of Cyber Science and Technology, College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China.

Bolin Yang and Yiran Zhang are with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: yangbolin@zju.edu.cn).

Xuanle Ren is with Alibaba Group, Hangzhou 311121, China.

Shivam Bhasin is with Temasek Laboratories, Nanyang Technological University, Singapore 637371.

Digital Object Identifier 10.1109/TCAD.2020.3023900

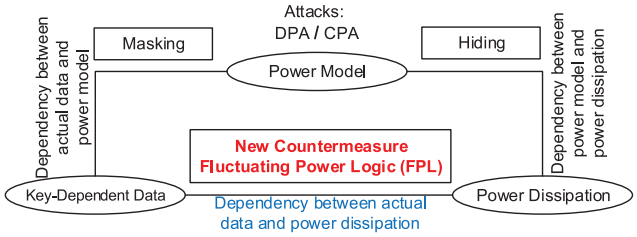


Fig. 1. Concept of the proposed FPL countermeasure.

specifically, in two distinct fashions as shown in Fig. 1. Examples of hiding countermeasures are noise generators [9], clock randomizers [9], and dual-rail precharge (DRP) logics, such as the sense-amplifier-based logic (SABL) [10] at the transistor level, and the wave dynamic differential logic (WDDL) [10] or the balanced cell-based dual-rail logic (BCDL) [11] at the gate level. The first two countermeasures have limited impacts on the attacking difficulty and can be eventually exploited. BCDL eliminates the early propagation effect (EPE) from WDDL by synchronizing pairs of inputs in a compound N-input gate. However, the logic styles, such as SABL, WDDL, and BCDL require a very strict complementary capacitive balance, making them quite difficult to implement in practice. Further, some researchers have explored quasi-delay insensitive (QDI) asynchronous circuits coupled with 1-to-N encoding to achieve side-channel resistance [12].

Masking [13] is an algorithm-level countermeasure which attempts to de-correlate the dependency between the actual data and the power model. Even with enough knowledge of power models, the adversary still cannot extract the secret because the key-dependent variables are actually masked with random and unknown values. Masking is one of the most widely studied countermeasures in the research community and comes with a formal proof of security [14].

In this article, we deal with the noise generation problem at the transistor-level. The key motivation of this article is to pursue a new type of countermeasure which, at the cell level, can remove the dependency between the actual data and the physical power dissipation, regardless of whether the power model is completely known to the adversary or not. Different from the well-known masking scheme, the proposed logic provides the protection at the underlying cell level. Unlike WDDL and other hiding schemes, the power dissipation will allow adjustable fluctuation independently with the data transitions, instead of maintaining a constant value. The proposal is designed to be efficient in terms of power consumption, circuit area, and manufacturing cost, which can be used in low-cost and high-security endpoints of IoT. The logic style is called fluctuating power logic (FPL). The initial idea was introduced but not elaborated in [15] and [16]. We extended our preliminary concept [16] by evaluating its combination with WDDL. FPL cells can also be used to implement masked algorithms to further elevate their security levels.

A. Related Work

It has been established that the major power consumption of a digital circuit comes from the clock distribution network and flip-flops (FFs) (estimated 30%–60%) [17]. FFs are also the normal target of SCA due to the synchronized power consumption. At the cell level, hiding countermeasures adopt the form of secure logic styles with constant power consumption, most of which are typically implemented as DRP circuits [10], [18]–[20]. The combination of the dual-rail (DR) logic and the precharge logic makes up the DRP circuits. All logic signals of DRP circuits are encoded on complementary rails. The logic values precharge and propagate at two interleaved phases, i.e., *Precharge* and *Evaluation* phases. During the precharge phase, the values on the complementary rails are set to the precharge value. When the circuit is switched to the evaluation phase, the values on the complementary rails are set to valid logic values, depending on the input logic values and the functionalities of the DRP cells. This behavior forms the basis of a DPA-resistant implementation, whose power consumption is constant in each clock cycle, regardless of the data being processed.

DRP logic styles generally lead to increased area overhead of more than 100% as compared to the standard-cell (SC)-based circuits. Due to the fact that the power consumption of a logic cell is proportional to the capacitive loads at the output, an essential necessity for constant power dissipations is to balance the capacitive loads at both the complementary output and the internal nodes of a DRP cell. This requirement also applies to the connecting routing. However, since this ideal and perfect balance is difficult to achieve in practice, DRP logic styles remain vulnerable to side-channel attacks.

Alternative hiding countermeasures like noise generators have also been widely studied in prior works. Güneysu and Moradi [9] proposed several generic designs for noise generators exploiting shift registers, block RAM write conflicts, clock randomization, etc. However, all these noise generators act independently to the sensitive circuits. Thus, advanced filtering and signal processing methods can be deployed to remove such added noise. In [21], on-chip voltage regulators were used to de-correlate the power consumption of sensitive activities from that of the load. Random voltage scaling was proposed as a side-channel countermeasure [22] to reduce the correlation between *VDD* and the power model. A thorough security evaluation of such *VDD* randomizer was recently published in [23]. Such randomization of voltage can be regarded as a sound noise generator which can be further exploited to strengthen mathematical countermeasures like masking. In summary, the aforementioned approaches mainly aim at FPGA scenarios, where the modulated supply voltage is isolated from the protected circuits and the universal power models still suit for them.

B. Contribution

Our contributions in this article are listed below.

1) A novel cell-level logic, named as FPL, is proposed for randomly fluctuating the power consumption of fixed data transitions. Since the conventional power model cannot reflect the actual dissipation, FPL is therefore considered to be SCA-resistant.
2) A compensatory unit (CU) is appended to enhance the logic to be DPA resistant by making the average power

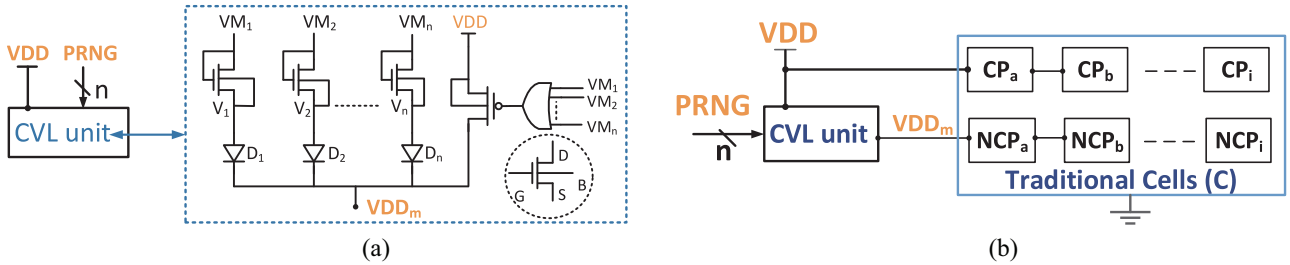


Fig. 2. Schematic of FPL and CVL unit. (a) Schematic of CVL unit. (b) Design of FPL logic with CVL unit.

consumption of variant and invariant data transitions indistinguishable.

3) The proposed logic is analyzed for side-channel security by practical CPA and test vector leakage assessment (TVLA) on PRESENT/AES-SBox modules implemented with FPL.
4) The FPL-based implementation is compared with the SC-based and the WDDL-based ones, to further verify our proposed scheme in terms of security, area, power, etc.
5) We show that FPL can also be used to improve WDDL-based implementations to reduce the dependency on capacitance bias in WDDL.

C. Organization

The remainder of this article is organized as follows. The FPL scheme and its secure FF implementation are described in Sections II and III, respectively. The transistor-level experiment results of FPL-FF and corresponding theoretical evaluations are presented in Section IV. In Section V, two illustrative case studies of PRESENT-SBox and AES-SBox modules are given. In addition, WDDL-based encryption modules are also implemented to compare with our proposed logic. Section VI reports the analysis and optimization for FPL logic, and gives advices for combining it with other cell-level countermeasures. Future works and conclusions are drawn in Sections VII and VIII, respectively. Additional information is provided in appendixes.

II. Proposed Logic

In this section, after thoroughly investigating the operational principles of cell-level-based hiding countermeasures and analyzing their merits and demerits, a novel SCA-resistant cell-level logic is proposed and implemented with limited physical resources. This scheme is based on a cascade voltage logic (CVL) and further enhanced with a CU.

A. Basic CVL Unit

Fig. 2(a) shows the schematic of the CVL. The CVL unit mainly consists of four components: 1) n nMOS; 2) n diodes (D_i); 3) one pMOS; and 4) one "$n-$input" OR-gate. n denotes the number of nMOS transistors or diodes. A larger value of n indicates that more randomness is introduced to the circuit, which is considered as more secure in our proposal. The function of CVL unit is to output a hybrid voltage (VDD_m) to substitute the original source voltage (VDD) with a random voltage drop (V_{dp}): $VDD_m = VDD - V_{dp}$. In this unit, the drain and gate terminals of every parallel nMOS are directly driven by randomized control signals VM_i ($1 \leq i \leq n$), which are generated by the pseudo-random number generator (PRNG). The random number generated by PRNG is only required to be updated for each encryption, which can provide the expected mitigation against the first order power and electromagnetic analysis. There is no need to apply the randomness to every clock cycle, which will cause too much performance degradation. Furthermore, the bulk and source terminals of every nMOS are connected, so that the bulk effect can be avoided. The general manufacturing process is NWELL technology. So the nMOS of FPL circuits needs to be inside a PWELL, which causes an additional cost. But compared to security that the FPL provides, it is a tradeoff between the security and the process cost. A diode is inserted between every parallel nMOS transistor and VDD_m terminal, so that each nMOS transistor can work in an isolated environment, i.e., the source terminal of every nMOS is separated from each other. In addition, considering the voltage drop of nMOS and diode, we have employed the low voltage threshold nMOS (LVT-NMOS) and the low voltage threshold diode (LVT-diode) rather than normal nMOS and diode, so as to make sure that VDD_m can provide enough driving capability. The input of the OR-gate consists of all VM_i, and its output directly controls the pMOS transistor.

