SN Computer Science (2021) 2:92
https://doi.org/10.1007/s42979-021-00482-2

ORIGINAL RESEARCH

Novel Secure MTJ/CMOS Logic (SMCL) for Energy-Efficient and DPA-Resistant Design

S. Dinesh Kumar[1] · Zachary Kahleifeh[1] · Himanshu Thapliyal[1]

Received: 28 June 2020 / Accepted: 21 January 2021 / Published online: 13 February 2021

Abstract
Hybrid MTJ/CMOS-based Logic-in-Memory (LiM) architecture-based circuits show high potential in designing low-power circuits by reducing the leakage power. In this work, we have proposed a novel energy-efficient and Secure MTJ/CMOS Logic (SMCL) circuits to design ultra-low-power and DPA-resistant MTJ/CMOS circuits. Similar to the existing MTJ/CMOS designs, the proposed MTJ/CMOS design also works in two different modes of clock. The proposed MTJ/CMOS designs have considerable power savings during the pre-charge of the clock. During the pre-charge phase, both output nodes are pre-charged to VDD/2, while during the evaluate phase, one node will be charged to VDD, while the other node will discharged to ground. Moreover, the proposed SMCL consumes uniform power by masking the MTJ during the write operation from the power supply, thereby thwarting the power analysis-based side-channel attacks. From our simulations, we have observed that the proposed SMCL-based PRESENT-80 cryptographic hardware has about 42% and 59% of energy savings as compared to the PCSA-based MTJ/CMOS and conventional CMOS-based implementation. Furthermore, we have also performed the DPA attack on the SMCL-based PRESENT-80 and the secret key was not revealed after 16,000 power traces.

Keywords Cryptography · Hardware security · Logic-in-memory (LiM) circuits · Low-energy computation · Magnetic tunnel junction (MTJ) · Side-channel attacks

Introduction

Spin Transfer Torque Magnetic Tunnel Junction (STT-MTJ) is considered as a promising candidate for designing low-power circuits [4, 7, 8]. Hybrid MTJ/CMOS-based Logic-In-Memory (LIM) architecture-based circuits show high potential in designing low-power circuits [22], especially in portable electronic devices. MTJ/CMOS-based LIM circuits have nearly zero leakage power dissipation and they are very appropriate to design low-power hardware. However, the security of the MTJ/CMOS circuit against side-channel attacks must be thoroughly verified before implementing in commercial devices.

Side-channel attack uses the unintentional information leaked by the cryptographic device to retrieve the secret key. Power analysis attack is one of the side-channel attack, where the attacker monitors the power consumption of the cryptographic device without making any physical changes to the device [9, 12]. In the recent years, researchers have focused on the security evaluation of Spin Transfer Torque Magnetic Random Access Memory (STT-MRAM) against power analysis attack [3, 6, 17]. However, there is no security evaluation of hybrid CMOS/MTJ circuits against power analysis attack.

In this paper, we are evaluating the security of the existing CMOS/MTJ-based LIM circuits against power analysis attacks. Furthermore, we are also proposing a novel CMOS/MTJ circuit which consumes 50% less energy than the existing CMOS/MTJ-based LIM circuits and less Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) values. In this paper, we have made the existing LIM-based CMOS/MTJ circuits secure against DPA attacks by masking the MTJ's during the writing of data in the MTJ. The preliminary version of this work has appeared in [10]. Furthermore, we have implemented a

This article is part of the topical collection "Hardware-Assisted Security Solutions for Electronic Systems" guest edited by Himanshu Thapliyal, Saraju P. Mohanty, Wujie Wen and Yiran Chen.

✉ Himanshu Thapliyal
hthapliyal@uky.edu

[1] Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY, USA

PRESENT-80 lightweight cryptographic hardware using the proposed SMCL logic. From our simulations, we have observed that the proposed SMCL-based PRESENT-80 cryptographic hardware has about 42% and 59% of energy savings as compared to the PCSA-based MTJ/CMOS and conventional CMOS-based implementation. Furthermore, we have also performed the DPA attack on the SMCL-based PRESENT-80 and the secret key was not revealed after 16000 power traces.

Section 2 discusses the background of MTJ device, CMOS/MTJ-based LIM architecture and Differential Power Analysis (DPA) attack. Section 3 analyzes the information leakage in the existing CMOS/MTJ LIM circuits. Section 4 presents the circuit design of the proposed low-power and DPA secure CMOS/MTJ circuit. Section 4 presents the proposed Secure MTJ/CMOS Logic (SMCL) circuits. Section 5 presents simulation results of SMCL-based logic gates. Section 6 presents the analysis of SMCL-based PRESENT-80 cryptographic hardware. Section 7 concludes the paper.

Background

Magnetic Tunnel Junction (MTJ)

Magnetic Tunnel Junction (MTJ) is a vertical nanopillar structure which consists of two ferromagnetic (FM) layers and an oxide barrier [13]. In the standard application of MTJ devices, the magnetization of one of the FM layers is fixed, while the other FM layer is free to take one of the two orientations (parallel and anti-parallel), as shown in Fig. 1 [20]. Based on the orientation of the FM layers, parallel (P) or anti-parallel (AP), MTJ device shows either a low resistance (RP) or high resistance (RAP) characteristic [1]. The resistance difference between the two configurations of MTJ device is given by the tunnel magnetoresistance ratio $TMR = (R_{AP} - R_P)/R_P$.

