IEICE Electronics Express, Vol.18, No.16, 1–6

LETTER

# A novel SCA-resilience flip-flop design utilizing the current mode logic based on the three-independent-gate field effect transistors

**Yuehui Li**[1, 2], **Yanjiang Liu**[3], **Xianzhao Xia**[1, 4], **and Yiqiang Zhao**[1, a)]

**Abstract** In this paper, current mode logic based on the three-independent-gate field effect transistor (TIGFET) is introduced as the circuit-level side-channel attack (SCA) countermeasures, and a SCA-resilience flip-flop (DyCML) is designed to make the power consumption constant. Then, a simplified advanced encryption system (AES) is built, and power analysis is performed to evaluate the SCA-resistance efficacy. Simulation results show that the key with the TIGFET-based DyCML is not revealed with 255 power traces. The proposed design occupies less area usage and requires less delay overhead compared to the original TIGFET-based true single-phase clock (TSPC) and modified TSPC (mTSPC).
**Keywords:** side-channel attack, circuit-level countermeasures, flip-flop, three-independent-gate field effect transistor, current mode logic
**Classification:** Integrated circuits (memory, logic, analog, RF, sensor)

## 1. Introduction

With the rapid development of information and communication technology, a tremendous amount of information in mobile phones, portable devices, smart cards, and social network rushes into daily life. Although the information makes life easier and more convenient, it also provides an opportunity for the attacker to retrieve the privacy information [1, 2]. To prevent information leakage in sensitive applications, cryptographic algorithms are widely studied and used to encrypt the critical information that is extremely difficult to recover. Furthermore, cryptographic algorithms are extended to physical implementations for further seeking high performance and cryptographic implementations are commonly applied to the embedded devices.

Since the side-channel attack is proposed by Kocher in 1996 [3], numerous attack approaches, including simple power analysis (SPA) [4], differential power analysis (DPA) [5], correlation power analysis (CPA) [6], template attack (TA) [7], etc, have been explored to reveal the sensitive information of the cryptographic implementations. Of all SCAs, DPA and CPA have become the main threat to the confidentiality of cryptographic implementations for its simplicity and effectiveness.

To address this issue, numerous circuit-level SCA countermeasures have been proposed over the past few decades. Kris et al. first propose a complementary logic (SABL) in [8], and its improvement wave dynamic differential logic (WDDL) [9]. Further, some differential logics, including the MDPL [10], iMDPL [11], iWDDL [12], STTL [13], BCDL [14], DDPL [15], TDPL [16] and CML [17, 18], have been explored to improve the security level. However, such approaches introduce non-negligible power and area overheads, which makes them difficult to be deployed in resource-constrained applications. For the sequential circuits, flip-flops are often the primary source of information leakage to an SCA and several secure flip-flops have been proposed to minimize the power variations at the rising/falling clock edge. As shown in Ref. [16, 19, 20], the cryptographic design with the secure flip-flops can achieve a high SCA-resilience level without less area cost and power overhead compared to the traditional circuit-level SCA countermeasures. However, the pull-up and pull-down network currents of those secure flip-flops are not the same due to the asymmetric I-V characteristics of CMOS devices, and the minor current differences of secure flip-flops under various transitions can leak information for a given power attack.

In this paper, a secure flip-flop based on the TIGFET is proposed, which can resist the SCA and maintain a low area overhead and delay cost. The SCA-resistance characteristics of TIGFET are analyzed, and the CML and TIGFETs are combined to achieve a low-cost solution against the SCA. Further, a dynamic current mode logic SCA-resistance flip-flop based on the TIGFET (DyCML) is designed and performance evaluation is executed to analyze the security characteristics under all possible transitions. Finally, a simplified AES circuit is set up with the proposed design, and the SCA-resilience efficacy is evaluated using the correlation power analysis compared to the other flip-flops. The main contributions are listed as follows.