Each parallel rail in the CVL unit consists of one LVT-NMOS and one LVT-diode, acting as an active resistance to produce a voltage drop if both are turned on. When an LVT-NMOS transistor is turned on, it produces a voltage drop from the source port to the drain port, whose value equals the threshold voltage V_{th} of the LVT-NMOS transistor. Meanwhile, the LVT-diode on the same rail is also turned on. The sum of the voltage drop over one LVT-NMOS and one LVT-diode is denoted as V_{th0}. The resistance of each parallel rail is mainly attributed to the LVT-NMOS transistor, which is associated with its size (the width W and the length L) when working at the saturation region. The combination of the OR-gate and the pMOS transistor guarantees that the original cell is still connected to the source voltage VDD when all LVT-NMOS are occasionally shut off, i.e., all VM_i equal 0. Denote the equivalent resistance for each parallel rail as R_i ($1 \leq i \leq n$) and that of all rails as R_a. Each rail contributes to the overall current drawn from the source voltage, resulting in variational power consumption.

Suppose k denotes the total number of VM_i whose value is 1 ($k = \sum_{i=1}^{n} VM_i, 0 \leq k \leq n$). For the sake of simplicity, all LVT-NMOS transistors and all LVT-diodes in CVL unit in the simulation setup are, respectively, of the same sizes, (i.e., all R_i are the same) which equal to R_c. Depending on the value of k, there are three cases.

1) $k = 0$, i.e., all $VM_i = 0$. All LVT-NMOS transistors are shut off and the OR-gate outputs a digital "0," which turns on the pMOS transistor. So CVL unit outputs VDD since the turned-on pMOS transistor produces no voltage drop, thus $V_{dp} = 0$.
2) $k = 1$, i.e., only one of VM_i equals 1. The LVT-NMOS transistor controlled by $VM_i = 1$ is the only conducting path while others are shut off, thus $V_{dp} = V_{th0}$.
3) $k > 1$, i.e., more than one LVT-NMOS transistor is turned on. Under this condition, the CVL unit consists of k parallel paths. If $R_i = R_c$, $R_a = R_c/k$, which forces V_{dp} to swing between 0 and V_{th0}. Note that the upper bound of the value of k is n, accordingly $1 < k \leq n$.

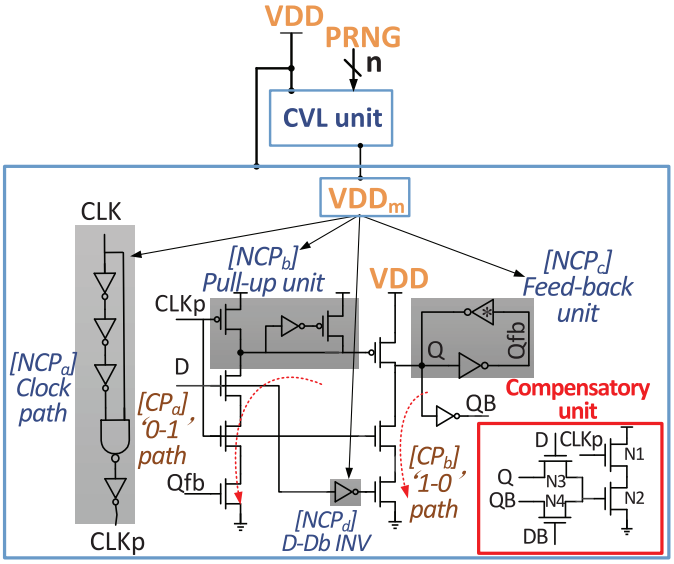


Fig. 3. Illustration of a standard FF under FPL scheme.

B. Proposed FPL Scheme

Fig. 2(b) shows the design of the proposed scheme, named FPL. It consists of three parts: 1) PRNG; 2) CVL unit; and 3) conventional logical cells (C). To be more specific, the n-bit PRNG generates all VM_i for CVL. The components in the original circuit C can be split into two parts, i.e., those on and off the critical paths denoted as CP_i and NCP_i, respectively. Note that the delay behavior of the entire circuit highly depends on the voltage of sequential elements, and note that all components in the FPL circuits which are connected to the CVL unit are powered by the hybrid voltage $VDD_m = VDD - V_{dp}$. So in order to keep the performance of modified FPL circuits behaving as normal, the CVL serves as a functional unit and is only inserted between the normal source voltage (VDD) and those components along the noncritical paths, such as NCP_a, NCP_b, etc. Due to the fact that VDD_m is corresponding to the value of k when n is chosen, the power consumption of the whole circuit is fluctuating with the varying k.

Depending on the values of VM_i in the CVL unit, there are different values of R_a and V_{dp}, resulting in different discrete power consumptions for some fixed data transition in the whole FPL circuit. More precisely, we define a metric *power step* denoted as N_{ps}, which is the number of all possible dynamic power values for each data transition when n is fixed. $N_{ps} = O(n)$ if all parallel paths in the CVL unit are of the same sizes. In this case, VDD_m can get $(n + 1)$ values between VDD and $(VDD - V_{th0})$. More importantly, N_{ps} can be as high as $O(2^n)$ only if the values of each R_i are properly tuned to be different for all parallel paths in the CVL unit.

III. Implementation of Secure Flip-Flop

A. Standard FF

In modern digital VLSI architectures, the clock system is composed of the clock distribution network and the FFs. Its power dissipation accounts for about 30% to 60% of the total power in the whole system. While about 90% of the clock system power is dissipated by the FFs and the last sections of the clock distribution network [17]. Consequently, the FF design is of great importance for VLSI. A conditional discharge FF (CDFF) is developed based on the conditional discharge technique, which is applied for both implicit and explicit pulse-triggered FFs [24]. In this article, we treat CDFF as a SC-based FF (SC-FF).

B. Modified FF With FPL

In Fig. 3, we show how to apply FPL to a SC-FF [24]. This illustration is named as FPL-FF, which is similar to the extension work of DRP-based FFs, such as SABL-FF or WDDL-FF in [8]. In Fig. 3, the critical paths are marked in brown and those components off the critical paths are marked in blue. CP_a and CP_b are two critical paths for $0 \rightarrow 1$ and $1 \rightarrow 0$ transitions, respectively.

The noncritical paths in SC-FF consist of four main components: 1) clock-path (NCP_a); 3) pull-up network (NCP_b); 3) double feed-back unit (NCP_c); and 4) $D - DB$ inverter (NCP_d), which are marked in Fig. 3. For example, the inverters in the clock path NCP_a are only for the purpose of providing certain delayed clock signal. In Fig. 3, those MOS transistors connected to VDD_m are highlighted in the grey shaded area.

The operational principle of the modified secure FF is explained as follows. According to the previous description, in the FPL-FF circuit, if all VM_i are 0, only the pMOS transistor is turned on, which connects VDD_m to VDD directly. In this case, the CVL unit becomes transparent and FPL-FF consumes about the same level of power as the pure SC-FF. While in other cases where at least one nMOS is turned on ($k \geq 1$), VDD_m is related to the varying value k, forcing the FPL-FF to consume various power consumptions. So the power of the entire circuit corresponding to some fixed data transitions is fluctuating, which makes the power model of SCA difficult for the adversary to estimate.

The delay of FF is mainly determined by the delay of its critical path. In the proposed FPL scheme, the cascade voltage

with randomness is only applied on the noncritical paths for variant transitions. As a result, the FPL has little negative effect on the total delay of FF after the modification.

C. Compensatory Unit

According to the logical functionality of standard FFs and the preliminary simulated verifications, the power consumption for variant data transitions ($0 \rightarrow 1$ and $1 \rightarrow 0$) is larger than that for invariant ones ($0 \rightarrow 0$ and $1 \rightarrow 1$), which forms the basic leakage elements that are explored by the generic SCA, such as DPA and CPA. Similar conditions are to be found in FPL-FF if the values of (n, k) are chosen once for all, where k is the number of random variables whose values are "1." This is because more charging and discharging activities happen at internal nodes, causing more power for variant data transitions. All in all, the vertical power characteristics can be fluctuated among different power steps by applying the FPL scheme alone, while the horizontal power properties in a fixed power step may still be statistically distinguishable by DPA.

In order to alleviate this contradiction, we append a CU to enhance its DPA-resistance, as highlighted in the red box of Fig. 3. Accordingly, when the FF makes a $0 \rightarrow 1$ or $1 \rightarrow 0$ transition during the clock pulse window (t_{CLK_p}), one of the pass-transistor gates controlled by D or DB is switched off while the other one outputs 0. So the short-circuit path is shut down, i.e., the CU is off. Otherwise, when the inputs of FF keep unchanged, the CU is turned on, which consumes compensatory dynamic power during CLK_p. As mentioned earlier, the total power of FPL-FF (P_{total}) consists of three portions: 1) the power of original FF (P_{FF}); 2) the power of CVL unit (P_{CVL}); and 3) the power of CU (P_{CU}). So the randomness of power is derived from the uncertain sum of three parts relying on VDD_m.

IV. Experiment Results of Secure FPL-FF

A. Power Performance

In order to verify the effectiveness of the designs described in previous sections, the power performance of secure FPL-FF has been tested and compared with the original SC-based FF. The testbench follows that in [25]. The results are obtained from HSPICE in the SMIC 65-nm CMOS technology at room temperature, and $VDD = 1.2$ V. We assume all the nMOS transistors in the CVL unit are of the same size throughout this article. In addition, we have also performed the simulation in the worst case (slow–slow corner) to evaluate the robustness of the proposed design, which is presented in Appendix A.

