SCIENCE CHINA
Information Sciences

• LETTER •

October 2017, Vol. 60 109401:1–109401:3
doi: 10.1007/s11432-016-9046-4

Transistor level SCA-resistant scheme based on fluctuating power logic

Liang GENG[1], Fan ZHANG[1,2*], Jizhong SHEN[1], Wei HE[3], Shivam BHASIN[3], Xinjie ZHAO[4] & Shize GUO[4]

[1]*College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou* 310027*, China;*
[2]*Science and Technology on Communication Security Laboratory, Chengdu* 610041*, China;*
[3]*Temasek Laboratories, Nanyang Technological University, Singapore* 637371*, Singapore;*
[4]*The Institute of North Electronic Equipment, Beijing* 100191*, China*

Received December 10, 2016; accepted February 23, 2017; published online July 28, 2017

Citation Geng L, Zhang F, Shen J Z, et al. Transistor level SCA-resistant scheme based on fluctuating power logic. Sci China Inf Sci, 2017, 60(10): 109401, doi: 10.1007/s11432-016-9046-4

Dear editor,

The main objective of side-channel analysis (SCA) is to extract the secret key using physical leakages from underlying fundamental logic elements. Power analysis (PA) is one type of SCA, such as simple power analysis (SPA), differential power analysis (DPA) and correlation power analysis (CPA), which relies on the fact that the power dissipation of hardware is correlated to its switching activity, and associates with the key-dependent data being processed [1]. Since PA brings serious threats to modern circuits, there is an urgent need for effective SCA countermeasures for constructing secure crypto systems. Two mainstream cell-level approaches have been proposed in prior literature to counter SCA: hiding and masking. The former is to hide the actual data into indistinguishable power patterns, which diffuses (or even removes) the dependency between the power model and the physical dissipation, such as wave dynamic differential logic (WDDL) [2]. The latter involves masking the key dependent data with random variables, which attempts to decorrelate the dependency between the actual data and the power model mainly at algorithmic or gate level.

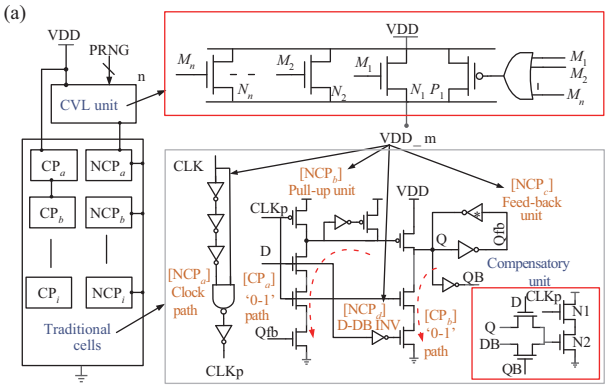
However, both masking and hiding techniques rely on a well known fact that the power consumptions for some data transitions are constantly distinguishable from other transitions [3]. Specifically in Hamming Distance model (HD), variant data transitions, e.g., $0 \rightarrow 1$ or $1 \rightarrow 0$, consume more power than invariant ones such as $0 \rightarrow 0$ or $1 \rightarrow 1$.

In this letter, a novel logic, named fluctuating power logic (FPL), is proposed for fluctuating the power fingerprint for some fixed data transitions. Therefore, the traditional power model cannot reflect the dependency between actual power dissipation and intermediate data transitions, hence making FPL-fortified cipher more difficult to be attacked.

First, a specially designed unit, named cascade voltage logic (CVL), is constructed with three components: n NMOS (N_i), one PMOS and one "n-input" OR gate, as shown at the top of Figure 1(a). The NMOS transistors and the OR-gate are controlled by random signals M_i and the PMOS transistor is controlled by the output of OR-gate. The components in the original circuit can be split into two parts, as shown at the right bottom of Figure 1(a), i.e., those on and off the critical paths denoted as CP_i and NCP_i, respectively. Each NMOS transistor in CVL acts as an

* Corresponding author (email: fanzhang@zju.edu.cn)

The authors declare that they have no conflict of interest.



