Fluctuating Power Logic: SCA Protection by V_{DD} Randomization at the Cell-level

Fan Zhang[*][†][‡][§], Bolin Yang[§], Bojie Yang[§][*], Yiran Zhang[§][‡], Shivam Bhasin[¶] and Kui Ren[*][‡]
[*]School of Cyber Science & Technology, College of Compute Science and Technology, Zhejiang University, Hangzhou, 310027, China
[†]State Key Laboratory of Cryptology, P.O.Box 5159, Beijing, 100878, China
[‡]Alibaba-Zhejiang University Joint Institute of Frontier Technologies, Zhejiang University, Hangzhou, 310027, China
[§]College of Information Science & Electronic Engineering, Zhejiang University, Hangzhou, 310027, China
[¶]Temasek Laboratories, Nanyang Technological University, 637371, Singapore
Corresponding Author: Bojie Yang, email: yangbojie@zju.edu.cn

***Abstract*—In this paper, we propose a novel cell-level side channel countermeasure *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. HSPICE based simulation results show that the modified flip-flop is resistant against power analysis at the cost of doubled power dissipation. Two illustrative case studies of PRESENT and AES substitutions have been explored. The resistance against Side-Channel Analysis(SCA) is evaluated by the correlation power analysis. 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 SCA such as electromagnetic analysis.**

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. 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 side-channel attack approaches, which includes simple power analysis (SPA), differential power analysis (DPA) [3], correlation power analysis (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 non-invasive manner [7]. The dependency can be approximately described by a power model such as the Hamming weight (HW) or the Hamming distance (HD) model. Then the adversary can extract the secrets with side-channel information and these leakage models. Since the power analysis 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, 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 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 difficult to implement in practice.

Masking [12] is an algorithm level countermeasure which attempts to de-correlate the dependency between the actual data and the power model. The key-dependent variables are actually masked with random and unknown values. This is one of the most widely studied countermeasures in the research community and comes with a formal proof of security [13]. Masking countermeasures can be more effective in the presence of high noise that one will see a big difference in leakages between unprotected and masked versions. Therefore, the following research direction leads towards effective noise generation circuits which can enhance the security of masking.

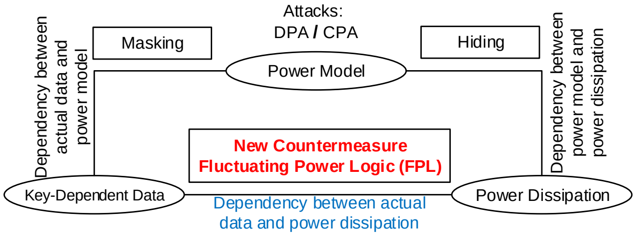

Attacks:
DPA / CPA
Masking
Hiding
Power Model
Dependency between actual data and power model
Dependency between power model and power dissipation
New Countermeasure
Fluctuating Power Logic (FPL)
Key-Dependent Data
Power Dissipation
Dependency between actual data and power dissipation

Fig. 1. Concept of the proposed FPL countermeasure.

In this paper, we deal with the noise generation problem at the transistor-level. The key motivation of this paper is to pursue a new type of countermeasure which, at the cell level, can remove the dependence between the actual data and the physical 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.

978-1-7281-3544-1/19/$31.00 © 2019 IEEE

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 concept was mentioned in [14]. Cryptographic circuits built with FPL cells have natural (although bounded) side-channel resistance. FPL cells can be used to implement masked algorithms to further elevate their security levels.

A. Related Work

At the cell level, hiding countermeasures adopt the form of secure logic styles with constant power consumption, most of which are typically implemented as dual-rail precharge (DRP) circuits [10], [15], [16], [17]. 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. In [9], authors proposed several generic designs for noise generators exploiting shift registers, block RAM write conflicts, clock randomization, etc. However, all these noise generators are acting independently to the sensitive circuits. Thus, advanced filtering and signal processing methods can be deployed to remove such added noise. In [18], 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 [19] to reduce correlation between VDD and the power model. A thorough security evaluation of such VDD randomizer was recently published in [20]. Authors concluded that such randomization of voltage can be seen as a sound noise generator which can be further exploited to strengthen mathematical countermeasures like masking. In all, 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

In this paper, a novel cell-level logic, named as *fluctuating power logic* (FPL), is presented for randomly fluctuating the power consumption of fixed data transitions. Since the conventional power model cannot reflect the actual dissipation, it is therefore considered to be SCA-resistant. Compared to the SABL and WDDL logics which require high level of balanced output capacitive loads, our proposed logic further alleviates this shortcoming.