Recall that n and k are the number of parallel paths and turned-on nMOS transistors in the CVL unit. Fig. 4 presents the transient waveforms of FPL-FF under the condition of $(n, k) = (4, 1)$ for the clock signals CLK and CLK_P, the input D, the output signals Q, etc. Due to the proper transistor size adjustment, FPL-FF functions properly when only one path in CVL is on and VDD_m reaches its minimum value about 0.7 V. Furthermore, glitches can be found at internal nodes (e.g., Qb) which cause the glitch power.

For simplicity, only the cases of $n \leq 4$ (n is a power of 2) are carefully discussed in order to demonstrate the efficiency and the improved security of the FPL scheme. Each case is corresponding to different values of k. Table I depicts the simulation results of the original SC-FF and the secure FPL-FF. In Table I, each row shows the power consumption for four different transitions in the same power step, denoting the different combinations of (n, k). Especially, $n = 0$ stands for SC-FF without any modification. Let $P_{00}^{n,k}, P_{01}^{n,k}, P_{10}^{n,k}, P_{11}^{n,k}$ denote the power consumption for corresponding transitions for specific (n, k). The data out-of (in) the parentheses are the results of FPL-FF without (with) the CU. Each cell in Table I is the average power for the same type of data transition in ten consecutive cycles. B_n^k is the binomial coefficient for choosing k from n. The last column Δ_n calculates the statistical power difference between variant and invariant transitions over all possible k, shown as the below of Table I.

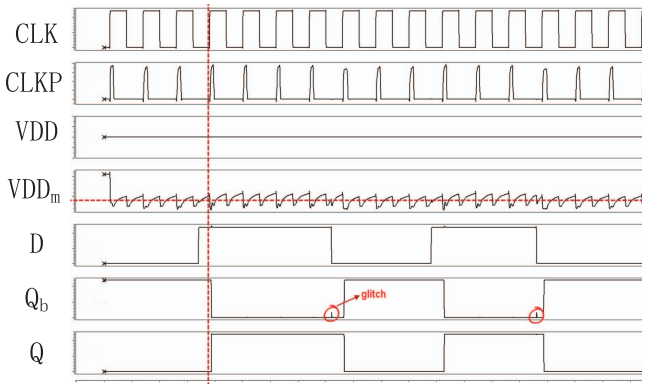


Fig. 4. Transient waveforms of FPL-FF.

TABLE I
Power Comparisons of FPL-FF at Various Conditions (μW).[1]

n	k	$P_{00}^{n,k}(0 \rightarrow 0)$	$P_{01}^{n,k}(0 \rightarrow 1)$	$P_{10}^{n,k}(1 \rightarrow 0)$	$P_{11}^{n,k}(1 \rightarrow 1)$	Δ_n
0	0	2.756	4.931	3.912	2.669	0.237
1	0	2.74 (6.82)	4.54 (5.72)	3.84 (5.90)	2.74 (6.76)	0.144 (0.030)
	1	5.57 (9.35)	5.10 (8.36)	5.69 (9.32)	3.27 (8.14)	
2	0	2.74 (5.83)	4.60 (5.64)	3.86 (5.57)	2.74 (5.77)	0.126 (0.029)
	1	5.59 (8.08)	5.16 (7.51)	5.72 (8.33)	3.28 (6.58)	
	2	4.45 (6.94)	4.51 (6.90)	5.06 (7.78)	3.18 (6.45)	
4	0	2.75 (7.33)	4.64 (5.88)	3.86 (6.29)	2.74 (7.45)	0.119 (0.009)
	1	5.61 (9.55)	5.16 (8.80)	5.69 (9.74)	3.31 (8.21)	
	2	4.49 (8.65)	4.59 (8.19)	5.08 (9.01)	3.18 (8.14)	
	3	3.91 (8.12)	4.32 (7.80)	4.70 (8.78)	3.05 (8.02)	
	4	3.63 (8.07)	4.15 (7.61)	4.45 (8.49)	2.97 (7.69)	

$$\Delta_n = \frac{\left|\sum B_n^k P_{01}^{n,k} + \sum B_n^k P_{10}^{n,k} - \sum B_n^k P_{00}^{n,k} - \sum B_n^k P_{11}^{n,k}\right|}{\sum B_n^k P_{01}^{n,k} + \sum B_n^k P_{10}^{n,k} + \sum B_n^k P_{00}^{n,k} + \sum B_n^k P_{11}^{n,k}}$$

In Table I, there are several important observations.

1) *Dynamic Fluctuation:* When $n > 1$, there are $(n + 1)$ power steps in total for every single data transition varying with the random number k (for both without or with the CU).
2) *Vertical Overlap:* For specific n in FPL-FF, the ranges of fluctuating power for different transitions are overlapped. For example, $P_{00}^{4,2} = 4.49(8.65)$ μW is larger than $P_{01}^{4,3} = 4.32(7.80)$ μW but smaller than $P_{01}^{4,1} = 5.16(8.80)$ μW. This is because that the change of P_{CU} may be larger or smaller than the change of sum of P_{FF} and P_{CVL}, leading to the variations in the total power.

[1]Source table from [15].

3) *Horizontal Overlap:* Even for the same (n, k), invariant transitions may consume more power than variant ones. For instance, $P_{00}^{4,1} = 5.61(9.55)\ \mu$W while $P_{01}^{4,1} = 5.16(8.80)\ \mu$W. This is because that the increment in P_{CU} is larger than the decrement in P_{FF} while P_{CVL} keeps unchanged. As a result, the fact of vertical and horizontal overlap contributes to further elevating the SCA resistance of the circuit.
4) *Reduced Statistical Difference:* With the CU, the statistical power difference between variant and invariant transitions is reduced, making DPA difficult. For example, compared to the SC-FF, the Δ_n of FPL-FF is reduced from 0.237 to 0.119 (without CU) and to 0.009 (with CU) when $n = 4$. Furthermore, Δ_n with CU is reduced by 4 to 13 times in comparison to that without CU.

As a consequence, the dependency of fluctuating power of the whole circuit on different data transitions is totally diffused. If n is increased, there will be more power steps for the same transition and more complicated overlaps between different transitions. Furthermore, this scheme can be combined with other existing countermeasures to achieve higher DPA-resistance. Even when all nMOS transistors are designed with the same size, there still exist slight differences among those theoretically equivalent resistances in the real deployment. Therefore, the fluctuating power characteristic of the entire circuit makes the traditional PA difficult to reveal the secret key.

In Table I, FPL-FF with CUs cost much more power consumption than that without CU, which is about twice of the original design. However, this is an expected result as there is always large overhead so as to improve the security of circuits, including power, area, etc. In this article, the emphasized power overhead is on its reduced amount when compared with SABL and WDDL-based logics. Section V uses two case studies to prove the efficiency of FPL logic.

B. Timing Performance

Except for the power performance of the scheme, the timing performance of FPL is also a necessary point to discuss. So the timing performance of FPL is also analyzed under the simulation environment. The delay parameter used in this test is the minimum $D - Q$ delay (t_{D-Q}), including both setup time (t_{setup}) and $CLK - Q$ delay (t_{CLK-Q}), so the delay characteristic can be reflected more appropriately. The t_{D-Q} is obtained by sweeping the low-to-high (D_{L-H}) and high-to-low (D_{H-L}) input data transition times with respect to the clock edge. Usually, the minimum t_{D-Q} delay differs for the (D_{L-H}) and (D_{H-L}) transitions, and the worst minimum t_{D-Q} delay is chosen. The (t_{setup}) is measured as the optimal time to minimize the (t_{D-Q}) delay. The hold time (t_{holdtime}) refers to the minimum time period after the clock edge to ensure that the input signal is captured by the corresponding clock edge. Here, the random control signals in CVL unit is $(n, k) = (4, 2)$, i.e., two of four VM_i are equal to 1. The specific simulation results are shown in Table II.

TABLE II
DELAY PERFORMANCES OF STANDARD AND FPL-BASED FF

	SC-FF	FPL-FF
$t_{D-Q}(ps)$	191.89	227.16
$t_{setup}(ps)$	-126.07	-168.75
$t_{CLK-Q}(ps)$	317.96	396.02
$t_{holdtime}(ps)$	286.52	529.55

As seen from the Table II, the delay performances of the standard and FPL-based FF stay at the same level. This is because that the FPL scheme is mainly applied to the noncritical paths, which has a limited side effect on the delay performances of the circuit. While the hold time of FPL-based FF is worse than the standard one, due to the reason that the clock pulse needs more time to sample the input signals.

V. CASE STUDIES—PRESENT/AES ENCRYPTION

The secure FPL-FF is developed as a building block for cryptographic circuits which should provide the basic cryptographic functionalities. Power-based SCA relies on the data-dependency between the power dissipation and the underlying data transitions. In our FPL, the power fingerprints from the encryptions vary significantly even if the measured traces are processing the same plaintext using the same key. This is due to the randomness from the VM_i.

In this section, we take PRESENT [26] and AES [27] as illustrative examples to evaluate the effectiveness of the proposed FPL scheme. For the simplicity, we only focus on the nonlinear table lookups in cryptographic encryptions which are the common target operation in side-channel analysis. Specifically, the power dissipation for the table lookup with the same plaintext and the same secret key will be still fluctuating, due to the random variables in CVL. The entropy introduced by the fluctuating factors in power increases the difficulty for the adversary to infer the power behavior of the target logic.