- A secure TIGFET-based flip-flip is proposed in this paper, which eliminate the power-to-data dependency under all possible transitions. To the best of our knowledge, this is one of the pioneers attempts to design the secure flip-flops using the emerging device TIGFET.
- A simplified AES is implemented with the TIGFET-based flip-flop, and correlation power analysis is used to evaluate the SCA-resilience efficacy. The proposed cryptographic implementation obtains a similar security level with a smaller area overhead and delay

[1] School of Microelectronics, Tianjin University, Tianjin 300072, China
[2] School of Information Science and Technology, Nantong University, Jiangsu 226019,China
[3] Information Engineering University, Henan 450000, China.
[4] China Automotive Technology and Research Center, Tianjin 300300, China.
[a)] yq_zhao@tju.edu.cn

**DOI: 10.1587/elex.18.20210248**
**Received June 7, 2021**
**Accepted July 6, 2021**
**Publicized July 20, 2021**
**Copyedited August 25, 2021**

cost compared to the other CMOS-based and TIGFET-based solutions.

The rest of this paper is organized as follows. Section 2. investigates the related work about the SCA countermeasures and Section 3. introduces the major vulnerabilities of current mode logic and its low-cost solution with the TIGFET. Section 4. presents the structure, functional simulation and security characteristic evaluation of the proposed secure flip-flop. Section 5. gives the implementation of AES and analyzes the simulation results. Section 6. concludes this paper.

## 2. Side-channel attack prevention: previous work

Concerning the catastrophic consequences caused by SCA in the cryptosystems, various circuit-level countermeasures have been proposed over the past few decades. Since the gate-level masking method was first presented in [21], Trichina et al. introduce several masked gate circuits [22], and Golic proposes a MUX technique for masking the AND and OR gates [23]. Moreover, the random switching logic presented in [24] can resist the second-order DPA. Even though such masking methods make the power consumption to be independent of processed data, the outputs' transitions of masked logic gates are dependent on the input signals when glitches exist. Several works described in [25] did a successful attack on the masked hardware implementations with glitches.To resist the glitch attacks, Furthermore, masking schemes apply to the WDDL and several improvements are presented as follows, including the MDPL [10], iMDPL [11], STTL [13], and BCDL [14]. However, the WDDL and its improvements still leak some side-channel information due to the asymmetric routing and unbalanced load conditions. Therefore, some full-customized differential logic styles are proposed to provide higher security levels. Bucci et al. also propose a three-phase dual-rail precharge logic [16] and Shen et al. propose a dynamic current mode logic secure flip-flop (DyCML) [20]. Although these schemes make the power consumption independent of the processed data, it also increases more than 2× area overheads.

To address this issue, several emerging devices are utilized to reduce the area and power of cryptographic circuits while improving the side-channel attack resilience. In [18], the current mode logic components based on the tunneling FETs (TFET) are utilized in the DPA-resilient block cipher design and several combinational secure cells are presented. Several improvements are proposed with the tunneling FTEs in [26, 27] and a TFET-based library that covers all basic logic gates is introduced. But the secure flip-flop is still not described. Moreover, a true single-phase clock flip-flop based on the three-independent-gate silicon nanowire FET (TSPC) is proposed in [28], which improves the area, delay and leakage power by nearly 20%, 30% and 7% respectively compared to CMOS design. Furthermore, Sharifi et al. propose a modified TSPC(mTSPC) and evaluate the SCA resiliency of 8-bit Sbox [29]. Although the mTSPC achieve a higher security level, the number of transistors required is 18, which is not allowed for resource-constrained devices in embedded applications.