(b)

n	k	$P_{00}^{n,k}$ (0→0)	$P_{01}^{n,k}$ (0→1)	$P_{10}^{n,k}$ (1→0)	$P_{11}^{n,k}$ (1→1)	Δ_n
0	0	2.756	4.931	3.912	2.669	0.237
1	0	2.74(5.83)	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)	

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

Figure 1 (Color online) (a) Illustration of standard Flip-Flop under FPL scheme; (b) power comparisons of FPL-FF at various conditions (μW).

active resistance, producing a voltage drop when turned on, which just associates with its size (W and L). Denote the equivalent resistance for each and all NMOS as R_i and R_a ($1 \leqslant i \leqslant n$), respectively. Without loss of generality, we can assume all NMOSs have the same sizes thus $R_i = R_c$. Each NMOS contributes to the overall current drawn from the source voltage, making power fluctuating. Suppose k denotes the number of M_i whose value is one ($1 \leqslant i, k \leqslant n$). The voltage drop over CVL is denoted as V_{dp}. Depending on k, there are three cases:

(1) $k = 0$, i.e., all $M_i = 0$. All NMOS transistors are shut off and the OR gate outputs a digital '0', which turns on the PMOS transistor with no voltage drop, thus $V_{dp} = 0$.

(2) $k = 1$, i.e., only one of M_i is 1. The NMOS transistor controlled by $M_i = 1$ is the only conducting path, thus $V_{dp} = V_{th}$.

(3) $k > 1$, i.e., more than one NMOS transistors are turned on. The CVL unit consists of k parallel resistors. If $R_i = R_c$, then $R_a = R_c/k$, thus $0 < V_{dp} < V_{th}$.

The proposed FPL scheme applies CVL to construct a SCA-resistant circuit whose logical behavior stays unchanged. Note that the speed of CMOS transistors becomes slow when they work at sub-voltage environment, therefore the delay behavior of the entire circuit highly depends on the voltage of sequential elements. So the CVL serves as a functional unit and is only inserted between the normal source voltage and those components along the non-critical paths, i.e., NCP_i. An n-bit pseudo random number generator (PRNG) generates all M_i for CVL. It should be noted that all components in NCP_i are connected to the sole CVL and powered by VDD_m ($\mathrm{VDD} - V_{dp}$). When $k > 1$, the power consumption of the whole FPL circuit is fluctuating with the varying value of k.

Depending on the values of k, there are different values of R_a and V_{dp}, resulting in different discrete values of power consumption for the whole FPL circuit. More precisely, we define a power metric for FPL-FF named power step, which is the number of all possible dynamic power values for each data transition when n is fixed. The number of possible power steps is denoted as N. If all NMOS transistors are of the same sizes, $N = O(n)$. VDD_m can get $(n + 1)$ values discretely distributed between VDD and $(\mathrm{VDD} - V_{th})$. Importantly, N can be as high as $O(2^n)$ only if the values of each R_i are properly tuned to be different for all these NMOS transistors in the CVL unit. Therefore, the fluctuating power characteristic of FPL makes power analysis much more difficult or even impossible in practice.

It is established that the major power consumption of a digital circuit stems from the global clock network and Flip-Flops (FFs) (estimated 30%–60%) [4]. FFs are also the preferred target of SCA due to the synchronized power consumption. We now give an illustration of how to apply FPL to a standard flip-flop (SFF) [5], named FPL-FF. In order to keep the performance of the FF behaving as normal, the CVL unit is only applied to the logical components that are off the critical paths, which consist of four main components: clock-path (NCP_a), pull-up transistor (NCP_b), double feedback unit (NCP_c) and D-DB inverter (NCP_d), as highlighted in Figure 1(a). CP_a and CP_b are two components on the critical paths for $0 \to 1$ and $1 \to 0$ transitions respectively.

Generally, the power consumption for variant data transitions in a basic circuit is larger than that for invariant ones, which forms the basis of DPA. Consequently, we append a compensatory unit (CU) to improve its DPA-resistance, as shown in Figure 1(a). When the input D makes a $0 \to 1$

or $1 \to 0$ transition, the CU is shut down. Otherwise, it consumes compensatory dynamic power.