A. Implementation and Cost

AES is a symmetric cipher standardized in 2001 by NIST [27] as a formal successor of preceding DES. PRESENT is an ultralightweight block cipher proposed in 2007 [26], which can be efficiently implemented in low-cost hardware. The nonlinear substitution is normally the target of SCA, we lay our focus on that. The input and output for the SBoxes in PRESENT and AES are 4 and 8 bits, respectively.

The applied experiment setup is set up with two 4/8-bit input registers (Data and Key), one 4/8-bit output register, one 4/8-bit XOR gate, and the SBox module from the PRESENT/AES algorithms. The standard supply voltage is 1.2 V. The load capacitances to the output nodes are 3 fF. The setup is working as a simplified testbed. Key is unknown thus requiring the PA to explore. Data, i.e., the plaintexts, are assumed to be known to the adversary. Plaintexts can be fixed in order to help detecting the power pattern in SPA. More often, they are randomized during advanced SCA, such as DPA and CPA.

TABLE III
SIMULATION RESULTS FOR THE ENCRYPTION CIRCUITS WITH PRESENT/AES SBOX MODULES

Testbench	PRESENT encryption circuit			AES encryption circuit		
	SC-based	FPL-based	WDDL-based	SC-based	FPL-based	WDDL-based
Area[GE]	152	221 (×**1.45**)	520 (×3.42)	1340	1478 (×**1.10**)	3111 (×2.32)
P_{max}[fJ]	2212.2	2335.9	7097.0	2590.9	3664.6	21249.0
P_{min}[fJ]	769.6	1132.2	6829.0	1301.0	2595.4	20842.0
P_{avg}[fJ]	1299.3	1532.3 (×**1.18**)	6958.0 (×5.36)	2249.6	3307.6 (×**1.47**)	21083.1 (×9.37)
σ_P	362.2	281.6	80.6	219.0	181.2	79.0

For the purpose of illustration and for the sake of page limitation, only the case of $n = 4$ is applied and verified in the same test bench for both algorithms.

Two simplified circuits of testbeds have been implemented, in order to evaluate the performance and the cost of different logics in practical encryptions. After compiling and synthesis by design compiler (DC), the core modules of the standard cell for PRESENT/AES-SBox are formed by 37 and 464 gates, respectively. In traditional designs, all simulated gates were supposed to be fed with stable static inputs at the beginning of the evaluation period. In this simulation setup, all power traces are acquired from ideal digital circuits by detailed transistor-level simulation through HSPICE. Note that in a real-world implementation, the inherent and the interconnecting noise in the chip inevitably impact the electrical behavior of the circuits. Accordingly, normally distributed noise is intentionally added to each power trace to approximate the reality. The noise is described by a mean value μ with an expectation about 2% of the highest power of the circuit along the time-domain and with the default variance σ^2.

To demonstrate the feasibility and effectiveness of our proposed scheme, the two circuits for PRESENT/AES are implemented with SC-based and FPL-based logics for comparisons. In order to compare with the existing cell-level-based countermeasures, the PRESENT/AES-SBox modules are also implemented with WDDL [10] logic. The implementation aspects of WDDL are discussed in Appendix B.

In Table III, the results for the two circuits including area, performance, and power dissipation overhead are summarized. To be specific, the gate equivalents (GEs) of SC-, FPL- and WDDL-based testbench implementations are summarized in the first row of Table III. Here, one GE represents the area of one NAND gate. In Table III, the area costs of the FPL-based implementations are very close (1.1 times for AES) or comparable (1.45 times for PRESENT) to those SC-based ones. The cost of PRNG is not considered, which will only add a slight overhead to FPL if included. In comparisons, the WDDL-based implementations actually increase a lot of area cost (3.42 times for AES and 2.32 times for PRESENT). The advantage of FPL over WDDL in terms of area cost comes from the fact that the proposed FPL only modifies the FFs instead of building an entire complementary rail.

The power generation in Table III is described as follows. For SC-based or FPL-based module, it requires two clock cycles to complete the encryption. At the beginning of the first cycle, the testbench evaluates the inputs of plaintext and key, while at the beginning of the second cycle, the testbench outputs the ciphertext. Note that the SBox lookup is completed during the second clock cycle. For every SC-based or FPL-based power trace, we collect 300 measurements points per input in total. While for the WDDL-based module, due to the alternation of precharge and evaluation operations, the whole encryption takes 4 clock cycles, i.e., 600 points for each power trace. N traces are collected where $N = 30$ for PRESENT and $N = 256$ for AES. The maximum power consumption ($P_{\max}$) and the minimum power consumption ($P_{\min}$) denote the maximum and minimum value of the points in the average of those N traces. P_{avg} and σ_P are the mean and standard deviation, respectively.

Specifically, average energy overheads, i.e., P_{avg}, of FPL-based PRESENT-SBox and AES-SBox modules are only increased by 18% and 47%, respectively, when compared with SC-based implementations, which noticeably outperform the WDDL-based circuit. In fact, WDDL-based PRESENT consumes 5.35 times of the power that SC-based implementation requires, while WDDL-based AES further increases this to 9.37 times.

B. Security Evaluation Methods

After acquiring the power traces for different input data, we then launch the PA to validate the enhanced security of the proposed logic.

Numerous evaluation tools have been proposed in prior literatures for evaluating the side-channel vulnerabilities, such as CPA [4], mutual information analysis (MIA) [28], TVLA [29], etc.

CPA proposed as an improvement to DPA, is the most common method to estimate the linear relationship between power models and real power traces [4]. As the most effective and fastest evaluation methodology among those approaches, TVLA has been standardized as a metric to assess the potential side-channel leakage. A main feature for TVLA is that the analysis does not require the leakage model. Since it just relies on the measured traces, TVLA is more generic. As a result, we choose CPA and TVLA as basic evaluation tools in this article due to their convenience and universality.

1) Correlation Power Analysis: CPA was proposed by Brier *et al.* [4]. The hypothetical power consumption in CPA, denoted as H, was set to the HW model, which is the number of bits set to 1 in an SBox output. Based on the linear relationship between the measured consumption W and the hypothetical power consumption H, CPA computes their correlation as below

$$\rho_{WH} = \frac{\text{cov}(W, H)}{\sigma_W \sigma_H} \tag{1}$$

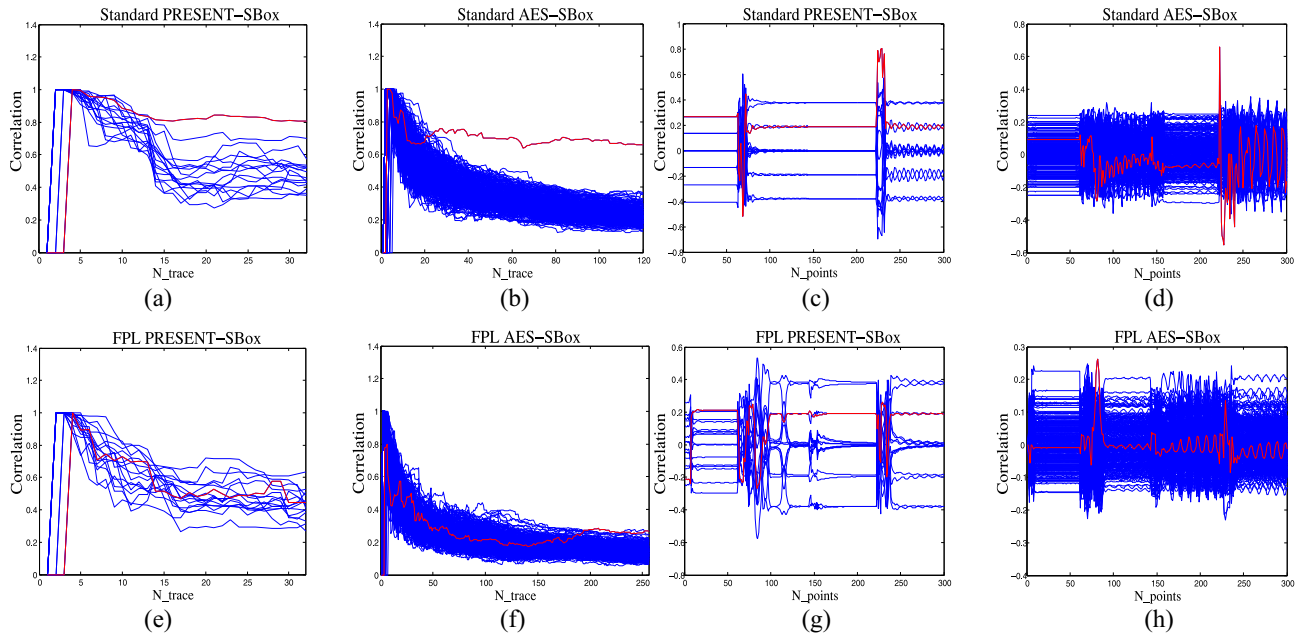


Fig. 5. CPA results of standard and FPL-based PRESENT/AES-SBox modules. (a) Correlation versus number of traces. (b) Correlation versus number of traces. (c) Correlation versus length of a trace. (d) Correlation versus length of a trace. (e) Correlation versus number of traces. (f) Correlation versus number of traces. (g) Correlation versus length of a trace. (h) Correlation versus length of a trace.

where σ_W and σ_H are the standard variances for W and H, respectively. Then in realistic cases with a set of power traces W_i and hypothetical intermediate power values H_i $(1 \leq i \leq N)$, the correlation can be computed as the Pearson correlation coefficient ρ for jth key hypothesis with N power traces

$$\hat{\rho}_{WH_j} = \frac{N\sum_1^N W_i H_{i,j} - \sum_1^N W_i \sum_1^N H_{i,j}}{\sqrt{N\sum_1^N W_i^2 - \left(\sum_1^N W_i\right)^2}\sqrt{N\sum_1^N H_{i,j}^2 - \left(\sum_1^N H_{i,j}\right)^2}}. \tag{2}$$

In (2), the index of the highest values of the matrix ρ_{WH} reveals the possible position(s) at which the chosen intermediate result has been processed and the key is used by the circuit [8]. From the statistic point of view, CPA reveals the strongest hypothesis (of secret key) at the place where the real-time power dissipation and the data being processed have the highest correlation.