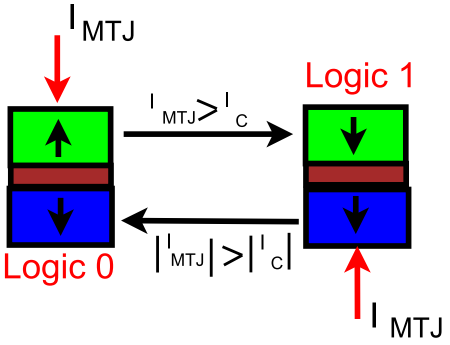

Fig. 1 Vertical Magnetic Tunnel Junction (MTJ) nanopillar structure with Spin Transfer Torque (STT) switching mechanism

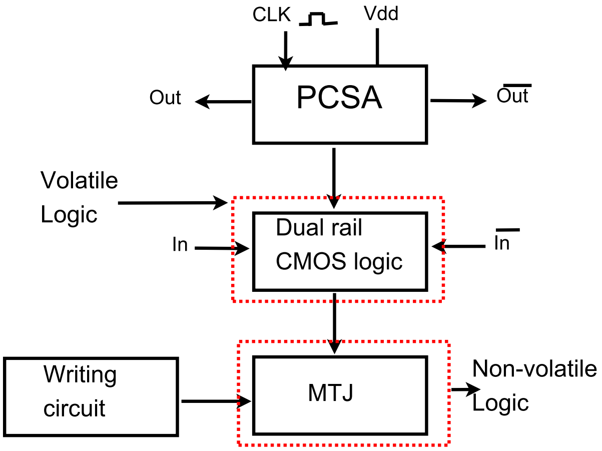

Fig. 2 Structure of existing LIM-based CMOS/MTJ circuits

CMOS/MTJ-based Logic-In-Memory (LIM) circuits

Figure 2 shows the structure of the existing Logic-In-Memory (LIM)-based CMOS/MTJ circuits. The LIM architecture consists of a Pre-Charged Sense Amplifier (PCSA) circuit which is used for sensing the outputs. The dual-rail CMOS logic tree is used to evaluate the inputs and the MTJs are used to store the non-volatile data.

Differential Power Analysis attack

Differential Power Analysis (DPA) attack is one of the most widely used hardware attack to reveal the secret key stored in the cryptographic device. DPA attack is used to reveal the secret key stored in the cryptographic device by correlating the instantaneous power consumed by the device with the input data. To guess the key, DPA uses statistical methods and evaluates the power traces with uniform plain texts.

Information Leakage in Pre-charge Sense Amplifier-Based CMOS/MTJ Circuits

This section explains the information leakage in the Pre-charge Sense Amplifier (PCSA)-based CMOS/MTJ circuit. As an example, the information leakage in the PCSA-based CMOS/MTJ circuit is illustrated by PCSA-based CMOS/MTJ XOR gate.

The operation of PCSA is explained through the existing PCSA-based CMOS/MTJ XOR gate (Fig. 3) [4, 5]. The PCSA works in two phases depending on CLK: (i) when CLK is set to “0”, the outputs (XOR, XNOR) are pre-charged to “1”; (ii) when CLK is set to “1”, the output voltages start discharging to ground. However, due to the difference in resistances of the different configuration of

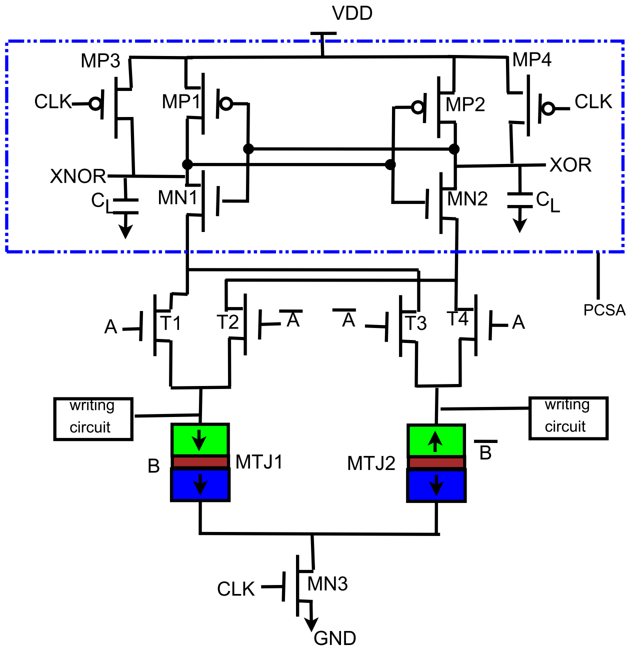

Fig. 3 Existing PCSA-based CMOS/MTJ XOR gate [4, 5]

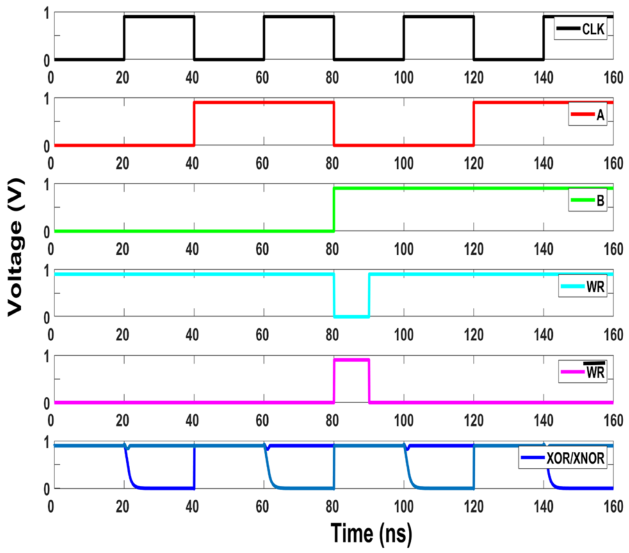

Fig. 4 Transient waveform of existing PCSA-based XOR gate

the MTJ (parallel and anti-parallel), the discharge speed will be different for each branch. For example, if the MTJ1 is configured in anti-parallel configuration and MTJ2 is configured in parallel configuration, then $R_{MTJ1} > R_{MTJ2}$. Due to the difference in resistances between R_{MTJ1} and R_{MTJ2}, the discharge current through MTJ2 will be greater than MTJ1. When XNOR becomes less than the threshold switching voltage of the inverter composed by MP2 and MN2, XOR will be charged to “1” and XNOR will be discharged to “0”.