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%) [21]. FFs are also the normal target of SCA due to the synchronized power consumption. The proposed logic is highlighted with a modified secure FF. Furthermore, to enhance the logic to be DPA resistant, a compensatory unit is appended, making the average power consumption of variant and invariant data transitions indistinguishable. The proposed logic is analyzed for side-channel security by practical attacks on PRESENT/AES-SBox modules implemented in FPL. FPL is also compared with standard-cell-based and WDDL-based implementations, so as to further verify our scheme in terms of security, area, power, etc.

C. Organization

The rest of this paper is organized as follows. The FPL scheme and its secure flip-flop implementation are introduced in Section II and III, respectively. In Section IV, two illustrative case studies, which are evaluated with correlation power analysis to demonstrate the security of the proposed method. Conclusions are drawn in Section V.

II. Proposed Logic

In this section, a novel SCA-resistant cell-level logic is proposed and implemented. This scheme is based on a *cascade voltage logic* (CVL) and further enhanced with a *compensatory unit* (CU).

A. Basic CVL Unit

Fig. 2 shows the schematic of the cascade voltage logic (CVL). The CVL unit mainly consists of four components: n NMOS, n diodes (D_i), one PMOS and 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). Furthermore, the bulk and source terminals of every NMOS are connected, so that the bulk effect can be avoided. A diode is inserted between every parallel NMOS transistor and VDD_m terminal, so that each of NMOS transistors 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 controls the PMOS transistor. Each parallel rail in CVL unit consists of one LVT-NMOS and one LVT-diode, acting as an active resistance to produce a voltage drop

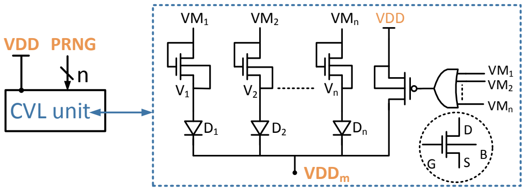


Fig. 2. The schematic of CVL unit.

if both are turned on. When a LVT-NMOS transistor is turned on, it produces a voltage drop from the source port to the drain port, whose value equals to 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 and that of all rails as R_a. Each rail contributes to the overall current drawn from the source voltage, resulting in variant powers.

Suppose k denotes the total number of VM_i whose value is 1 ($k = \sum_{i=1}^{n} VM_i, 0 \le k \le n$). 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 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 $1 < k \le n$.

B. Proposed FPL Scheme

Fig. 3 shows the design of the proposed scheme, named as *fluctuating power logic* (FPL). It consists of three parts: PRNG, CVL unit and 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 behaviour 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 non-critical 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.

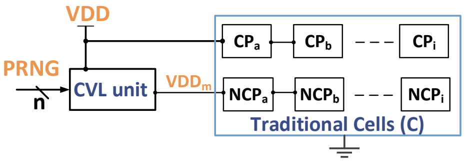


Fig. 3. The design of FPL logic with CVL unit.

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 flip-flops (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 flip-flops and the last sections of the clock distribution network [21]. 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 [22]. In this paper, we treat CDFF as a standard-cell-based FF (SC-FF).

B. Modified FF with FPL

In Fig. 4, we now show how to apply FPL to a SC-FF [22]. This illustration is named as FPL-FF, which is similar to the extension work of dual-rail precharge based FFs, such as SABL-FF or WDDL-FF in [8]. In Fig. 4, 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 non-critical paths in SC-FF consist of four main components: clock-path (NCP_a), pull-up network (NCP_b), double feed-back unit (NCP_c) and $D - DB$ inverter (NCP_d), which are marked in Fig. 4. For example, the inverters in the clock path NCP_a are only for the purpose of providing certain delayed clock signal. In Fig. 4, those MOS transistors connected to VDD_m are highlighted in the grey shaded area.