2) Test Vector Leakage Assessment: Unlike CPA, TVLA does not aim for key recovery. It performs leakage detection, i.e., detects any data-dependent leakage in measured traces through hypothesis testing. In principle, two sets of traces are required for TVLA computation: the first trace group corresponds to a fixed key and chosen fixed plaintexts, serving as the reference; The second trace group corresponds to random plaintexts and the same key. The tests on these two groups are known as fixed versus random (FVR) test. A null hypothesis is assumed to test if both groups are identical. A rejected null hypothesis confirms the presence of data-dependent leakage.

In TVLA, the two sets of power traces are specified as the group A and B. Denote (X_A, S_A) and (X_B, S_B)—the mean and the standard deviation of the traces in A and B, respectively. Let N_A and N_B be the cardinality of A and B. Then the t-statistic T (over the same time) is computed by (3). If the t-statistic stays within the range ± 4.5, the null hypothesis is accepted with a confidence level of 99.999% [30]

$$T = \frac{X_A - X_B}{\sqrt{S_A^2/N_A + S_B^2/N_B}}. \tag{3}$$

C. Experimental Results

CPA: In the first step, We evaluate the security of SC-based (SC) implementation of PRESENT/AES-SBox modules against CPA analysis. We have collected 30/120 power traces of the encryption circuit corresponding to independent and uniformly distributed plaintexts. The goal of our CPA is to explore the first nibble/byte of the secret key that is used in encryptions. The attack results are provided in Fig. 5, where the red curve stands for the correct key hypothesis. The minimum number of traces to disclose the key nibble/byte is denoted N_{MTD}. The correlations of the various key hypotheses corresponding to the number of power traces (N_{trace}) are shown in Fig. 5(a) and (b) for PRESENT and AES, respectively. When $N_{\text{trace}} \geq N_{MTD}$, the coefficient curve for the correct hypothesis will be always above those for the wrong hypotheses. $N_{MTD} \approx 12$ for PRESENT as shown in Fig. 5(a) and $N_{MTD} \approx 22$ for AES in Fig. 5(b). The correlations of the various key hypotheses corresponding to the length of the trace (N_{points}) are shown in Fig. 5(c) and (d). As for the correct hypotheses, the maximum coefficient is observed as an obvious peak at the rising edge of the second clock cycle.

In a similar way, we have performed a CPA analysis on the FPL-based PRESENT/AES-SBox modules with 32/256 power traces. Here, we employ the same keys as the experiment of SC implementations. For a better comparison, the attack results are also demonstrated in Fig. 5. In Fig. 5(e), the curve for the correct hypothesis is buried among all other curves and can not

be distinguished. In Fig. 5(g), there is no peak observed, therefore, CPA on FPL-based PRESENT is considered as fail. In Fig. 5(f), $N_{MTD} \approx 250$ for FPL-based AES, which is about 10 times of that for SC-based AES. The FPL logic greatly boosts the security of the AES-SBox module. Unlike real measurement, the results from the precise simulation will not change with more measurements.

Furthermore, by observing Fig. 5(c) and (d) and (g) and (h), we find that a significant wide-range of correlation values are fluctuating around the 60th and 240th point in each power trace. This is mainly due to the driving supply current of FFs flowing at the rising edge of clock, which is normally the timing points where critical information may leak. Note that the FPL-based cells are built in a simple way upon the SC-based cells. Through the results in Fig. 5, we find that the expected security escalation from the proposed FPL enhancement has been achieved in comparison with SC-based implementations. For the sake of completeness, the evaluations of FPL-based implementation without the CU are also conducted for comparisons, which are listed in Appendix C for reference.

To evaluate the security of the WDDL implementation, CPA attacks are also conducted. As aforementioned, under the condition that the capacitive loads at both complementary rails are balanced, the WDDL-based logic can prevent the nonlinear parts of encryption algorithms from the first-order CPA attack. The CPA results in Appendix B also verify this point. To this extent, both WDDL and our proposed FPL can be used to mitigate or prevent the PA attacks. However, there are two shortcomings for WDDL-based implementation. One is that the implementation cost of area and the performance cost are very high as shown in Table III. The other is that the prerequisite of capacitive load balance is difficult to satisfy in practice.

As with the evaluation of most countermeasures, the protection can be attributed to either the reduction of leakage or the wrong assumption on leakage models. The former is a good countermeasure but the latter is a bad evaluation methodology. To confirm it, we next perform TVLA evaluation which are leakage model agnostic. Passing a TVLA test confirms the reduction in leakages.

TVLA: In the experiment, we further use the TVLA method to conduct further security evaluation. In Fig. 6, the leakages of SC-, FPL-, and WDDL-based implementations are marked in blue, red, and pink, respectively. A total of 129 power traces have been collected for plotting the TVLA leakage. The target circuit is AES with different implementation formats. As discussed before, we follow the regular threshold line selection (+4.5, −4.5) as the secure region. The experimental results are plotted in Fig. 6. As seen in this figure, the FPL-based implementation is the only one whose leakage values along the whole trace are within the threshold (±4.5) throughout the time window. It should be stressed that TVLA is a universal measurement method, which does not rely on specific leakage models. Hence, the leaked information for different circuit may represent totally different implementation vulnerabilities. In this joint TVLA plot, the leakage styles vary significantly, particular for the leak regions. This is due to the variant circuit

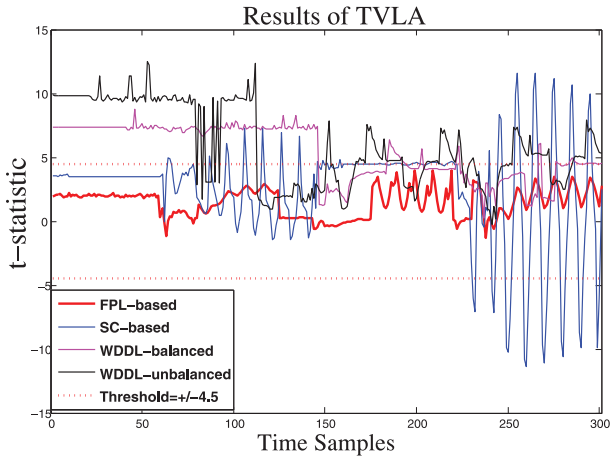


Fig. 6. TVLA tests for AES encryption circuit with various implementations.

structures. From Fig. 6, it is seen that the testbench with FPL-based implementation is the only candidate logic that passes the TVLA leakage test in this experiment. The beginning parts of all traces of *t*-statistic values are flat due to the preparation of the rising edge of the clock or precharge phase. Note that the TVLA test is also applied to WDDL-based implementation with unbalanced capacitive loads and fails the test, which is marked in grey in Fig. 6. The details of unbalanced WDDL-based implementation will be given in Section VI.

For a summary, given a number of traces, FPL shows the least leakage from the TVLA evaluations.

D. Further Discussions

According to the observations and analysis achieved from previous sections, several important conclusions can be drawn.

1) The encryption modules (both PRESENT and AES) with simple SC-based logics are vulnerable to the generic first-order CPA attacks.
2) PRESENT can be effectively protected against CPA by both the traditional WDDL logic and our proposed FPL logic. Yet the overheads (area and power) of our FPL logic are similar to the SC logic, because only FFs are modified. Comparatively, the overheads of WDDL-based implementation are greatly increased at the cost of 2+ times of area, 6–7 times of evaluation time, and 3–4 times of power consumption [18]. In WDDL [10], the average power consumption is increased about 5.36 times to that of SC-based implementation.
3) For AES, WDDL-based logic can counteract the first-order CPA. Based on the aforementioned simplified realization of the FPL-based module (adopting the same sizes of nMOS transistors in the CVL unit), our proposed FPL logic provides high-level protection as well, which is comparable to the WDDL-based logic and better than SC logic. It should be noted that the overheads of WDDL logic are significantly larger than FPL logic and SC logic. More concretely, the WDDL-based module for AES needs about 9.37 times of power against the SC-based module, which is more serious compared with the

FPL-based module (about 1.47 times). The extra specified overheads induced by WDDL logic are introduced in details in the Appendix B.

4) The TVLA results for the testbench show that the proposed FPL logic has less side-channel leakages than SC- and WDDL-based logical modules, which is the only circuit that satisfies the empirical secure threshold (± 4.5).

In our proposal, the simulation results are based on a simplified realization of FPL-based module, which only used a 4-bit PRNG controlling 4 rails of nMOS paths in the CVL unit. The nMOS transistors in CVL and CU are of the same size in the current deployment. It is emphasized that in real scenarios those critical parameters can be sophisticatedly tuned by slightly diversifying the sizes of all transistors in both CVL and CU. This adjustment can result in the actual difference among those trails and generate more different power steps, which will make the adversary's PA much more difficult. Since FPL is designed at the cell level, theoretically it should also naturally protect the circuit against the first-order electromagnetic analysis.

In order to further improve its SCA-resistance, the proposed FPL can apply more bits of PRNG controlling more rails of nMOS paths in the CVL unit.