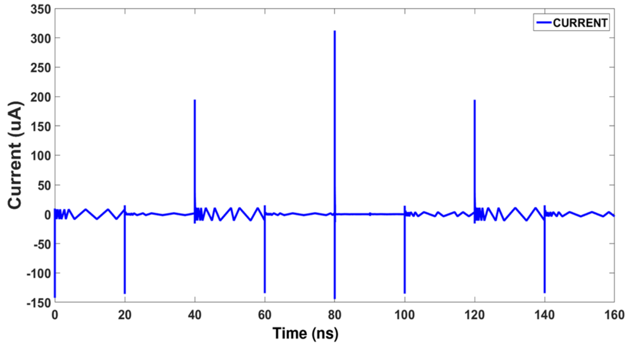

Fig. 5 Current consumption of PCSA-based CMOS/MTJ XOR gate for input in Fig. 4

As we can see in Fig. 5, during the input change in MTJ, PCSA-based CMOS/MTJ circuit consumes huge current. The current consumption during the writing of data to MTJ can reveal the data stored in MTJ which can be vulnerable to DPA attack.

Proposed Secure MTJ/CMOS Logic (SMCL) circuits

This section explains the operation of the proposed Secure MTJ/CMOS Logic (SMCL) circuits. In the proposed SMCL circuit, the MTJs are masked from the power supply during the data are written to the MTJ. If the MTJ value is not changed, then both PCSA and SMCL circuits will consume uniform power. However, our proposed SMCL-based MTJ/CMOS logic gates are more energy-efficient than the existing PCSA-based MTJ/CMOS logic gates.

Operation of the Proposed SMCL Circuit

This section explains the operation of the proposed SMCL circuit. The circuit operation of the proposed SMCL circuit is explained by the operation of an XOR gate. Figure 6 shows the schematic diagram of the proposed SMCL-based XOR gate. Transistor MP1 is used to disconnect the MTJ from V_{dd} when the data are written in it. Transistors MP2, MP3, MN1, and MN2 are used to stabilize the outputs. Transistors MP4 and MP5 are used for charge sharing the outputs.

The operation of the proposed SMCL circuit is explained with the example of XOR gate through each phase of the clock.

Charge-sharing phase: During the charge-sharing phase, CLK = 0, $\overline{CLK}$ = 1. When CLK = 0, transistor MP4

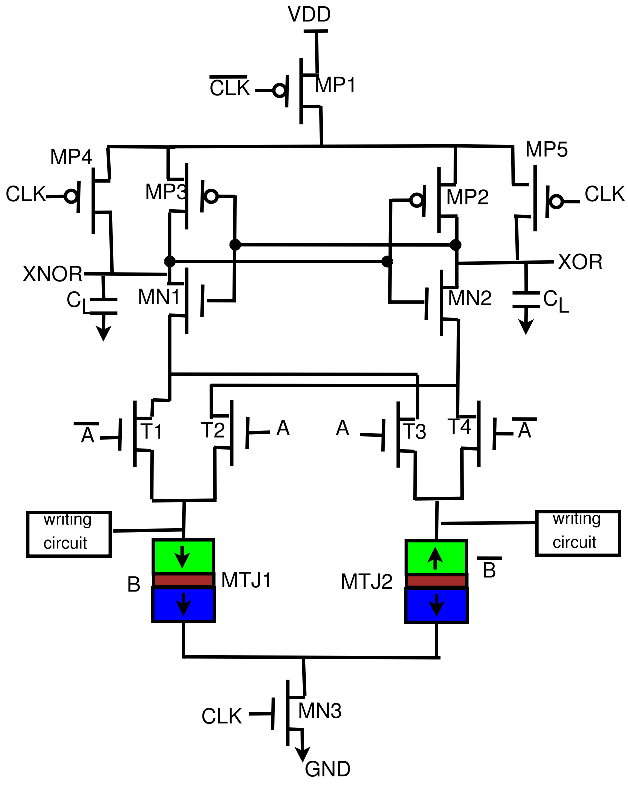

Fig. 6 Schematic of the proposed SMCL-based XOR gate

and MP5 will be turned ON. Since, the proposed SMCL XOR gate is dual rail in nature, the outputs will be shared between the output nodes during the charge-sharing phase. During the charge-sharing phase, MP1 is turned OFF to mask the MTJ while writing the data in the MTJs. Moreover, in the proposed SMCL circuits, the outputs are pre-charged to $V_{dd}/2$ unlike the conventional PCSA MTJ/CMOS circuit where the outputs are pre-charged to V_{dd}. Since, the outputs are pre-charged to $V_{dd}/2$, the proposed SMCL circuits consume low power as compared to the existing PCSA-based MTJ/CMOS circuits.

Evaluate phase: During the evaluate phase, CLK = 1, $\overline{CLK} = 0$. In this phase, transistor MP1 and MN3 will be turned ON and MP4 and MP5 will be turned OFF. For analysis, let us assume that the input A = 0, B = 1. When A = 0, transistor T2 and T3 will be turned OFF, while T1 and T4 will be turned ON. The resistance of MTJ1 will be less as compared to resistance of MTJ2. When CLK = 1, the charge stored in XNOR output will be discharged to ground through T1 and MTJ2 which makes transistor MN2 to turn OFF. Since, the transistor MN2 is turned OFF, the XOR output will be charged to V_{dd}. The transient waveforms of the proposed SMCL XOR gate are shown in Fig. 7. Figure 8 shows the uniform current consumption of the proposed SMCL XOR gate. Figure 9 shows the schematic of the proposed SMCL AND gate.