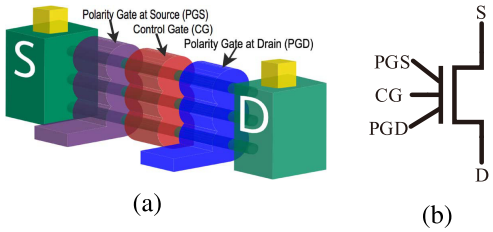


**Fig. 1** Structure (a) and symbol (b) of the TIGFET.

## 3. The current mode logic and its low-cost solution based on the TIGFET

The current mode logic is mainly composed of three parts: pull-up network, differential pull-down network and tail current source. The pull-up network works as the load resistor to achieve a voltage swing on the output, and the load resistance value determines the output voltage swing. The pull-down network implements the differential logic function according to the differential inputs and provides a complementary output in every clock cycle, while the n-type transistor operates in the saturation region as a tail current source and the voltage value of gate of the n-type transistor (Vbias) determines the current flowing through the ground. Such differential logic structure offers high robustness to the ambient noises. Moreover, the low output swing and constant current source reduce the dynamic power consumption of CML, which has emerged as an effective countermeasure against the side-channel attack [17, 18]. However, the CML introduces non-negligible power and area overheads, which makes them difficult to be deployed in resource-constrained applications. Therefore, the TIGFET is introduced to the CML, which can achieve a high SCA-resistance level without sacrificing area cost and power overhead.

Fig. 1 shows the structure of the TIGFET. Compared to the traditional CMOS transistor, the TIGFET has added 2 independent gates that control the device's electrical characteristics. As shown in Fig. 1, source gate (denoted as S) and drain gate (denoted as D) connect with 3 vertically stacked silicon nanowires, and polarity gate at source (denoted as PGS) and polarity gate at the drain (PGD) close to the control gate (denoted as CG). There exist 4 states of this device, which is ON states, OFF states, low-leakage OFF states and uncertain states, and the detailed bias gate conditions are presented in [30]. More specifically, the two-inputs configuration of TIGFET can realize the complex Boolean logic (e.g. 2 series nFETs/pFETS and XOR), which reduces the area overhead compared with the CMOS devices.

In summary, the TIGFET has shown its advantages in area usage relying on their unique and unconventional properties, and the CML with low output swing and a constant current source has already proven as an effective countermeasure against the SCA. Therefore, the current mode logic based on the TIGFET presents an appealing option for high-performance and high-security cryptographic systems under resource-constrained implementations.

**Table I** Comprehensive comparison

| FF Design | CMOS | | | TIGFET | | |
|---|---|---|---|---|---|---|
| | Original TSPC | mTSPC | DyCML | Original TSPC | mTSPC | DyCML |
| Maximum Current Variation (%) | 24.76 | 6.8 | 2.07 | 24.76 | 0.11 | 0.31 |
| Area Usage (transistors) | 11 | 14 | 30 | 12 | 18 | 7 |
| Clock-to-output (ps) | 14.79 | 5.02 | 9.16 | 54.15 | 15.2 | 3.38 |
| Number of Clock Domains | 1 | 1 | 3 | 1 | 1 | 0 |

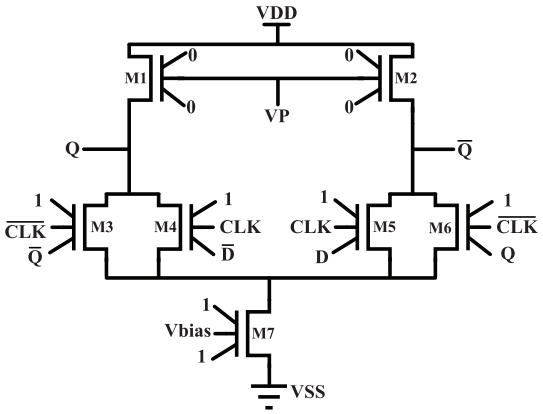


**Fig. 2** Structure of TIGFET-based DyCML.

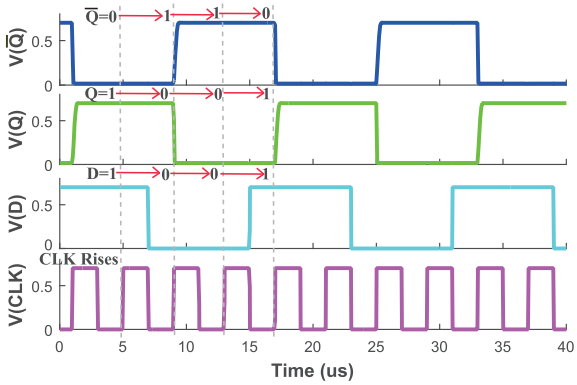


**Fig. 3** The sequence diagram of TIGFET-based DyCML.

## 4. The proposed secure CML-based DFF design

The flip-flop is the basic sequential element of the digital circuit, which is the main weakness of information leakage because there exists a correlation between the input transitions and power consumption at the rising edge of the clock [19]. To hiding the power consumption, a TIGFET-based CML D-type flip-flop (DyCML) is proposed. The structure of TIGFET-based DyCML is shown in Fig. 2.