VI. Improving WDDL With the Combination of FPL

Apart from the SC-based logic, our proposed logic can also be combined with other classical cell-level countermeasure logics, such as SABL and WDDL. Note that the WDDL-based modules should satisfy the necessity for balanced capacitive loads at both internal nodes and complementary output nodes. The combination with FPL can relax the WDDL-based solution from that limitation, which will further improve the SCA-resistance of the circuit. We compare the resistance of the WDDL-based and FPL-WDDL-based AES-SBox modules against CPA.

The fundamental cells applied for FPL-WDDL-based module are shown in Fig. 7, including traditional WDDL-based AND-gates and OR-gates, the precharge wave generation scheme, and the modified FPL-FFs. Note that according to the nature of FPL design, only FFs are updated (marked in red at the right part of Fig. 7) and small compensation units are appended. The specific process of the FPL-WDDL-based module construction and the corresponding security evaluation are described as follows. First, we change the capacitive loads at the complementary output nodes, i.e., one rail increases those by 10% while the other rail decreases by 10%. Second, we keep the other conditions unchanged and resimulate the testbench. Third, we combine the FPL scheme with the conventional WDDL by replacing the single-rail standard-cells-based FF (SR-FF) with FPL-FF. Finally, we redo the simulation and compare the results.

Fig. 8 presents the specific CPA attack results of WDDL-based and FPL-WDDL-based AES-SBox modules. Under the same condition of unbalanced complementary output capacitive loads, CPA reveals the right key using about 180 power traces. That is, $N_{MTD} \approx 180$, as shown in Fig. 8(a). Note that

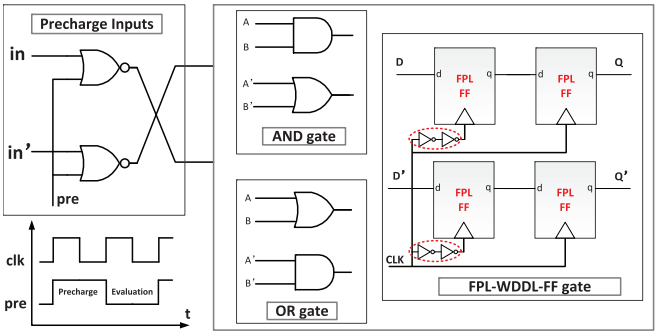


Fig. 7. Improved WDDL precharge with the combination of FPL logics.

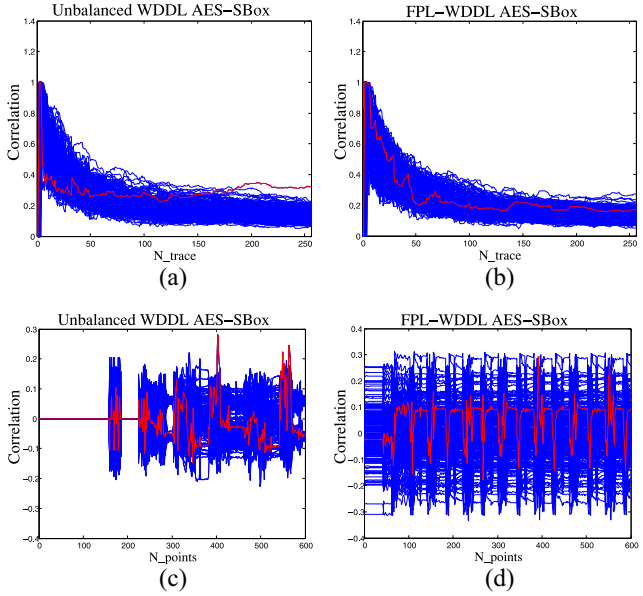


Fig. 8. Comparisons of WDDL- and FPL-WDDL AES-SBox modules. (a) Correlation versus number of traces. (b) Correlation versus number of traces. (c) Correlation versus length of a trace. (d) Correlation versus length of a trace.

the peaks of correlation coefficients corresponding to the correct key hypothesis can be found in multiple locations along the trace in Fig. 8(c). To this extent, the unbalanced WDDL-based module is vulnerable to the first-order CPA analysis. Meanwhile, the TVLA test in Fig. 6 also shows that the unbalanced WDDL has quite a lot of leakages because most of the curve marked in grey is located outside of the ± 4.5 threshold.

The combination with the FPL scheme greatly improves the SCA-resistance of the FPL-WDDL-based module, which is broadly in line with the expected security escalation, and can be reflected in two facts:

1) In Fig. 8(b), the correct key guess can not be deduced with 256 traces. In fact, when the number of traces is increased to thousands or more, the red curve for the correct guess is indistinguishable from the wrong guesses, which makes CPA fail in this experiment.
2) Different from Fig. 8(c), the value of the maximal correlation coefficient for FPL-WDDL AES-SBox module in Fig. 8(d), is very close to other neighboring coefficients. This makes it more difficult for the adversary in finding

the corresponding rank of the correct key nibble/byte through key enumerations. To some extent, this combination prevents traditional PA with a higher success rate.

VII. Future Work

In this article, the FPL scheme is realized at the cell level and is applied to the noncritical paths in a single cell. The presimulation in Section V and VI has verified that the security is improved with limited transistors overheads. In the future, the resistance of FPL against electro-magnetic (EM) attacks will be analyzed. The result of the area overhead and delay of FPL will be further verified in the post-simulation test, for ensuring that the cost of the FPL scheme is affordable for normal place & route step in the back-end design stage of the IC manufacturing. The exploitation of security impacts from the randomness in PRNG, the performance testing of the AES circuits as a whole including both power and delay, and the advanced evaluation via higher-order SCA constitutes another part of the future work.

VIII. Conclusion

In this article, we proposed a power-diffusing logic named FPL, which randomizes the correlation between the real power consumption and the fixed data transitions. Our proposed FPL employs the CVL driven by a PRNG, in order to twist the basis of the generic side-channel attacks, such as DPA and CPA. To verify the proposal in real attack scenarios, we have implemented PRESENT/AES-SBox modules as a preliminary step with the SC-based, FPL-based, and WDDL-based logics, respectively. The detailed cell-level experimental results show that the FPL scheme provides elevated security level for hardware-implemented crypto cores against generic power-based SCA. Furthermore, the simple nature of FPL-FF allows it to be merged with other cell-level logic style to achieve higher security. This fact has been proved by the combination of FPL with WDDL, which can relax the WDDL from the constrained requirement of the balanced capacitive loads with a very limited overhead. The TVLA results for the testbench show that the proposed FPL logic has much fewer leakages than SC and WDDL logical modules. So our proposed FPL logic suits for not only SC-based modules but also for the existing protected modules with cell-level countermeasures.

Appendix A
Simulation Results of FPL-FF Under SS Corner

In order to test the influence of process variations on the FPL-FF, we have simulated the FPL-FF at Slow-Slow (SS) corner, where the supply voltage is 1.1V and the temperature is 125°C. The corresponding waveform is shown in Fig. 9. It shows that the testbench functions properly under the worst condition, proving the robustness of the proposed design. And for simplicity, we just collected the power performance results by transient simulation for $n = 4$, as shown in Table IV.

In Fig. 9, under different combinations of (n, k), the output voltage of CVL unit (VDD_m) takes different values, which provides the power fluctuation for the whole circuit. And

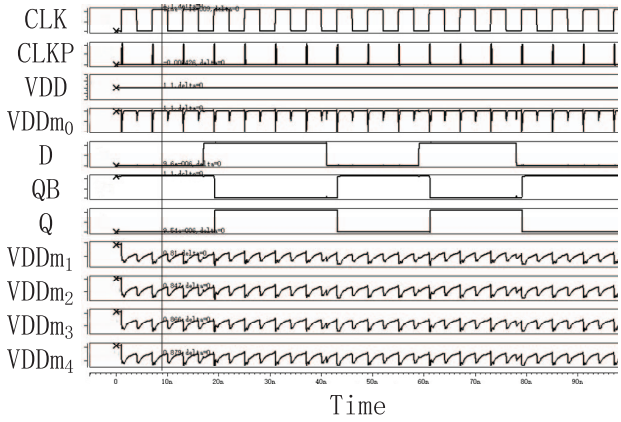


Fig. 9. Transient waveforms of FPL-FF at SS corner.

TABLE IV
Power Comparisons of FPL-FF at SS Corner (μW)

n	k	$P_{00}^{n,k}$ $(0 \to 0)$	$P_{01}^{n,k}$ $(0 \to 1)$	$P_{10}^{n,k}$ $(1 \to 0)$	$P_{11}^{n,k}$ $(1 \to 1)$	Δ_n
0	0	2.28	4.53	3.51	2.18	0.286
4	0	2.25 (4.65)	4.35 (4.99)	3.45 (4.56)	2.14 (4.94)	0.176 (0.008)
	1	3.58 (6.17)	3.94 (5.91)	3.89 (6.23)	2.28 (5.99)	
	2	2.90 (5.61)	3.69 (5.53)	3.60 (5.77)	2.23 (5.58)	
	3	2.63 (5.44)	3.55 (5.36)	3.45 (5.41)	2.19 (5.49)	
	4	2.46 (5.36)	3.44 (5.25)	3.33 (5.33)	2.13 (5.40)	

$$\Delta_n = \frac{|\sum B_n^k P_{01}^{n,k} + \sum B_n^k P_{10}^{n,k} - \sum B_n^k P_{00}^{n,k} - \sum B_n^k P_{11}^{n,k}|}{\sum B_n^k P_{01}^{n,k} + \sum B_n^k P_{10}^{n,k} + \sum B_n^k P_{00}^{n,k} + \sum B_n^k P_{11}^{n,k}}$$

observing the power metrics in the table, we can find that the power consumption of $0 \to 0$ data transition is larger than that of $1 \to 1$ data transition when CU is neglected, which is due to the fact that the leakage power caused by leakage current flowing through the switched-off transistors is significantly increased in deep submicrometer CMOS technology. Furthermore, it should be noted that the total power of the module heavily depends on the width of clock-pulse, so the pulse period should be as narrow as possible on the premise that the whole testbench functions properly.