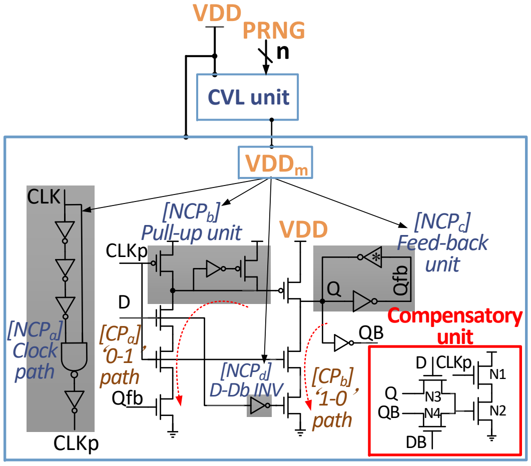


Fig. 4. Illustration of standard Flip-Flop under FPL scheme.

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 ($k \ge 1$), 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 non-critical paths for variant transitions. As a result, FPL has little negative effect on the total delay of FF after the modification.

C. Compensatory Unit (CU)

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 FPL scheme alone, while the horizontal power properties in a fixed power step may still be statistically distinguishable by DPA.

To alleviate this contradiction, we append a *compensatory unit* (CU) to enhance its DPA-resistance, as highlighted in the red box of Fig. 4. 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 aforementioned, the total power of FPL-FF (P_{total}) consists of three parts: the power of original FF (P_{FF}), the power of CVL unit (P_{CVL}) and 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. Case Studies —PRESENT/AES Encryption

In order to testify the effectiveness of the designs introduced 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 [23]. The results are obtained from HSPICE in the SMIC 65nm CMOS technology at room temperature, and $VDD = 1.2V$. We assume all the NMOS transistors in the CVL unit are of the same size throughout this paper.

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

In this section, we take PRESENT and AES as illustrative examples to evaluate the effectiveness of the proposed FPL scheme. For the simplicity, we only focus on the non-linear 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 behaviour of the target logic.

A. Implementation and Cost

AES [24] is a symmetric cipher standardized in 2001 by NIST as a formal successor of preceding DES. PRESENT is an ultra-lightweight block cipher proposed in 2007 [25], which can be efficiently implemented in low cost hardware. The non-linear 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 consists of two 4/8-bit input registers (Data, 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 1.2V. The load capacitances to the output nodes are 3fF. The setup is working as a simplified testbed. Key is unknown thus requiring the power analysis 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.

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 in 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, a realization of 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 whole 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 implemented with WDDL [10] logic are also realized.

In Table. I, the results for the two circuits covering area, performance and power dissipation overhead are summarized. To be specific, the Gate equivalents (GE) of SC-, FPL- and WDDL-based testbench implementations are summarized in the first row of Table. I. Here, one GE represents area of one NAND gate. In Table. I, 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. I 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

TABLE I

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

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

Numerous evaluation tools have been proposed in prior literatures for evaluating the side-channel vulnerabilities, such as correlation power analysis (CPA) [4], and test-vector-leakage-assessment (TVLA) [26], etc.

CPA is the most common method to estimate the linear relationship between power models and real power traces [4]. The hypothetical power consumption in CPA, denoted as H, was set to the Hamming weight 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: $\rho_{WH} = \frac{cov(W,H)}{\sigma_W \sigma_H}$ 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 j-th key hypothesis with N traces:

$$\hat{\rho}_{WH_j} = \frac{N\sum_1^N W_i H_{i,j} - \sum_1^N W_i \sum_1^N H_{i,j}}{\sqrt{N\sum_1^N W_i^2 - (\sum_1^N W_i)^2}\sqrt{N\sum_1^N H_{i,j}^2 - (\sum_1^N H_{i,j})^2}} \tag{1}$$

In Eq.(1), 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 most correlation.