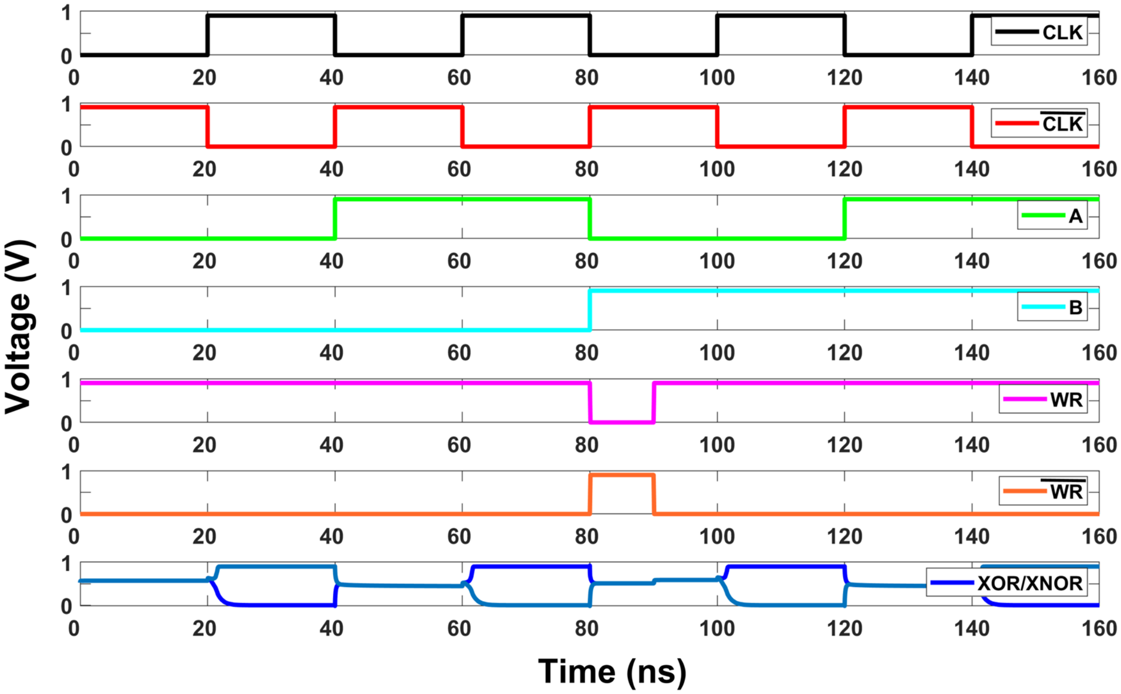

Fig. 7 Transient analysis of the proposed SMCL-based XOR gate

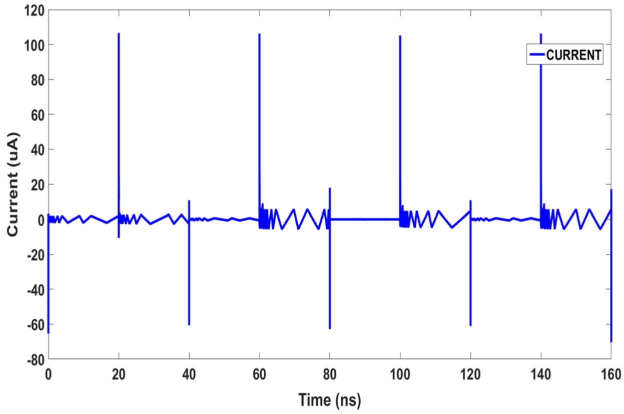

Fig. 8 Current consumption of the proposed SMCL-based XOR gate

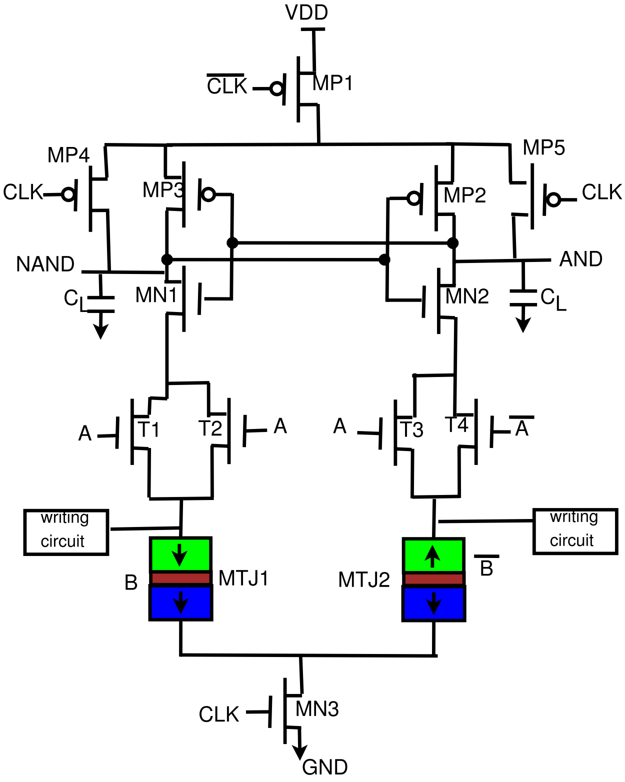

Fig. 9 Schematic of the proposed SMCL AND gate

Simulation Results of SMCL-Based Logic Gates

This section presents the simulation results of the proposed SMCL circuits. Simulations are performed using Cadence Spectre simulator with 45 nm standard CMOS technology with perpendicular anisotropy CoFeB/MgO MTJ model [16]. The MTJ device parameters used for simulations in this work can be found in [10]. The simulations are performed at 50 MHz with $V_{dd} = 0.9$V and load capacitor is 1fF.

The sizes of all the transistors are W/L = 120nm/45nm. Table 2 gives the comparison of the PCSA-based XOR gate and the proposed SMCL XOR gate. From Table 1, we can see that the proposed SMCL XOR gate has 50% of energy savings as compared to the existing PCSA-based XOR gate which is same as the results obtained in theoretical analysis.