Appendix B
Process to Implement the WDDL-Based Encryption Modules With Some Modifications

The specific process to implement the WDDL-based cells in PRESENT/AES-SBox is shown in Fig. 10, where a stands for one input signal and a' stands for the complementary (inverted) signal. For an arbitrary SC module (gate), decompose it into AND-OR-Inverter (AOI-) based module; then duplicate the AOI-based module, keep the first one unchanged while substitute the AND gate with OR gate, and substitute the OR gate with AND gate in the other module. Finally, remove the inversion in both modules by exchanging the complementary output nodes. It should be noted that the inversion should be avoided since it halts the precharge wave (normally all '0's) through the combinatorial logic chain and hence leads to unbalanced power between the complementary rails.

Specifically, the entire testbench for WDDL-based logic is shown as in Fig. 11. However, based on the simulation results, we can find that the alternation between the precharge phase

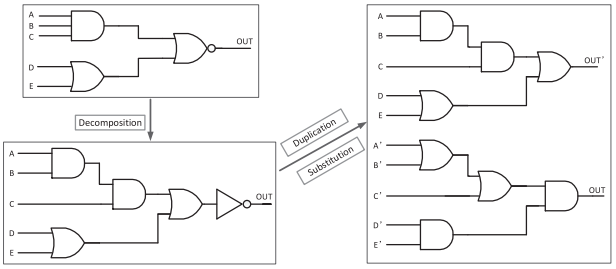


Fig. 10. Process for building the WDDL-based module.

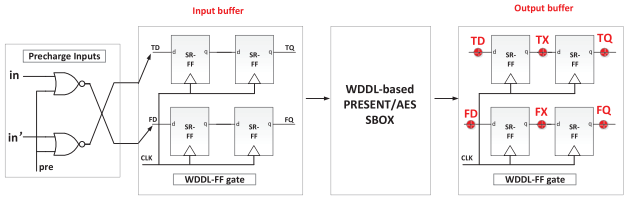


Fig. 11. Whole testbench for WDDL-based logic.

and the evaluation phase in the WDDL-FF was broken. Note that we have applied a state-of-the-art pulsed-trigged FF which propagates the input to the output during the transparent window just at the positive edge of the clock signal, and the four SR-FF are directly connected to the clock signal simultaneously. According to the digital circuit theory, the alternation between the precharge phase and the evaluation phase in the WDDL-FF should function properly. However, after simulated observation and theoretical analysis, we discovered that the nodes Q (highlighted in both complementary rails, denoted as TQ and FQ) were either consistently keeping pace with the internal nodes X (highlighted in both complementary rails, denoted as TX and FX) or always keeping 0 following the precharge signal. The specific reason is that during the evaluation phase of WDDL-FF, the node D (denoted as TD and FD) in the output buffer directly impacted the node X in the output of the first SR-FF, which should propagate to node Q independently during the same period. As a result, the alternation between the precharge phase and the evaluation phase was broken, leading to *race problems or hazards*.

Without loss of generality, we have simulated an exemplary data flow: $1 \rightarrow 0 \rightarrow 0 \rightarrow 1 \rightarrow 1$, in order to further elaborate the problem. First, we modified the width of the clock pulse (CLK_P) and kept the other parts of the original WDDL-FF unchanged. The simulated results are given in Fig. 12. As seen from the above figures, there are two cases: one scenario is that if the CLK_P is too narrow, only internal nodes TX and FX responds to the input data, yet the output nodes TQ and FQ just follow the precharged signal and always keep 0; the other scenario is that if the CLK_P is wide enough, all the internal nodes and output nodes follow the input data and the alternation between the precharge phase and the evaluation phase is corrupted. Consequently, the original WDDL-FF is correct in digital theory, yet hard to be realized in reality.

Second, we made a small correction by delaying the input clock for the SR-FFs in the first column of WDDL-FF with two specially sized cascaded inverters, as highlighted in red

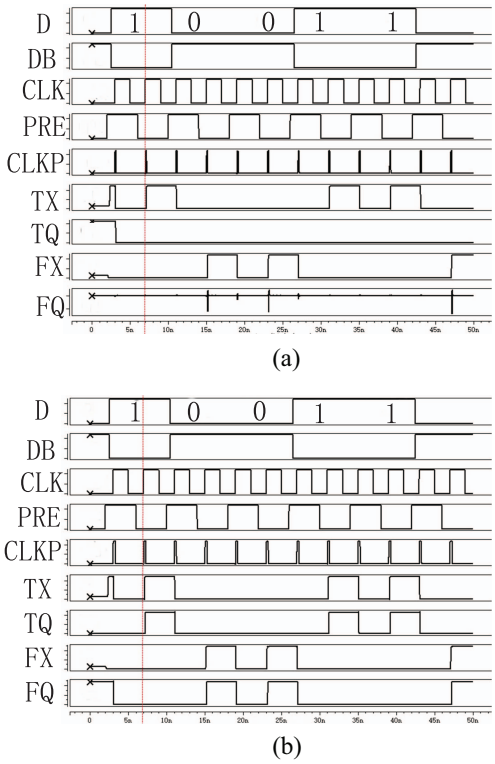


Fig. 12. Transient waveforms of a portion of signals in the WDDL-FF under different conditions. (a) With short CLK_p. (b) With long CLK_p.

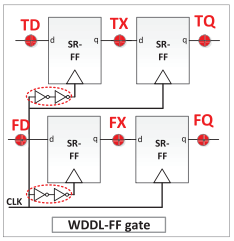


Fig. 13. Correction for the WDDL-FF module.

dashed circuit in Fig. 13. This modification can be treated as a supplemental method for theory in real scenarios. The simulated results are shown in Fig. 14, where P denotes the precharge signal. The key point here is that the precharge signal (0) is inserted between the two valid signals, which ensures that both the HW and HD models are balanced. As a result, considering these four nodes together (TX, FX, TX, FX in complementary rails), at every rising clock edge there are constantly two and only two flips: one $0 \rightarrow 1$ flip and one $1 \rightarrow 0$ flip, leading to constant total power consumption. In addition, the duration of the onset ramp at the clock and input data nodes, i.e., the transit time from the initial value to the pulse plateau value should not be too long, or the sequential race competition problems may happen at the output nodes.

The CPA attack results are shown in Fig. 15 under the same input vectors (keys and plaintexts). Seen from the simulation results, the WDDL-based logic can protect the nonlinear parts of encryption algorithms from the first-order CPA attack. After observing Fig. 15(c) and (d), due to the employed input/output

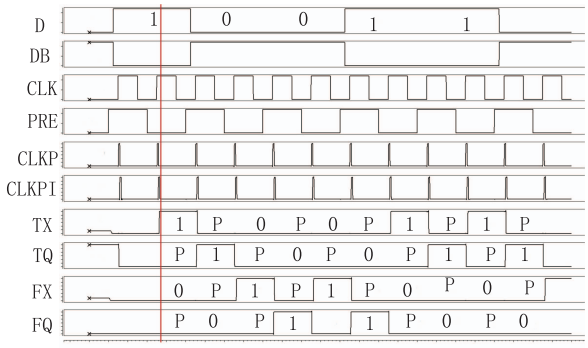


Fig. 14. Transient waveforms of part of signals in the modified WDDL-FF.

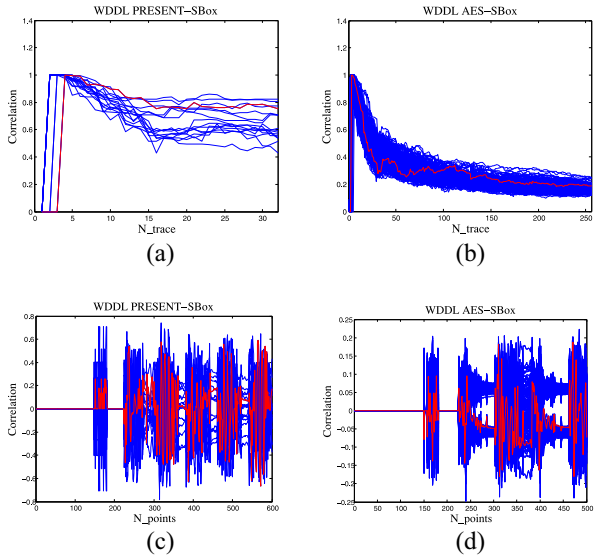


Fig. 15. CPA results of WDDL-based PRESENT/AES-SBox modules. (a) Correlation versus number of traces. (b) Correlation versus number of traces. (c) Correlation versus length of a trace. (d) Correlation versus length of a trace.

WDDL-based FF-buffers, the correlation based on the various key hypotheses in a single power trace is greatly increased around every rising edge of input clock signal, which complies with the principle of WDDL logic. As a caveat, due to the propagation of precharge signal('0') in the WDDL circuit, the correlation coefficients in Fig. 15(c) and (d) remain 0 until the second rising edge of the input clock (about 160th point along a single power trace). However, one thing should be emphasized that the evaluation time for the WDDL-based testbench accounts about 6-7 times of the FPL/SC-based testbench because of the alternation of precharge signals and real signals when propagating.

