Dynamic current mode logic based flip-flop design for robust and low-power security integrated circuits

Jizhong Shen✉, Liang Geng and Fan Zhang

Side-channel analysis (SCA) is a powerful technique to reveal the secrets using detectable physical leakages from logic elements, which brings severe security threats to modern circuits. To alleviate this problem, applying cell-level countermeasure is usually a suitable solution, which is mainly implemented as dual-rail precharge logic. Mace *et al.* has the proposed dynamic current mode logic (DyCML) scheme as a novel technology to resist SCA, whose power consumption is constant regardless of the data processed. However, the DyCML-based sequential elements are still in blank field. So, we have implemented a novel flip-flop compatible with DyCML, whose enhanced security has been proved by corresponding simulations.

Introduction: Cryptographic technologies and secure implementations of cryptographic algorithms have been widely used in the field of information security, especially in the applications of Internet of things and cyber–physical systems [1]. Under the circumstances, Kocher *et al.* has the proposed side-channel analysis (SCA), which is a powerful and efficient technique aiming to reveal the secrets using detectable physical leakages from underlying fundamental logic elements [2]. Among various SCA attack approaches, power analysis (PA) is the most typical one, which relies on the fact that the power dissipation of hardware implementations of cryptographic modules inherently correlate to the key-dependent data being processed in a non-invasive mode [3].

Since PA attacks are quite simple and convenient to carry out, and more efficient than mathematical based attacks, there is consequently an urgent need for putting forward effective SCA countermeasures. A straightforward way to counter PA at cell level is to make the cryptographic module implemented in a logic, whose power consumption is independent of the operated data transitions. Examples are dual-rail precharge (DRP) logics such as sense-amplifier-based logic (SABL) and wave dynamic differential logic (WDDL) [4], of which the power traces exhibit relatively low variations. Besides traditional DRP logic styles, dynamic current mode logic (DyCML) is another cell-level choice for counteracting PA [5]. The power consumption of DyCML-based implementations is independent of the key data processed due to its dynamic and differential logic style. Furthermore, DyCML-based cells exhibit low-power efficiency because of low-swing internal operations. However, the research of flip-flop (FF) designs based on DyCML is still in blank state. Note that FFs are the preferred target of SCA due to synchronised power, so we implement the FF design compatible with DyCML in this Letter.

DyCML scheme: The DyCML scheme can be treated as a novel method to resist SCA, which utilises a dynamic current source with a fictitious ground [6]. Owing to the dynamic and differential structure, the power consumptions of cell-level DyCML-based circuits are independent of the data processed, leading to the same level SCA resistance as other DRP circuits. Furthermore, active loads are used in DyCML instead of the traditional loading resistors in the conventional static current-source mode logic to decrease power consumption.

As shown in Fig. 1, the generic structure of a DyCML-based cell is made up of four blocks: the precharge block ($P1$, $P2$), a latch for holding logic values after evaluation stage ($P3$, $P4$), dynamic current source ($N1$, $C1$) and the function block to sample the input values during the evaluation stage. When the input clock is low, the cell is at precharge phase, during which transistors $P1$, $P2$ and $N2$ are turned on, pulling up the internal nodes (TA, TB) to VDD and pulling down the internal node TX to GND. When the input clock is high, the cell is at evaluation phase, during which transistors $N1$ is turned on, providing a conducting path from the two output nodes to the capacitor $C1$.

On the basis of the operating principles of DyCML cells, we can easily find that there are constantly one precharge phase and one evaluation phase in every clock cycle. During the precharge phase, all internal nodes are keeping high level, whereas during the evaluation phase, only one node is pulled down to low level according to the inputs. As a result, the DyCML structure is SCA resistant, which has constant power consumption and is independent of the processed data under the condition of balanced capacitive loads.