Table 2 shows the comparison of the PCSA-based AND gate and the proposed AND gate. From Table 2, we can see that the proposed SMCL AND gate has 42.7% and 50% of power and energy savings as compared to the existing PCSA-based AND gate.

Furthermore, we preformed a reliability analysis on the SMCL XOR gate. We varied our TMR and V_{dd} and determined that at $V_{dd} = 0.9$ and TMR values ranging from 50 to 500, the output is correct for each combination. For $V_{dd} = 0.8$, the output produces incorrect results at TMR values 350 and above. For $V_{dd} = 0.7$, the output produces incorrect results at TMR values 300 and above.

Security Metrics Analysis of the MTJ/CMOS Gates

This section discusses the security metric analysis of the MTJ/CMOS gates. The parameter Normalized Energy Deviation (NED), defined as $(E_{\max} - E_{\min})/E_{\max} \times 100$, is used to indicate the percentage difference between minimum and maximum energy consumption for all possible input transitions. Normalized Standard Deviation (NSD) indicates the energy consumption variation based on the inputs, and it is calculated as $\frac{\sigma_E}{\bar{E}} \times 100$. $\bar{E}$ denotes the average energy dissipation for various input transitions. In general, 'n' input gate will have 2^{2n} possible input transitions. For example, 2 input gate will have 16 input transitions. σ_E denotes the standard deviation of the energy

Table 1 Performance comparison of PCSA-based XOR gate and proposed SMCL XOR gate

	PCSA-based XOR [4]	Proposed SMCL XOR gate	% impr.
Avg. energy (fJ)	3.604	1.871	50
Avg. power (nW)	40.34	23.1	42.7
Device count	11MOS +2MTJ	12MOS+2MTJ	–

Table 2 Performance comparison of PCSA-based AND gate and proposed SMCL AND gate

	PCSA-based AND [4]	Proposed SMCL AND gate	% impr.
Avg. energy (fJ)	3.414	1.768	50
Avg. power (nW)	38.24	21.37	44.11
Device count	10MOS +2MTJ	12MOS+2MTJ	–

Table 3 Simulated and calculated results for XOR gate for various DPA-resistant adiabatic logic families

Logic family	PCSA-based XOR gate	Proposed XOR gate
$E_{\min}$ (fJ)	2.9	1.431
$E_{\max}$ (fJ)	6.3	1.85
NED (%)	53.9	22.6
NSD(%)	61.27	12.3

Table 4 Simulated and calculated results for AND gate for various DPA-resistant adiabatic logic families

Logic family	PCSA-based AND gate	Proposed SMCL AND gate
$E_{\min}$ (fJ)	2.77	1.25
$E_{\max}$ (fJ)	6.56	2.9
NED (%)	57.7	56.8
NSD(%)	64.33	32.2

consumed dissipated by the circuit, and it is shown as $\sqrt{\frac{\sum_{i=1}^{n}(E_i-\bar{E})^2}{n}}$.

From Tables 3 and 4, we can see that the NED and NSD values for the proposed SMCL circuit are very less than the existing PCSA-based MTJ/CMOS circuit. Lower the values of NED and NSD, higher the resilience of the circuit towards power analysis attack.

Analysis of SMCL-based PRESENT-80 Cryptographic Hardware

This section discusses the energy-efficiency and security analysis of the proposed SMCL-based PRESENT-80 cryptographic hardware. MTJ/CMOS logic circuits is not energy-efficient as compared to the CMOS-based logic circuit when data stored in MTJs toggle [14]. To minimize this issue, we look to Look-Up Table-based design, so that the MTJs are only switched once. Numerous MTJ-based look-up tables have been proposed and shown to be energy efficient [19, 21]. As proposed in [11], we have used the Look-Up Table (LUT) method to implement PRESENT-80 cryptographic hardware [2, 15] in proposed SMCL logic.

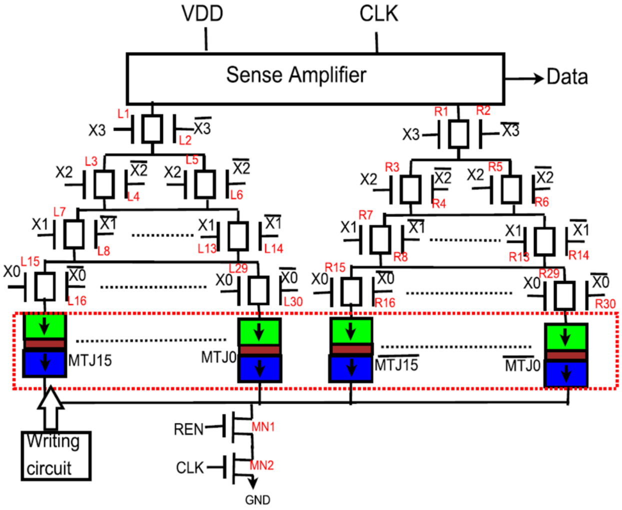

Fig. 10 Circuit design of the MTJ-based LUT with four selection lines

Figure 10 shows the LUT-based SBOX with four selection lines.

Figure 11 shows the sense amplifier circuit to read the data stored in MTJ. Figure 11a shows the existing PCSA-based sense amplifier and Figure 11b shows the proposed SMCL-based sense amplifier circuit. As discussed in previous section, SMCL-based circuit is more energy-efficient than the PCSA-based circuit due to pre-charging the output nodes to VDD/2. Therefore, to have charge sharing, we are increasing the width MP3 and MP4 to 6 times than the other PMOS transistors (refer Fig. 11b). As we know that increasing width of transistors reduces the resistance which helps to charge share the output nodes fast.

