SN Computer Science (2020) 1:199
https://doi.org/10.1007/s42979-020-00212-0

ORIGINAL RESEARCH

Performance and Security Evaluation of S-Box Using Current-Pass Optimized Symmetric Pass Gate Adiabatic Logic

Hiroki Koyasu[1] · **Yasuhiro Takahashi**[1]

Received: 26 April 2020 / Accepted: 29 May 2020 / Published online: 11 June 2020

Abstract
Secure adiabatic logics are identified as the optimal solution for cryptographic modules. We previously proposed an adiabatic logic called Current-Pass Optimized Symmetric Pass Gate Adiabatic Logic (CPO-SPGAL). The proposed CPO-SPGAL realizes a flat current waveform by considering the current path compared with conventional adiabatic logics. In this paper, to confirm more details about countermeasure against power analysis attacks, we compare S-box circuits based on the conventional and proposed adiabatic logics which are implemented using 0.18 µm standard CMOS. From the SPICE simulation for correlation power analysis (CPA), 409,600 power consumption traces are obtained, and the hamming distance/weight are calculated. The simulation results show that the proposed S-box is more resistant to CPA attacks than the existing adiabatic S-boxes.

Keywords Adiabatic logic · Dual rail logic · Secure · Current trace

Introduction

A new era of Internet of Things (IoT) has arrived and much information is transmitted through various cryptographic devices. In cryptographic devices, there are cases requiring countermeasures at the cell/gate-level design that are resilient to power analysis attacks (PAA). In the past 2 decades, numerous designs of PAA resistant logic (e.g., SABL [1] and TDPL [2]) have been presented. In addition, adiabatic switching-based energy-efficient PAA-resistant logics have been proposed [3–7]. In particular, our previously proposed adiabatic logic called Current-Pass Optimized Symmetric Pass Gate Adiabatic Logic (CPO-SPGAL) is a cryptographic logic gate which has the characteristic of low power and high security [7].

This paper presents an extended version of "Current-Pass Optimized Symmetric Pass Gate Adiabatic Logics" [7]. Herein, we evaluate the performance and security a S-box circuit using our previously proposed adiabatic logic, CPO-SPGAL. The proposed circuit logic focuses on the current pass through the input section and optimizes the pass by dummy input transitions, as shown in Figs. 1 and 2, at the time of cryptographic processing. As a result, the proposed circuit is successful in reducing the current fluctuation and improving the security against power analysis attacks. For more details about mechanism of the dummy pass section, Sect. 4 will be described.

The rest of this paper is organized as follows. Section 2 briefly describes a basic theory of adiabatic switching. Section 3 shows the conventional adiabatic logic, SPGAL, and its logical function. Section 4 describes the proposed logic, CPO-SPGAL, and in Section 5, the S-box circuit design for advanced encryption standard (AES) is described. Section 6 shows the simulation results compared with the conventional adiabatic logics. Finally, in Sect. 7, the conclusions are drawn.

Basic Theory of Adiabatic Switching

Adiabatic switching [8] is a circuit design technique that reduces the energy consumption of the transistor using periodic (e.g., trapezoidal wave) power supply. In addition, as the energy stored in the load capacitor is returned to the power supply, the adiabatic logic reduces the energy lost compared to the conventional static CMOS logic; hence, this

✉ Yasuhiro Takahashi
yasut@gifu-u.ac.jp

[1] Department of EECE, Faculty of Engineering, Gifu University, 1-1 Yanagido, Gifu 501-1193, Japan

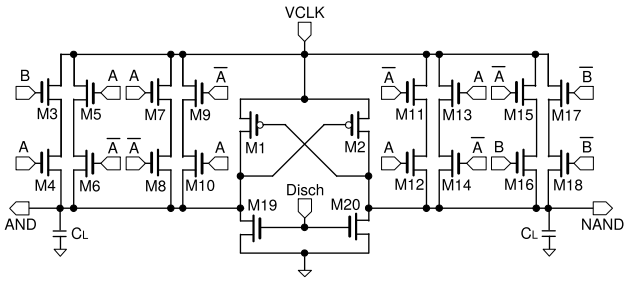

Fig. 1 Proposed logic: CPO-SPGAL-NAND/AND

logic is suitable for low power consumption IoT devices and encryption logic circuits.