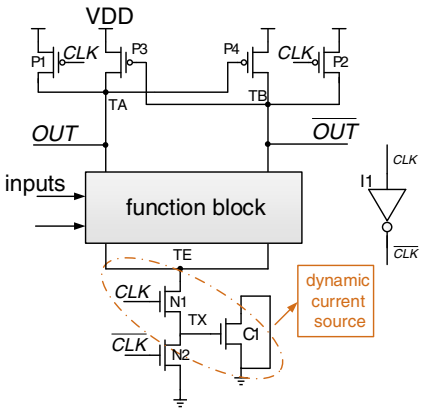

Fig. 1 *Transistor schematic of generic DyCML cell*

FF design based on DyCML: Owing to the SCA resistance of DyCML scheme for its dynamic and differential structure and its low gate and interconnect power dissipation, we have designed a novel FF based on DyCML (DyCML-FF), whose schematic diagram is depicted in Fig. 2. To realise constant power dissipation, DyCML-FF adopts two stages, i.e. a pseudo-P-type and an N-type DyCML single-rail latch, which are derived by the inverted input clock signal and the original input clock. Accordingly, stage 1 is in the precharge phase when stage 2 is in the evaluation phase and vice versa. Furthermore, due to the low-swing current mode feature of a DyCML-based cell, we have applied a normal inverter as the interface with the full-swing logic-based gates.

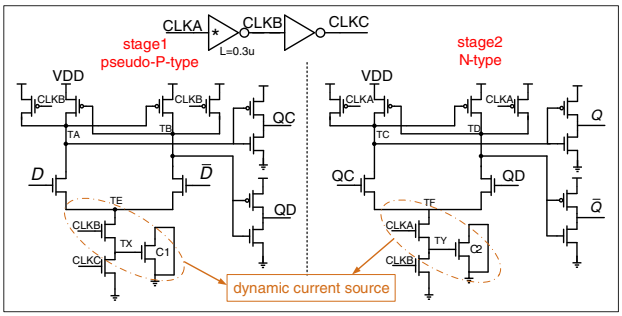

Fig. 2 *Schematic diagram of proposed DyCML-FF*

The operational principle of the proposed DyCML-FF is explained as follows. At the falling edge of CLKA, stage 2 first enters the precharge phase and outputs 0 at nodes Q and $\bar{Q}$. After an inverter delay, stage 1 enters the evaluation phase and samples the input complementary values. At the subsequent rising edge of the input clock (CLKA), stage 2 first enters the evaluation phase, which samples the complementary values provided by stage 1. Then, stage 1 clocked by CLKB enters the precharge phase by an inverter delay with respect to CLKA, whose output terminals are precharged to 0. In short, the DyCML-FF samples the complementary input values at the falling edge of the clock and outputs the complementary values at the subsequent rising edge of the clock. Note that stage 1 is clocked by the delayed clock signal, so negative setup time can be provided in our proposed design, *i.e.* the time of the input signal transitions can be lagging behind the clock signal, which greatly improves the delay performance of the device.

As described above, considering both internal and output nodes together (QC, QD, $Q\&\bar{Q}$) in complementary rails, at every rising or falling clock edge there are constantly one $0 \rightarrow 1$ flip, one $1 \rightarrow 0$ flip and two $0 \rightarrow 0$ transitions. This fact leads to constant total power consumption, which builds the basis for its SCA resistance. As a result, we think that the proposed DyCML-FF is compatible for most cell-level-based implementations of secure applications against SCA.

Experiment results: To evaluate the functionality and efficiency of the proposed design against SCA, the power metric of DyCML-FF has been simulated and compared with the SABL- and WDDL-based FF designs. The testbench follows that in [7]. The pre-simulation results are acquired by HSPICE (Version: C-2009.09) in the SMIC 65 nm CMOS technology. The source voltage is 1.2 V. The input clock

frequency is 1 GHz. The input data is a pseudo-random data set with an activity factor of 15%. Furthermore, the complementary output nodes are loaded with balanced capacitance loads of 3 fF.