For the TIGFET-based DyCML, M5 is turned on and the output ($Q$ and $\overline{Q}$) capture the input value when the input $D$ is logic "1" at the rising edge of the clock (CLK). Otherwise, the M6 is turned on and the last state of Q is held in the flip-flop when the CLK falls to logic "0". The M4 is turned on when the input $D$ is logic "0" and the CLK rises to logic "1", while the M6 is turned off and the M3 is turned on when the CLK falls to logic "0". The sequence diagram of the DyCML is shown in Fig. 3 and the timing results are consistent with the traditional flip-flop's logic function.

As described above, the value of VP and Vbias determine the voltage swing of CML gates. Besides, the transistor's size also affects the dynamic characteristic of TIGFETs. Therefore, voltage sweeping analysis on VP and Vbias is performed and the transistor size is also adjusted to minimize the variations of power consumption under all possible transitions. The VP and Vbias of TIGFET-based DyCML are set to 0.25 V and 0.5 V respectively. The supply current of TIGFET-based DyCML is ranging from -1090.5 nA to -1087.1 nA, while the CMOS-based DyCML falls within the -2073.1 nA and -2071.9 nA. The variations of supply current under all possible transitions are minor, which implies the power-to-data dependency under all possible transitions is eliminated.

The maximum current variation (MCV) is used to evaluate the variation of power during circuit transitions [29]. The smaller the MCV is, the more balance the design consumes per cycle, and the better the SCA resists. When a circuit has a higher MCV, it is more susceptible to SCAs [19, 29]. In this paper, 10nm TIGFET and CMOS device spice models are used to evaluate the performance and security of the proposed flip-flops. The MCV of TIGFET-based DyCML during state transitions is calculated, and the results are shown in Table I. The MCV of TIGFET-based DyCML is 0.31%, while the MCV of the CMOS-based DyCML is 2.07%. This suggests that the symmetry property of TIGFET, and the tail current source and differential logic structure of current mode logic can considerably improve the SCA resiliency of the current mode logic circuits. Further, the original TIGFET-based TSPC design is compared to the proposed design, the MCV of TIGFET-based DyCML is greater than the original TIGFET-based TSPC (0.31% to 24.76%). Besides, the MCV of TIGFET-based DyCML and TIGFET-based mTSPC is less than 0.5%, which shows these flip-flops maintain a constant power dissipation under various transitions.

The third row of Table I lists the number of required transistors. For the TIGFET-based DyCML, the number of required transistors is only 7, which is lower than the other flip-flops. As described above, a single TIGFET device can realize several complex Boolean logic functions by configuring the value of three independent programmable gates. For a complex circuit, the TIGFET-based cryptographic circuits require a smaller number of transistors compared with the CMOS counterparts. The static structure of the TIGFET-based TSPC and mTSPC require more transistors to ensure the same number of transitions (0->1 and 1->0) under all possible transitions. Therefore, the area usage of DyCML is smaller than the other implementations.