Figure 12 shows the transient waveforms of the PRESENT-S-box circuit [2, 15] implemented using the proposed SMCL logic-based sense amplifier circuit. The MTJs in the SMCL-based PRESENT-80 S-box circuit are used to store the S-box data, while the CMOS logic is used to choose the corresponding data from the MTJ. SMCL-based sense amplifier is used to read the data stored in the MTJs. As discussed in previous section, SMCL-based circuits precharge the output nodes to Vdd/2 which improves its energy efficiency as compared to existing PCSA-based circuits. In Fig. 12, X0, X1, X2, and X3 represent the input to the S-box, while S0, S1, S2, and S3 represent the output of the SMCL-based PRESENT-80 S-box circuit.

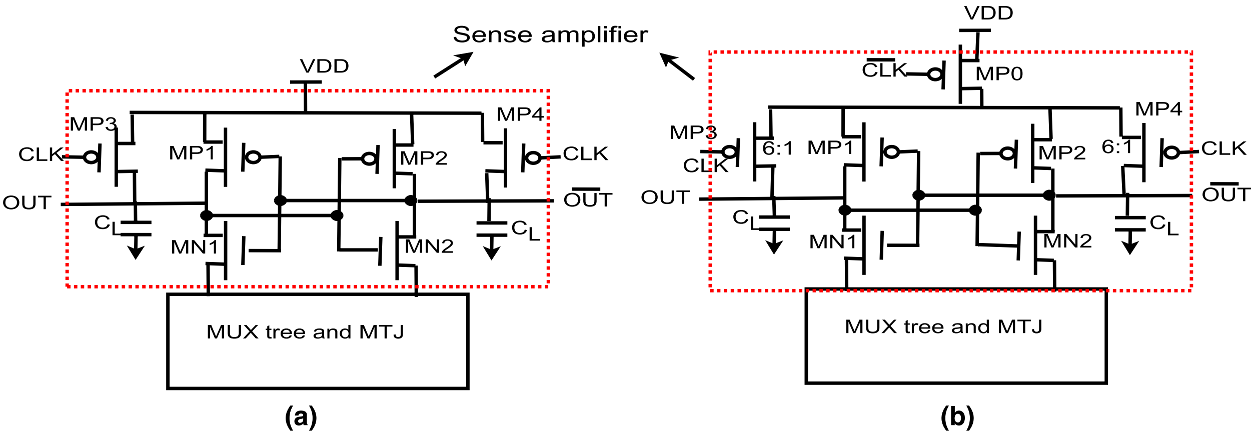

Fig. 11 **a** PCSA-based sense amplifier and **b** proposed SMCL-based sense amplifier circuit

Fig. 12 Transient waveforms of the PRESENT S-Box circuit implemented using proposed SMCL logic-based sense amplifier

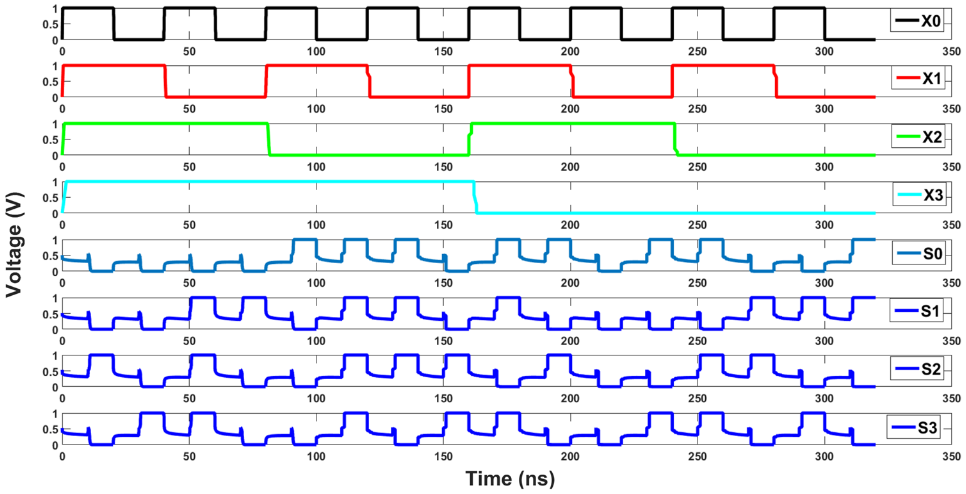

Table 5 Energy consumption comparison of PRESENT-80 S-box circuit

Implementation	Energy/cycle	Avg. power	Energy savings
PCSA-based MTJ/CMOS [11]	24.3 fJ	1.23 μW	45%
CMOS	32.4 fJ	1.72 μW	59%
Proposed SMCL-based MTJ/CMOS	13.4 fJ	0.74 μW	–

Table 6 Energy consumption comparison of PRESENT-80 cryptographic hardware

Implementation	Energy/cycle	Avg. power	Energy savings
PCSA-based MTJ/CMOS [11]	402.96 fJ	20.65 μW	42.18%
Conventional CMOS	566.8 fJ	28.336 μW	59%
Proposed SMCL-based MTJ/CMOS	232.96 fJ	12.65 μW	–

Energy-Efficiency Analysis of SMCL-Based PRESENT-80 Cryptographic Hardware

This section presents the energy-efficiency analysis of the SMCL-based PRESENT-80 cryptographic hardware. We initially implemented a PRESENT-80 S-box circuit using the existing state-of-art PCSA-based MTJ/CMOS circuit [11] and proposed SMCL-based circuits. Furthermore, we have also implemented CMOS-based PRESENT-80 S-box circuit to compare its energy efficiency with the proposed

SMCL-based PRESENT-80 S-box circuit. To characterize the CMOS and MTJ/CMOS designs in equivalent condition, 32 D Flip-Flops are added to CMOS-based one round of PRESENT-80 cryptographic hardware to synchronize the outputs with clock signal as PCSA-based MTJ/CMOS circuits are naturally synchronized. Furthermore, it has to be noted that in our MTJ/CMOS-based PRESENT S-box design, data are written only one time. Once the data are written in the S-box circuit, there is no need to flip the data stored in the MTJs. The constant storage of data in MTJs without toggling helps in improving the overall energy-efficiency of the MTJ/CMOS circuits.