To evaluate the resistance of the proposed design against PA attacks, two parameters normalised energy deviation (NED) and normalised standard deviation (NSD) are considered [8]. The parameter NED is defined as the percentage difference between the maximum energy consumption (E_{max}) and minimum energy consumption (E_{min}) over all possible input combinations and transitions as shown in (1). The parameter NSD indicates how much the energy consumption varies based on the inputs as shown in (2). Ideally these two parameters should approximate zero for better resistance to PA attacks [3]

$$\text{NED} = \frac{E_{max} - E_{min}}{E_{max}} \tag{1}$$

$$\text{NSD} = \frac{\sigma_E}{E_{avg}} \tag{2}$$

where

$$\sigma = \sqrt{\sum_{i}^{n} (E_i - E_{avg})^2 / n}, \quad E_{avg} = \left(\sum_{i}^{n} E_i\right) / n \tag{3}$$

Except for NED and NSD, we have also applied several other essential measurement criteria to compare the performance of DyCML-FF with other FF implementations, *e.g.* minimum $D - Q$ delay (t_{D-Q}), power consumption, power-delay-product (PDP) etc. On the basis of these parameters, the corresponding simulation results are shown in Table 1.

Table 1: Comparison of various FF designs

FF designs		SC	SABL	WDDL	DyCML
Number of transistors		30	26	128	30
Total power (μW)	0 → 0	16.46	14.76	78.54	16.67
	0 → 1	18.16	14.72	79.41	16.69
	1 → 0	17.45	14.66	79.15	16.81
	1 → 1	15.67	14.62	78.26	16.72
	all	16.94	14.76	78.84	16.71
NED		0.137	0.0128	0.0145	0.0083
NSD		0.056	0.0048	0.0058	0.0032
Min. $D - Q$ (ps)		191.80	653.48	929.02	512.54
Min. setup (ps)		−126.07	12.56	−188.78	−75.71
Min. CLKA − Q (ps)		317.87	640.92	1117.80	587.96
PDP (fJ)		3.249	9.645	73.244	8.565

The simulation results prove that DyCML-FF functions properly and at every rising or falling clock edge, there are, respectively, two variant and invariant data transitions, which is broadly in conformity to the theory in the above section. As is obvious from Table 1, the DyCML-FF has achieved great improvement in both NED and NSD when compared with standard-cell (SC)-FF, and is more efficient than SABL-FF and WDDL-FF, proving that the proposed FF is more resistant to SCA. In terms of delay performance, DyCML-FF takes the minimum t_{D-Q} delay among various designs, except for SC-FF due to its negative setup time feature, whereas SABL-FF has positive setup time and the WDDL-FF takes more than one clock cycle due to its wave logic. In terms of power performance, the DyCML-FF consumes about the same level power as SABL-FF, whereas the WDDL-FF consumes the largest power. This is mainly attributed to the total four standard-cell FFs applied in WDDL-FF. Furthermore, the dynamic current-source logic applied in the simplified latch of DyCML-FF contributes to its low-power efficiency. Accordingly, the PDP performance of the DyCML-FF ranks the best mainly due to its low-power characteristic and relatively good speed performance, which is 11.20 and 88.31% less than SABL-FF and WDDL-FF, respectively. Consequently, the new design conforms with the design rules for DRP-FFs, which can absolutely provide high SCA resistance for hardware implementations of security algorithms.

To further evaluate how the proposed scheme mitigates PA attacks in real scenarios, experiments are carried out on a complete implementation of AES-SBox module. The correlation power attack (CPA) attack results show that with about 20 power traces SC-based module can be successfully attacked, whereas DyCML scheme and other cell-level countermeasure logic can perfectly protect the AES-SBox module. Specially, the attack result of DyCML-based circuit is demonstrated in Fig. 3.