Furthermore, the delay from the rising edge of the clock

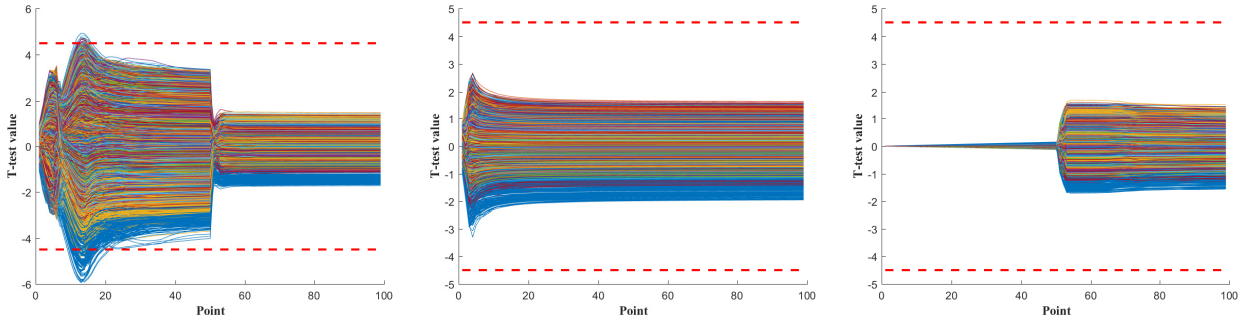


**Fig. 4** T-test results of 8-bit AES datapath with TIGFET-based original TSPC (a), mTSPC (b), and DyCML (c).

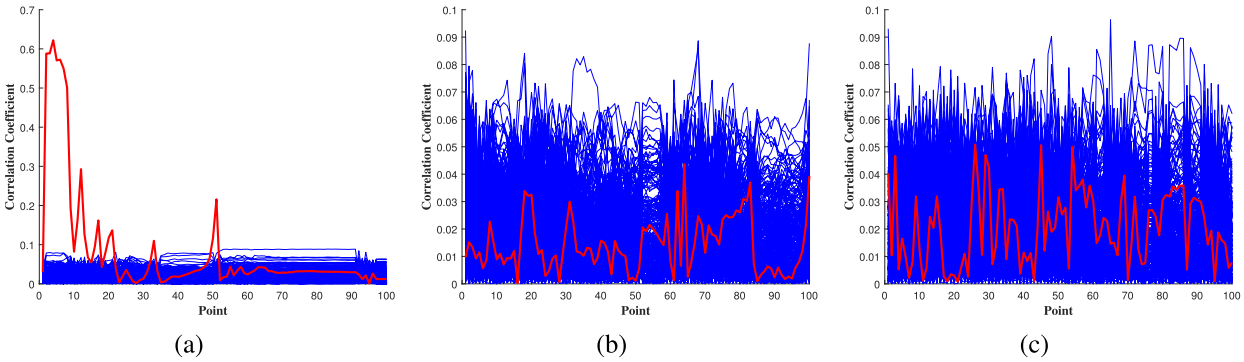


**Fig. 5** CPA attack results of 8-bit AES datapath with TIGFET-based original TSPC (a), mTSPC (b), and DyCML (c).

to the output is calculated and results are shown in the fourth row of Table I. The delay of TIGFET-based DyCML is 3.38ps, while the delay of TIGFET-based mTSPC is 15.2ps. The number of transistors required of TIGFET-based DyCML is smaller than the TIGFET-based mTSPC, thus the delay of DyCML is smaller than the TSPC and mTSPC. Besides, DyCML captures and outputs the value immediately at the rising/falling edge of clock, while the other flip-flops need at least 1 clock period. In summary, the TIGFET-based DyCML offers a better delay metric compared to the other flip-flops. Overall, the TIGFET-based DyCML achieves stable power consumption with lower latency and smaller area compared to the other flip-flops.

## 5. SCA-resilience evaluation

Advanced encryption standard is widely applied in critical applications and sensitive fields, such as communication, finance, Internet of things, and so on. In AES, four operations form the basic AES encryption or decryption datapath and the smallest unit of four operations is one byte. SCA reveals the key byte by byte and the power consumption of the other 15 bytes datapath can be considered as noise for SCA. Due to the other 15 bytes datapath, the SCA efficacy is decreased drastically. Considering the low area and computation cost, an 8-bit AES datapath is an ideal choice to be used in the SCA-resistance evaluation [29, 31]. As long as the 8-bit AES datapath resists the SCA attack, there is no doubt that the corresponding AES implementation with the proposed design achieves a higher SCA-resilience ability than the 8-bit AES datapath. Therefore, an 8-bit AES encryption datapath instead of AES is built in this paper. In this paper, the 8-bit AES datapath includes 8-bit AddRoundKey, SubBytes, ShiftRows and MixColumns operation, and the output is sampled by a group of 8 TIGFET-based DyCMLs.