Table 5 shows the energy consumption comparison of the PRESENT-80 S-box circuit implemented using PCSA-based MTJ/CMOS [11], conventional CMOS circuit, and proposed SMCL-based MTJ/CMOS circuit. From the table, we can see that the proposed SMCL-based MTJ/CMOS implementation of PRESENT-80 S-box circuit saves up to 59% of energy as compared to the conventional CMOS-based PRESENT-80 S-box circuit. Moreover, the proposed SMCL-based MTJ/CMOS-based PRESENT-80 S-box circuit saves up to 45% of energy/cycle compared to PCSA-based MTJ/CMOS design proposed in [11].

Furthermore, in this research, we have also implemented one round of PRESENT-80 cryptographic hardware with the proposed SMCL-based MTJ/CMOS circuit. Table 6 shows the energy consumption comparison of the PRESENT-80 cryptographic hardware implemented using PCSA-based MTJ/CMOS, conventional CMOS-based circuits, and proposed SMCL-based MTJ/CMOS. From our simulations, we can see that the proposed SMCL-based MTJ/CMOS saves up to 42.18% of energy as compared to the PCSA-based MTJ/CMOS circuits proposed in [11]. Furthermore, SMCL-based MTJ/CMOS PRESENT-80 cryptographic hardware saves up to 59% of energy as compared to the conventional CMOS-based PRESENT-80 cryptographic hardware.

Security Analysis of SMCL-Based PRESENT-80 Cryptographic Hardware

This section presents the security analysis of the SMCL-based PRESENT-80 cryptographic hardware. Figure 13 shows the current consumption of the PRESENT-80 S-box circuit implemented using conventional CMOS circuits, proposed SMCL-based MTJ/CMOS circuits, and PCSA-based MTJ/CMOS circuits. From the Fig. 13, we can see that the conventional CMOS-based PRESENT-80 S-box circuit consumed non-uniform power consumption which makes it susceptible to DPA attack. In this research, we have used the look-up table-based method (refer [11]) to implement the cryptographic circuit using MTJ/CMOS circuit. From Fig. 13, we can see that the proposed SMCL MTJ/CMOS-based PRESENT-80 S-box circuit has reduced uniform current consumption as compared to the PCSA MTJ/CMOS-based PRESENT-80 S-box circuit. Figure 14 shows the non-successful DPA attack on the proposed SMCL-based PRESENT-80 S-box circuit with key = 06.

Conclusion

In this paper, we have shown the susceptibility of MTJ/CMOS circuits to power analysis attacks where the attacker uses the power traces to reveal the secret key. To improve the security of the existing MTJ/CMOS circuits against power analysis attacks, we have proposed a novel Secure MTJ/CMOS Logic (SMCL) circuit which has uniform power consumption. The proposed SMCL consumes uniform power by masking the MTJ during the write operation from the power supply, thereby thwarting the power analysis-based side-channel attacks. From our simulations, we have observed that the proposed SMCL-based PRESENT-80

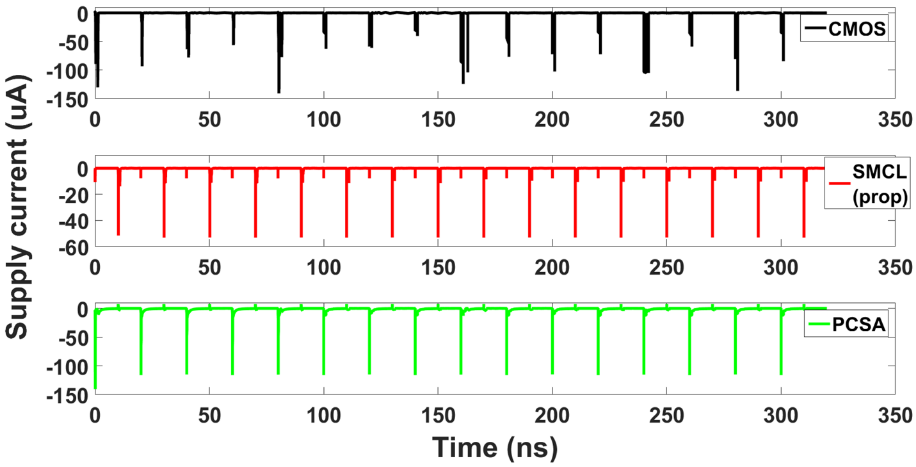

Fig. 13 Current consumption of the CMOS, proposed SMCL-based MTJ/CMOS, and PCSA-based MTJ/CMOS implementation of PRESENT S-Box

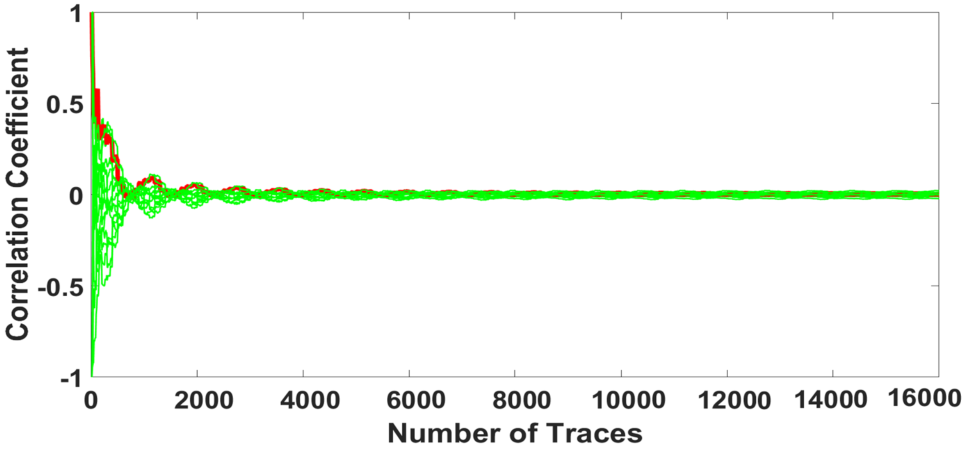

Fig. 14 A non-successful DPA attack on PRESENT S-box implemented using proposed SMCL logic with key = 06