The results are obtained from HSPICE transient simulation (Version: C-2009.09) using the SMIC 65 nm CMOS technology at room temperature and VDD = 1.2 V. The simulation results of original SFF and the modified FPL-FF are shown in Figure 1(b). Here, (n, k) denotes the number of M_i and the number of M_i equalling 1. In Figure 1(b), $n = 0$ stands for SFF and each row shows the power of four different transitions in the same step. The data out-of (in) the parentheses is the result of FPL-FF without (with) the CU. 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). B_n^k is the binomial coefficient for choosing k from n. The last column denoted as Δ_n calculates the statistical power difference between variant and invariant transitions over all possible k, which can be directly exploited by SCA.

There are several observations drawn from the simulation results.

(i) When $n > 1$, there are $n + 1$ power steps for the same data transition varying with the random number k (for both without or with the CU).

(ii) For specific n in FPL-FF, the ranges of total power for different data 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.

(iii) Even for the same group of (n, k), invariant transitions may consume more power than variant ones due to the introduced glitchy noise. For instance, $P_{00}^{4,1} = 5.61(9.55)$ μW while $P_{01}^{4,1} = 5.16(8.80)$ μW.

(iv) With the compensation of the CU, the statistical power difference between variant and invariant transitions is significantly reduced.

Obviously, the dependency of fluctuating power on a common HW (HD) model of different data transitions is totally diffused, which makes it difficult for an adversary to distinguish variant transitions from invariant ones. Compared to the intrinsic difference of SFF, the Δ_n of FPL-FF is reduced from 0.237 to 0.009 when $n = 4$. Δ_n with CU is reduced by a factor of 4 to 13 in comparison to that without CU. In other words, the difficulty of launching a successful DPA can be significantly increased, at the expense of only a doubled power consumption, which is more competitive than the counterpart WDDL. In the real deployment, there are slight differences among those theoretically equivalent resistances even when all NMOS transistors are of the same sizes. Furthermore, if NMOS is properly tuned, the power steps can be further increased by reaching $O(2^n)$.

To evaluate how the proposed FPL scheme mitigates power analysis attacks and how it is compared with standard-cell (SC) logic, experiments are carried out on a complete implementation of the module of AES SBox lookup table. This work is detailed in the supplementary file.

The CPA attack results show that with about 22 power traces SC based implementation can be successfully attacked while it needs over 250 power traces to reveal the secret keys (with low stability) of the FPL-based module. Furthermore, proposed FPL can also be combined to traditional cell-level countermeasures, bringing in a random variable in an extra dimension, to get higher security.

To conclude, apart from the traditional cell-level hiding and masking countermeasures, we propose an innovative breakthrough — fluctuating power logic (FPL) in this paper, which diffuses the intrinsic correlations between the real power and the fixed data transitions by employing cascade voltage logic (CVL). In addition, a compensatory unit (CU) can be merged into the design for enhancing the DPA-resistance of FPL-based circuits. The escalated security is certified by simulated power CPA, by applying the proposed scheme to a standard FF and an SBox module.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61173191, 61272491, 61309021, 61472357, 61571063), National Basic Research Program of China (973 Program) (Grant No. 2013CB338004), and Science and Technology on Communication Security Laboratory (Grant No. 9140C110602150C11053).

Supporting information Appendix A. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Saravanan P, Kalpana P. An energy efficient XOR gate implementation resistant to power analysis attacks. J Eng Sci Tech, 2015, 10: 1275–1292
2 Mangard S, Oswald E, Popp T. Power Analysis Attacks: Revealing the Secrets of Smart Cards. Berlin: Springer Science & Business Media, 2008
3 Moradi A, Kirschbaum M, Eisenbarth T, et al. Masked dual-rail precharge logic encounters state-of-the-art power analysis methods. IEEE Trans Very Large Scale Integr Syst, 2012, 20: 1578–1589
4 Kawaguchi H, Sakurai T. A reduced clock-swing flip-flop (RCSFF) for 63% power reduction. IEEE J Solid-State Circ, 1998, 33: 807–811
5 Zhao P, Darwish T, Bayoumi M. High-performance and low power conditional discharge flip-flop. IEEE Trans Very Large Scale Integr Syst, 2004, 12: 477–484