After the power simulation, Welch's t-test is used to assess the information leakage of cryptographic circuits and provide a leakage value for each particular point in the power traces. The power traces are divided into two subsets (fixed plaintext and random plaintext) and the t-test values between two sets are calculated. During the analysis based on Welch's t-tests, a confidence level of 99.99% implies the threshold value of t-test is ±4.5. The t-test results are shown in Fig. 4. Regarding the Fig. 4, all the t-test values of TIGFET-based mTSPC and DyCML are within the range of -4.5 and 4.5, which means that the TIGFET-based mTSPC and DyCML do not leak the secret key. For the t-test values of TIGFET-based TSPC, there exist some point exceed the threshold value (±4.5). Therefore, the TIGFET-based TSPC is vulnerable to the SCA.

Furthermore, correlation power analysis is performed to reveal the secret key of cryptographic implementations using correlation of actual power traces with calculated hypothetical power values. The maximum correlation coefficient corresponds to the hypothetical key is considered as the correct key. The correlation coefficients of TIGFET-based TSPC, mTSPC, and DyCML are shown in Fig. 5. The red and blue lines are the correct and the other 254 wrong hypothetical key. Regarding Fig. 5 (a), the correlation coefficients correspond with the correct key reach to the peak value which indicates that obvious information leakage could be observed at this sample point, and the CPA perform a successful attack on the AES datapath with the TIGFET-based original TSPC. For the Fig. 5 (b) and (c), all the correlation coefficients are

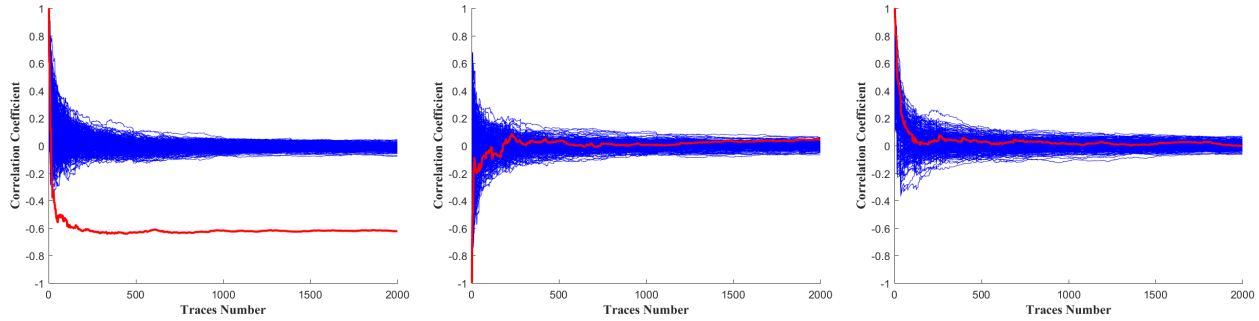


**Fig. 6** MTD results of 8-bit AES datapath with TIGFET-based original TSPC (a), mTSPC (b), and DyCML (c).

lower than 0.1 and the correlation coefficients of the correct key are buried by the other wrong keys. This means that CPA fails to reveal the correct key for TIGFET-based mTSPC and DyCML implementations. The other 15 AES datapaths and random noise in the actual experiment will reduce the signal-to-noise ratio undoubtedly, and the CPA-resilience efficacy of AES implementation may be further improved. In summary, the cryptographic circuit with TIGFET-based DyCML can provide a similar security level compared with mTSPC equivalences, but it has lower delay and area overhead that is suitable for the resource-constrained applications.