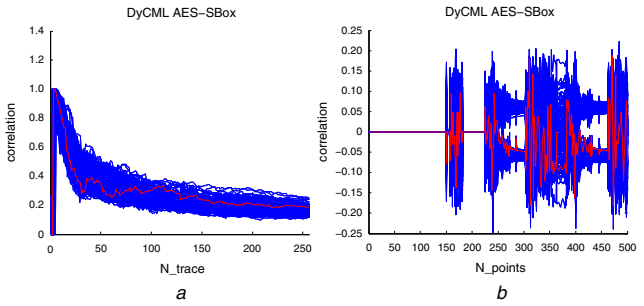

Fig. 3 *CPA attack results of DyCML-based AES-SBox circuit*
a Correlation against number of traces
b Correlation against length of traces

Consequently, due to the fact that DyCML-FF not only offers excellent SCA resistance, but also exhibits high-level PDP performance when compared with SABL-FF and WDDL-FF for its low-power consumption and relatively high speed, we prefer this DyCML-based implementation to be a good choice for sequential elements in cryptographic application specific integrated circuit (ASIC) instead of SABL- and WDDL-based FF implementations.

Conclusions: In this Letter, we have proposed a novel full-custom FF design based on DyCML scheme, which consumes constant power regardless of all possible input data combinations. The detailed cell-level experimental results show that the proposed design gains an improvement in terms of NED and NSD, which proves the moderate level of side-channel resistance against its counterparts. Meanwhile, the DyCML-FF has made a reduction by 10.60 and 88.35% in terms of PDP when compared with SABL-FF and WDDL-FF, respectively. In addition, the case study of AES substitution has further proved the SCA resistance of the proposed scheme. As a consequence, the proposed DyCML-FF is an appropriate choice for sequential elements in ASIC, where both security and PDP are highly required.

Acknowledgments: This work was supported in part by the National Natural Science Foundation of China (grant no. 61471314, 61432357) and by the China Scholarship Council (grant no. CSC201606325012).

Submitted: *22 June 2017* E-first: *4 August 2017*
doi: 10.1049/el.2017.2415
One or more of the Figures in this Letter are available in colour online.

Jizhong Shen, Liang Geng and Fan Zhang (*College of Information Science & Electronic Engineering, Zhejiang University, Hangzhou, People's Republic of China*)

✉ E-mail: jzshen@zju.edu.cn

References

1 He, W., Breier, J., Bhasin, S., *et al.*: 'Bypassing parity protected cryptography using laser fault injection in cyber–physical system'. Proc. Second ACM Int. Workshop on Cyber–Physical System Security, Xi'an, China, May 2016, pp. 15–21
2 Kocher, P., Jaffe, J., and Jun, B.: 'Differential power analysis'. Advances in Cryptology – CRYPTO '99, Santa Barbara, CA, USA, August 1999, pp. 388–397
3 Saravanan, P., and Kalpana, P.: 'An energy efficient XOR gate implementation resistant to power analysis attacks', *J. Eng. Sci. Technol.*, 2015, **10**, pp. 1275–1292
4 Mangard, S., Oswald, E., and Popp, T.: 'Power analysis attacks: revealing the secrets of smart cards' (Springer Science & Business Media, 2008)
5 Mace, F., Standaert, F.X., Hassoune, I., *et al.*: 'A dynamic current mode logic to counteract power analysis attacks'. Proc. DCIS, Bordeaux, France, November 2004
6 Allam, M.W., and Elmasry, M.I.: 'Dynamic current mode logic (DyCML): a new low-power high-performance logic style', *J. Solid-State Circuits*, 2001, **36**, pp. 550–558
7 Stojanovic, V., and Oklobdzija, V.G.: 'Comparative analysis of master–slave latches and flip-flops for high-performance and low-power systems', *J. Solid-State Circuits*, 1999, **34**, pp. 536–548
8 Bucci, M., Giancane, L., Luzzi, R., *et al.*: 'Three-phase dual-rail precharge logic'. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES '06), Yokohama, Japan, October 2006, pp. 232–241