C. Experimental Results

We evaluate the security of standard-cell-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. 5a and Fig. 5b for PRESENT and AES, respectively. When $N_{trace} \geq N_{MTD}$, the coefficient curve for the correct hypothesis will be always above those for wrong hypotheses. $N_{MTD} \approx 12$ for PRESENT as shown in Fig. 5a and $N_{MTD} \approx 22$ for AES in Fig. 5b. The correlations of the various key hypotheses corresponding to the length of the trace (N_{points}) are shown in Fig. 5c and Fig. 5d. 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 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 better comparison, the attack results are also demonstrated in Fig. 5. In Fig. 5e, the curve for the correct hypothesis is buried among all other curves and can not be distinguished. In Fig. 5g, there is no peak observed, therefore CPA on FPL-based PRESENT is considered as fail. In Fig. 5f, $N_{MTD} \approx 250$ for FPL-based AES, which is about 10 times of that for SC-based AES. The FPL logic greatly boosts the security of AES-SBox module. Unlike real measurement, the results from the precise simulation will not change with more measurements.

Furthermore, by observing Fig. 5c-5d and Fig. 5g-5h, we find that 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 found that the expected security escalation from the proposed FPL enhancement has been achieved in comparison with SC-based implementations.

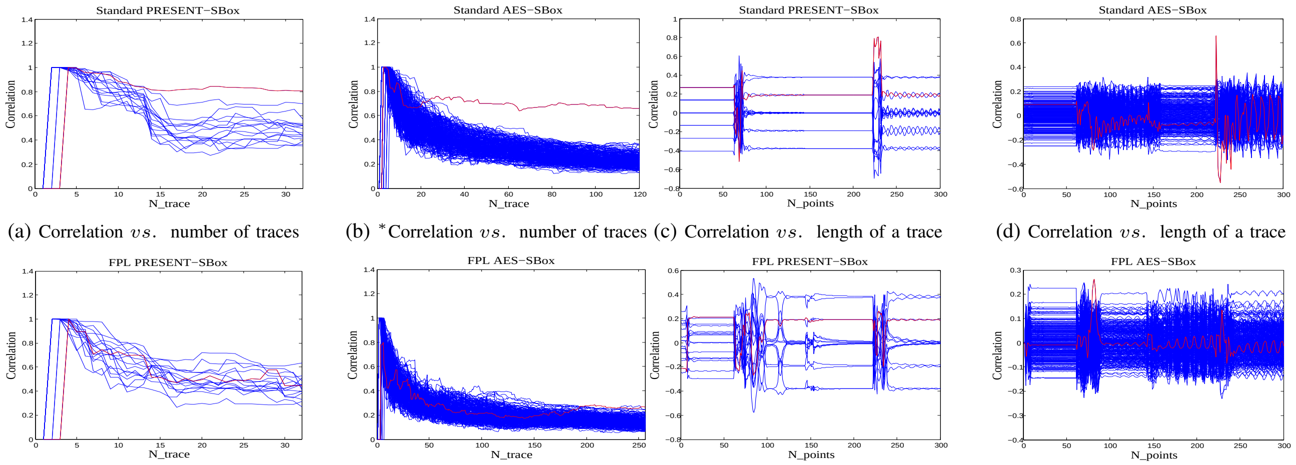
V. CONCLUSIONS

In this paper, we proposed a power-diffusing logic named as fluctuating power logic (FPL), which employs the cascade voltage logic (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 using FPL. The cell-level experimental results show that the FPL scheme provides elevated security level against generic power-based side-channel analysis.

ACKNOWLEDGMENT

This work was supported in part by Alibaba-Zhejiang University Joint Institute of Frontier Technologies, by Zhejiang Key R&D Plan (Grant No. 2019C03133), by Major Scientific Research Project of Zhejiang Lab (Grant No. 2018FD0ZX01), by Open Fund of State Key Laboratory of Cryptology (Grant No. MMKFKT201805), by the

*Source figures from [14].



(a) Correlation $vs.$ number of traces (b) *Correlation $vs.$ number of traces (c) Correlation $vs.$ length of a trace (d) Correlation $vs.$ length of a trace

(e) Correlation $vs.$ number of traces (f) *Correlation $vs.$ number of traces (g) Correlation $vs.$ length of a trace (h) Correlation $vs.$ length of a trace

Fig. 5. CPA results of standard PRESENT/AES-SBox modules.

National Natural Science Foundation of China (Grant No. 61772236, 61972348), by Young Elite Scientists Sponsorship Program by CAST (Grant No. 17-JCJQ-QT-045) and by Research Institute of Cyberspace Governance in Zhejiang University.