Further, the minimum number of traces to disclose the correct key (denoted as MTD) based on the highest correlation coefficient is calculated to assess the side-channel leakage and the MTD results are shown in Fig. 6. As shown in Fig. 6 (a), the red lines are clearly separated from the others which indicate there exists obvious key-related information leakage, and the cryptographic circuit with the TIGFET-based TSPC is not resilient to the CPA attack. For the Fig. 6 (b) and (c), the correlation coefficients do not increase after the increasing number of traces, and the correlation coefficient corresponds to the correct key is buried by the other wrong keys. It's mean that the cryptographic circuit with the TIGFET-based mTSPC and DyCML are not successfully attacked with those traces. Therefore, we can confirm that the TIG SiNWFET-based DyCML can resist the CPA. In summary, the cryptographic circuit using the TIGFET-based DyCML is well suitable for resource-constrained applications given its low area overhead and delay cost combined its comparable security levels compared to mTSPC.

## 6. Conclusion and future work

In this paper, TIGFETs and CML are combined to the circuit-level SCA countermeasures, because it maintains a similar security-level against SCA and reduces the power consumption and area overhead compared to the other solutions. The TIGFET-based DyCML is designed and optimized according to the performance evaluation. Further, a simplified AES circuit is built and correlation power analysis is performed to validate the SCA-resistance. Experimental results show that the TIGFET-based DyCML achieves a similar SCA-resistance level with a smaller area and delay consumption compared to the TIGFET-based mTSPC.

## References

[1] J. Yang, *et al.*: "Countering power analysis attacks by exploiting characteristics of multicore processors," IEICE Electron. Express **15** (2018) 20180084 (DOI: 10.1587/elex.15.20180084).
[2] N. Makoto, *et al.*: "Protecting cryptographic integrated circuits with side-channel information," IEICE Electron. Express **14** (2017) 20162005 (DOI: 10.1587/elex.14.20162005).
[3] P.C. Kocher: "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," Ann. Inf. Crypto. Conf. (1996) 104 (DOI: 10.1007/3-540-68697-5_9).
[4] C. Giraud: "An rsa implementation resistant to fault attacks and to simple power analysis," IEEE Trans. Comput. **55** (2006) 1116 (DOI: 10.1109/tc.2006.135).
[5] W. Wang, *et al.*: "Ridge-based dpa: improvement of differential power analysis for nanoscale chips," IEEE Trans. Inf. Forensics Security **13** (2017) 1301 (DOI: 10.1109/tifs.2017.2787985).
[6] W. Shan, *et al.*: "Evaluation of correlation power analysis resistance and its application on asymmetric mask protected data encryption standard hardware," IEEE Trans. Instrum. Meas. **62** (2013) 2716 (DOI: 10.1109/tim.2013.2259754).
[7] M.O. Choudary and M.G. Kuhn: "Efficient, portable template attacks," IEEE Trans. Inf. Forensics Security **13** (2018) 490 (DOI: 10.1109/tifs.2017.2757440).
[8] K. Tiri and I. Verbauwhede: "Securing encryption algorithms against dpa at the logic level: next generation smart card technology," Int. Workshop Crypto. Hardw. Embedded Sys. (2003) 125 (DOI: 10.1007/978-3-540-45238-6_11).
[9] K. Tiri and I. Verbauwhede: "A logic level design methodology for a secure dpa resistant asic or fpga implementation," Des. Autom. Test Eur. Conf. (2004) (DOI: 10.1109/date.2004.1268856).
[10] T. Popp and S. Mangard. "Implementation aspects of the dpa-resistant logic style mdpl," IEEE Int. Symp. Cir. Syst. (2006) 2916 (DOI: 10.1109/iscas.2006.1693234).
[11] A. Moradi, *et al.*: "Masked dual-rail precharge logic encounters state-of-the-art power analysis methods," IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **20** (2012) 1578 (DOI: 10.1109/tvlsi.2011.2160375).
[12] R. Mcevoy, *et al.*: "Isolated wddl: a hiding countermeasure for differential power analysis on fpgas," ACM Trans. Reconf. Tech. Syst. **2** (2009) 1 (DOI: 10.1145/1502781.1502784).
[13] R. Soares, *et al.*: "Evaluating the robustness of secure triple track logic through prototyping," Symp. Integr. Cir. Syst. Des. (2008) 193 (DOI: 10.1145/1404371.1404425).
[14] M. Nassar, *et al.*: "Bcdl: a high speed balanced dpl for fpga with global precharge and no early evaluation," Des. Autom. Test Eur. Conf. Exhibit. (2010) 849 (DOI: 10.1109/date.2010.5456932).
[15] M. Bucci, *et al.*: "Delay-based dual-rail pre-charge logic," IEEE Int. Conf. Electron. Cir. Syst. (2009) 53 (DOI: 10.1109/icecs.2009.5410921).
[16] M. Bucci, *et al.*: "A flip-flop for the dpa resistant three-phase dual-rail pre-charge logic family," IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **20** (2012) 2128 (DOI: 10.1109/tvlsi.2011.2165862).