APPENDIX C
FPL-BASED MODULES WITHOUT COMPENSATORY UNIT

In addition, we have also performed a CPA analysis on the FPL implementations of PRESENT/AES-SBox modules without CU by 32/256 power traces. Here we employ the same keys as the experiment of SC implementations. The attack results are demonstrated in Fig. 16. The correlations of the various key hypotheses corresponding to the number of power

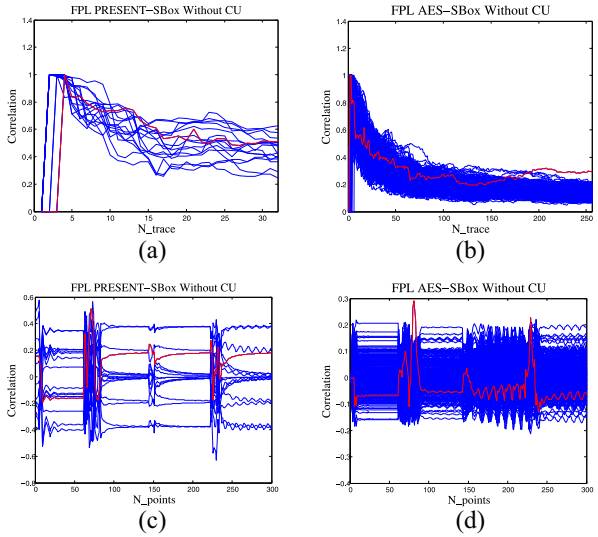


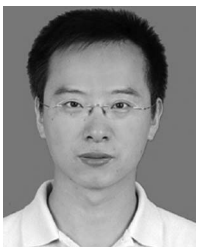
Fig. 16. CPA of FPL-based PRESENT/AES-SBox modules without CU. (a) Correlation versus No. of traces. (b) Correlation versus No. of traces. (c) Correlation versus length of a trace. (d) Correlation versus length of a trace.

traces (N_{trace}) are, respectively, plotted in Fig. 16(a) and (b), which shows that the FPL logic without CU can still protect PRESENT-SBox module to some extent, while the security of AES-SBox module is weakened compared with the implementations with CU. Especially, it requires about 190 traces to reveal the secret keys of the AES-SBox module.

REFERENCES

[1] K. Ly and Y. Jin, "Security challenges in CPS and IoT: From end-node to the system," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, 2016, pp. 63–68.
[2] W. He, J. Breier, S. Bhasin, and A. Chattopadhyay, "Bypassing parity protected cryptography using laser fault injection in cyber-physical system," in *Proc. 2nd ACM Int. Workshop Cyber Phys. Syst. Security*, 2016, pp. 15–21.
[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.*, 1999, pp. 388–397.
[4] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2004, pp. 16–29.
[5] N. H. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective*. Upper Saddle River, NJ, USA: Pearson Educ. India, 2015.
[6] K. Roy and S. C. Prasad, *Low-Power CMOS VLSI Circuit Design*. New York, NY, USA: Wiley, 2009.
[7] P. Saravanan and P. Kalpana, "An energy efficient XOR gate implementation resistant to power analysis attacks," *J. Eng. Sci. Technol*, vol. 10, no. 1, pp. 1275–1292, 2015.
[8] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, vol. 31. New York, NY, USA: Springer, 2008.
[9] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2011, pp. 33–48.
[10] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. IEEE Design Autom. Test Europe Conf. Exhibit.*, vol. 1, 2004, pp. 246–251.
[11] M. Nassar, S. Bhasin, J.-L. Danger, G. Duc, and S. Guilley, "BCDL: A high speed balanced DPL for FPGA with global precharge and no early evaluation," in *Proc. IEEE Design Autom. Test Europe Conf. Exhibit. (DATE)*, 2010, pp. 849–854.
[12] F. Bouesse, G. Sicard, and M. Renaudin, "Path swapping method to improve DPA resistance of quasi delay insensitive asynchronous circuits," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2006, pp. 384–398.

[13] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2001, pp. 309–318.
[14] E. Prouff and M. Rivain, "Masking against side-channel attacks: A formal security proof," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2013, pp. 142–159.
[15] L. Geng *et al.*, "Transistor level SCA-resistant scheme based on fluctuating power logic," *Sci. China Inf. Sci.*, vol. 60, no. 10, 2017, Art. no. 109401.
[16] F. Zhang *et al.*, "Fluctuating power logic: SCA protection by VDD randomization at the cell-level," in *Proc. IEEE Asian Hardw. Orient. Security Trust Symp. (AsianHOST)*, 2019, pp. 1–6.
[17] H. Kawaguchi and T. Sakurai, "A reduced clock-swing flip-flop (RCSFF) for 63% power reduction," *IEEE J. Solid-State Circuits*, vol. 33, no. 5, pp. 807–811, Mar. 1998.
[18] R. P. McEvoy, C. C. Murphy, W. P. Marnane, and M. Tunstall, "Isolated WDDL: A hiding countermeasure for differential power analysis on FPGAs," *ACM Trans. Reconfig. Technol. Syst.*, vol. 2, no. 1, pp. 1–23, 2009.
[19] P. Wang, Y. Zhang, and X. Zhang, "Design of two-phase SABL flip-flop for resistant DPA attacks," *Chin. J. Electron.*, vol. 22, no. 4, pp. 833–837, 2013.
[20] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. IEEE 28th Eur. Solid-State Circuits Conf.*, 2002, pp. 403–406.
[21] V. Telandro, E. Kussener, A. Malherbe, and H. Barthelemy, "On-chip voltage regulator protecting against power analysis attacks," in *Proc. 49th IEEE Int. Midwest Symp. Circuits Syst.*, vol. 2, 2006, pp. 507–511.
[22] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *Proc. 20th Int. Conf. VLSI Design 6th Int. Conf. Embedded Syst. (VLSID)*, 2007, pp. 854–862.
[23] D. Kamel *et al.*, "Towards securing low-power digital circuits with ultra-low-voltage vdd randomizers," in *Proc. Int. Conf. Security Privacy Appl. Cryptography Eng.*, 2016, pp. 233–248.
[24] P. Zhao, T. K. Darwish, and M. A. Bayoumi, "High-performance and low-power conditional discharge flip-flop," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 12, no. 5, pp. 477–484, May 2004.
[25] V. Stojanovic and V. G. Oklobdzija, "Comparative analysis of master–slave latches and flip-flops for high-performance and low-power systems," *IEEE J. Solid-State Circuits*, vol. 34, no. 4, pp. 536–548, Jan. 1999.
[26] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2007, pp. 450–466.
[27] J. Daemen and V. Rijmen, "Reijndael: The advanced encryption standard," *Dr. Dobb's J. Softw. Tools Prof. Program.*, vol. 26, no. 3, pp. 137–139, 2001.
[28] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2008, pp. 426–442.
[29] B. J. G. Goodwill *et al.*, "A testing methodology for side-channel resistance validation," in *Proc. NIST Noninvasive Attack Test. Workshop*, vol. 7, 2011, pp. 115–136.
[30] T. Schneider and A. Moradi, "Leakage assessment methodology," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2015, pp. 495–513.



Fan Zhang received the B.S. degree in 2001, the M.S. degree in 2004, and the Ph.D. degree from the Department of Computer Science and Engineering, University of Connecticut, Mansfield, CT, USA, in 2011.

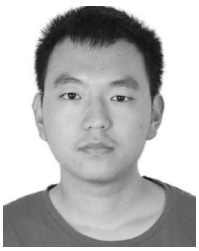
He is an Associate Professor with the School of Cyber Science and Technology, College of Computer Science and Technology, Zhejiang University, Hangzhou, China, and affiliated with the College of Information Science and Electronic Engineering, Zhejiang University. His research interests include hardware security, system security, cryptography, and computer architecture.

Bolin Yang (Student Member, IEEE) received the bachelor's degree from the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China, in 2019, where he is currently pursuing the Ph.D. degree.

His research interests include hardware security and post quantum cryptography.

Bojie Yang received the bachelor's degree in microelectronic science and engineering from Zhejiang University, Hangzhou, China, in 2020, where she is currently pursuing the Ph.D. degree with the School of Cyber Science and Technology.

Her current research focuses on high-speed implementation of cryptographic algorithm.



Yiran Zhang (Student Member, IEEE) received the bachelor's degree from Zhejiang University, Hangzhou, China, in June 2018, where he is currently pursuing the master's degree with the College of Information Science and Electronic Engineering.

His research mainly focuses on the hardware security.

Xuanle Ren received the B.S. degree in microelectronics from Peking University, Beijing, China, in 2012, and the Ph.D. degree in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA, USA, in 2018.

He is currently working as a Research Scientist with Alibaba Group, Hangzhou, China. His research is focused on design of secure computer architecture and hardware security.

Shivam Bhasin (Member, IEEE) received the bachelor's degree from UP Tech, India, in 2007, the master's degree from Mines Saint-Etienne, Saint-Étienne, France, in 2008, and the Ph.D. degree from Telecom ParisTech, Paris, France, in 2011.

He held the position of Research Engineer with Institut Mines-Telecom, Paris. He was also a Visiting Researcher with Université Catholique de Louvain, Ottignies-Louvain-la-Neuve, Belgium, in 2011 and Kobe University, Kobe, Japan, in 2013. He has been a Senior Research Scientist and a Principal Investigator with PACE Labs, Nanyang Technical University, Singapore, since 2015. His research interests include embedded security, trusted computing, and secure designs.

Kui Ren (Fellow, IEEE) received the B.S. degree in 1998, the M.S. degree in 2001, and the Ph.D. degree from Worcester Polytechnic Institute, Worcester, MA, USA, in 2007.

He is currently a Professor of Computer Science and Technology and the Director of the Institute of Cyberspace Research with Zhejiang University, Hangzhou, China. His current research interest spans cloud and outsourcing security, wireless and wearable system security, and artificial intelligence security.

Prof. Ren was a recipient of the IEEE CISTC Technical Recognition Award in 2017 and the NSF CAREER Award in 2011. He is a Distinguished Scientist of ACM.