References

[1] K. Ly and Y. Jin, “Security challenges in cps and iot: from end-node to the system,” in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 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 *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*. ACM, 2016, pp. 15–21.

[3] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[4] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2004, pp. 16–29.

[5] N. H. Weste and D. Harris, *CMOS VLSI design: a circuits and systems perspective*. Pearson Education India, 2015.

[6] K. Roy and S. C. Prasad, *Low-power CMOS VLSI circuit design*. John Wiley & Sons, 2009.

[7] P. Saravanan and P. Kalpana, “An energy efficient xor gate implementation resistant to power analysis attacks,” *J. Eng. Sci. Technol*, vol. 10, pp. 1275–1292, 2015.

[8] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008, vol. 31.

[9] T. Güneysu and A. Moradi, “Generic side-channel countermeasures for reconfigurable devices,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 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 *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 1. IEEE, 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 *Proceedings of the Conference on Design, Automation and Test in Europe*. European Design and Automation Association, 2010, pp. 849–854.

[12] M.-L. Akkar and C. Giraud, “An implementation of des and aes, secure against some attacks,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2001, pp. 309–318.

[13] E. Prouff and M. Rivain, “Masking against side-channel attacks: A formal security proof,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2013, pp. 142–159.

[14] L. Geng, F. Zhang, J. Shen, W. He, S. Bhasin, X. Zhao, and S. Guo, “Transistor level sca-resistant scheme based on fluctuating power logic,” *Science China Information Sciences*, vol. 60, no. 10, pp. 270–272, 2017.

[15] R. P. McEvoy, C. C. Murphy, W. P. Marnane, and M. Tunstall, “Isolated wddl: a hiding countermeasure for differential power analysis on fpgas,” *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 2, no. 1, pp. 1–3, 2009.

[16] P. Wang, Y. Zhang, and X. Zhang, “Design of two-phase sabl flip-flop for resistant dpa attacks,” *Chinese Journal of Electronics*, vol. 22, no. 4, pp. 833–837, 2013.

[17] 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 *Proceedings of the 28th European solid-state circuits conference*. IEEE, 2002, pp. 403–406.

[18] V. Telandro, E. Kussener, A. Malherbe, and H. Barthelemy, “On-chip voltage regulator protecting against power analysis attacks,” in *2006 49th IEEE International Midwest Symposium on Circuits and Systems*, vol. 2. IEEE, 2006, pp. 507–511.

[19] K. Baddam and M. Zwolinski, “Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure,” in *20th International Conference on VLSI Design held jointly with 6th International Conference on Embedded Systems (VLSID’07)*. IEEE, 2007, pp. 854–862.

[20] F.-X. Standaert, D. Flandre, and D. Bol, “Towards securing low-power digital circuits with ultra-low-voltage vdd randomizers,” in *Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings*, vol. 10076. Springer, 2016, pp. 233–248.

[21] H. Kawaguchi and T. Sakurai, “A reduced clock-swing flip-flop (rcsff) for 63% power reduction,” *IEEE Journal of Solid-State Circuits*, vol. 33, no. 5, pp. 807–811, 1998.

[22] P. Zhao, T. K. Darwish, and M. A. Bayoumi, “High-performance and low-power conditional discharge flip-flop,” *IEEE transactions on very large scale integration (VLSI) systems*, vol. 12, no. 5, pp. 477–484, 2004.

[23] V. Stojanovic and V. G. Oklobdzija, “Comparative analysis of master-slave latches and flip-flops for high-performance and low-power systems,” *IEEE Journal of solid-state circuits*, vol. 34, no. 4, pp. 536–548, 1999.

[24] V. Rijmen and J. Daemen, “Advanced encryption standard,” *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, pp. 19–22, 2001.

[25] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, “Present: An ultra-lightweight block cipher,” in *International workshop on cryptographic hardware and embedded systems*. Springer, 2007, pp. 450–466.

[26] B. J. Gilbert Goodwill, J. Jaffe, P. Rohatgi *et al.*, “A testing methodology for side-channel resistance validation,” in *NIST non-invasive attack testing workshop*, vol. 7, 2011, pp. 115–136.