cryptographic hardware has about 42% and 59% of energy savings as compared to the PCSA-based MTJ/CMOS and conventional CMOS-based implementation. Furthermore, we have also performed the DPA attack on the SMCL-based PRESENT-80 and the secret key was not revealed after 16000 power traces. The proposed SMCL will find applications in the design of sudden power outage resilient non-volatile DPA secure processors.

Acknowledgements This research was partially supported by Grants from Kentucky Science and Engineering Foundation per Grant Agreement under Grant KSEF-3526-RDE-019.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Behin-Aein B, Wang JP, Wiesendanger R. Computing with spins and magnets. MRS Bull. 2014;39(08):696–702.
2. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. Present: an ultra-lightweight block cipher. In: International Workshop on Cryptographic Hardware and Embedded Systems; 2007. pp. 450–466. Springer
3. Chakraborty A, Mondal A, Srivastava A. Correlation power analysis attack against stt-mram based cyptosystems. IACR Cryptol. ePrint Arch. 2017;2017:413.
4. Deng E, Zhang Y, Klein JO, Ravelsona D, Chappert C, Zhao W. Low power magnetic full-adder based on spin transfer torque mram. IEEE Trans. Magn. 2013;49(9):4982–7.
5. Gang Y, Zhao W, Klein JO, Chappert C, Mazoyer P. A high-reliability, low-power magnetic full adder. IEEE Trans. Magn. 2011;47(11):4611–6.
6. Iyengar A, Ghosh S, Rathi N, Naeimi H. Side channel attacks on sttram and low-overhead countermeasures. In: Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2016 IEEE International Symposium on. 2016; pp. 141–146. IEEE
7. Kang W, Lv W, Zhang Y, Zhao W. Low store power high-speed high-density nonvolatile sram design with spin hall effect-driven magnetic tunnel junctions. IEEE Trans. Nanotechnol. 2017;16(1):148–54.
8. Kang W, Zhang Y, Wang Z, Klein JO, Chappert C, Ravelosona D, Wang G, Zhang Y, Zhao W. Spintronics: emerging ultra-low-power circuits and systems beyond mos technology. ACM J. Emerg. Technol. Comput. Syst. (JETC). 2015;12(2):16.
9. Kocher P, Jaffe J, Jun B. Differential power analysis. In: Advances in cryptology–CRYPTO'99.Springer. 1999; pp. 789.
10. Kumar SD, Thapliyal H. Security evaluation of mtj/cmos circuits against power analysis attacks. In: 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS). 2017; pp. 117–122
11. Kumar SD, Thapliyal H. Exploration of non-volatile mtj/cmos circuits for dpa-resistant embedded hardware. IEEE Trans. Magn. 2019;55(12):1–8.
12. Mangard, S., Oswald, E., Popp, T. Power analysis attacks: revealing the secrets of smart cards. Springer Sci. Bus. Media. 2008;31
13. Moodera JS, Kinder LR, Wong TM, Meservey R. Large magnetoresistance at room temperature in ferromagnetic thin film tunnel junctions. Phys. Rev. Lett. 1995;74(16):3273.
14. Ren F, Markovic D. True energy-performance analysis of the mtj-based logic-in-memory architecture (1-bit full adder). IEEE Trans. Electron Dev. 2010;57(5):1023–8.
15. Rolfes C, Poschmann A, Leander G, Paar C. Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents. In: International Conference on Smart Card Research and Advanced Applications. Springer. 2008; pp. 89–103.
16. Wang Y, Cai H, de Barros Naviner LA, Zhang Y, Zhao X, Deng E, Klein JO, Zhao W. Compact model of dielectric breakdown in spin-transfer torque magnetic tunnel junction. IEEE Trans. Electron Dev. 2016;63(4):1762–7.
17. Winograd, T., Salmani, H., Mahmoodi, H., Gaj, K., Homayoun, H. Hybrid stt-cmos designs for reverse-engineering prevention. In: Proceedings of the 53rd Annual Design Automation Conference. ACM. 2016; p. 88.
18. You W, Yue Z, Jacques-Olivier K. Thibaut Devolder, Dafiné Ravelosona, Claude Chappert. Weisheng Zhao: compact model for perpendicular magnetic anisotropy magnetic tunnel junction. 2017.
19. Zand R, Roohi A, Fan D, DeMara RF. Energy-efficient nonvolatile reconfigurable logic using spin hall effect-based lookup tables. IEEE Trans. Nanotechnol. 2016;16(1):32–43.
20. Zand R, Roohi A, Salehi S, DeMara RF. Scalable adaptive spintronic reconfigurable logic using area-matched mtj design. IEEE Trans. Circ. Syst. II Express Briefs. 2016;63(7):678–82.

21. Zhao W, Belhaire E, Chappert C, Jacquet F, Mazoyer P.: New non-volatile logic based on spin-mtj. Physica Status Solidi (a). 2008;205(6):1373–1377
22. Zhao W, Moreau M, Deng E, Zhang Y, Portal JM, Klein JO, Bocquet M, Aziza H, Deleruyelle D, Muller C, et al. Synchronous non-volatile logic gate design based on resistive switching memories. IEEE Trans. Circ. Syst. I: Regular Pap. 2014;61(2):443–54.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.