[17] H. Kim, *et al.*: "Mutual information analysis for three-phase dynamic current mode logic against side-channel attack," J. Etri **37** (2015) 584 (DOI: 10.4218/etrij.15.0114.0297).
[18] Y. Bi, *et al.*: "Leverage emerging technologies for dpa-resilient block cipher design," Des. Autom. Test Eur. Conf. Exhibit. (2016) 1538 (DOI: 10.3850/9783981537079_0992).
[19] I. Levi, *et al.*: "A survey of the sensitivities of security oriented flip-flop circuits," IEEE Access **5** (2017) 24797 (DOI: 10.1109/access.2017.2766243).
[20] J. Shen, *et al.*: "Dynamic current mode logic based flip-flop design for robust and low-power security integrated circuits," Electron. Lett. **53** (2017) 1236 (DOI: 10.1049/el.2017.2415).
[21] Y. Ishai, *et al.*: "Private circuits: Securing hardware against probing attacks," Lect. Notes Comput. Sci. **2729** (2003) 463 (DOI: 10.1007/978-3-540-45146-4_27).
[22] E. Trichina, *et al.*: "Simplified adaptive multiplicative masking for aes," Int. Workshop Crypto. Hardw. Embedded Syst. (2002) 187 (DOI: 10.1007/3-540-36400-5_15).
[23] J.D. Golić and R. Menicocci.: "Universal masking on logic gate level," Electron. Lett. **40** (2004) 526 (DOI: 10.1049/el:20040385).
[24] T. Ichikawa, *et al.*: "Random switching logic: A new countermeasure against dpa and second-order dpa at the logic level," IEICE Trans. Fundamentals **E90-A** (2007) 160 (DOI: 10.1093/ietfec/e90-a.1.160).
[25] M. Alam, *et al.*: "Effect of glitches against masked aes s-box implementation and countermeasure," IET Inf. Secur. **3** (2009) 34 (DOI: 10.1049/iet-ifs:20080041).
[26] Y. Bi, *et al.*: "Tunnel fet current mode logic for dpa-resilient circuit designs," IEEE Trans. Emerg. Topics Comput. Intell. **5** (2017) 340 (DOI: 10.1109/tetc.2016.2559159).
[27] Y. Bi, *et al.*: "Emerging technology-based design of primitives for hardware security," ACM J. Emerg. Tech. Comput. Syst. **13** (2016) 1 (DOI: 10.1145/2816818).
[28] X. Tang, *et al.*: "TSPC flip-flop circuit design with three-independent-gate silicon nanowire FETs," IEEE Int. Sym. Cir. Syst. (2014) 1660 (DOI: 10.1109/iscas.2014.6865471).
[29] M.M. Sharifi, *et al.*: "A novel TIGFET-based DFF design for improved resilience to power side-channel attacks," Des., Auto. Test Eur. Conf. Exhibit. (2020) 1 (DOI: 10.23919/date48585.2020.9116554).
[30] J. Romero-Gonzalez and P.-E. Gaillardon: "Bcb evaluation of high-performance and low-leakage three-independent-gate field-effect transistors," IEEE J. Explor. Solid-State Computat. **4** (2018) 35 (DOI: 10.1109/jxcdc.2018.2821638).
[31] X. Wang, *et al.*: "Role of power grid in side channel attack and power-grid-aware secure design," Des. Autom. Conf. (2013) 1 (DOI: 10.1145/2463209.2488830).