Figure 3 shows the RC model of the conventional CMOS, where R is the equivalent resistance of the PMOS pull-up (or NMOS pull-down) network and C is the load capacitance. In the conventional CMOS logic, the dissipated energy in R is given by:

$$E_{\mathrm{CMOS}} = R\int_0^{\infty} I_{\mathrm{CMOS}}^2 \mathrm{d}t = \frac{1}{2}CV_{\mathrm{dd}}^2. \tag{1}$$

On the other hand, the energy dissipation in the channel resistance R of the adiabatic logic (shown in Fig. 4) is as:

$$\begin{aligned} E_{\mathrm{Adia}} &= R\int_0^{\infty} I_{\mathrm{adia}}^2 \mathrm{d}t \\ &= \frac{R(CV_{\mathrm{dd}})^2}{\tau}\left[1 - \frac{RC}{\tau}\left(1 - e^{-\frac{\tau}{RC}}\right)\right] \\ &\approx \frac{RC}{\tau}CV_{\mathrm{dd}}^2, \end{aligned} \tag{2}$$

where τ is the time period of the power supply. To compare the E_{CMOS} and E_{Adia}, if τ is a long time, the energy of adiabatic logic is approximately equal to "0." Thus, to achieve low power designs, adiabatic logic is one of the noted technologies.

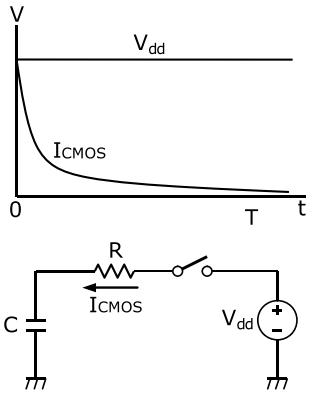

Fig. 3 CMOS equivalent RC model and its voltage/current waveform

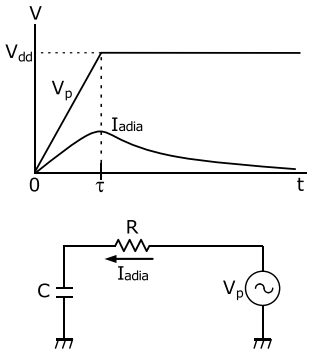

Fig. 4 Adiabatic equivalent RC model and its voltage/current waveform

SPGAL

This section briefly describes the SPGAL proposed in [6]. Figure 5 shows the inverter/buffer circuit using SPGAL. The timing chart of the buffer is depicted in Fig. 6. This logic family uses a 4-phase timing, that is wait/discharge (T1),

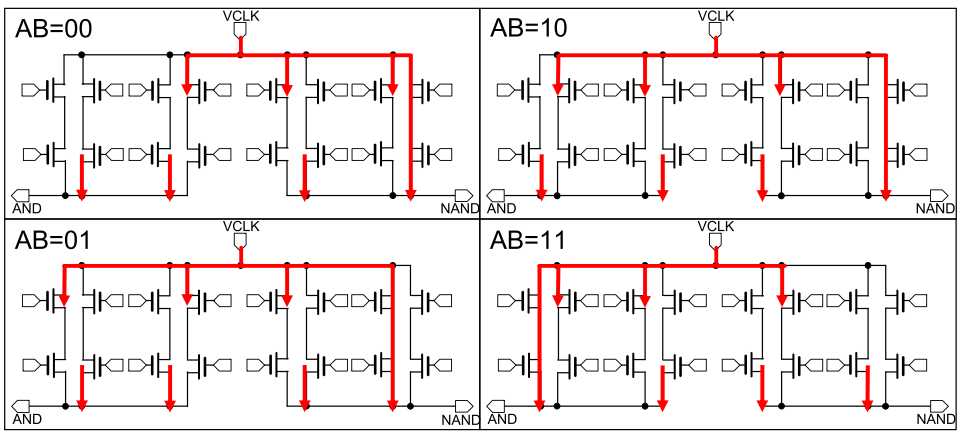

Fig. 2 Current pass of each CPO-SPGAL-NAND/AND transitions

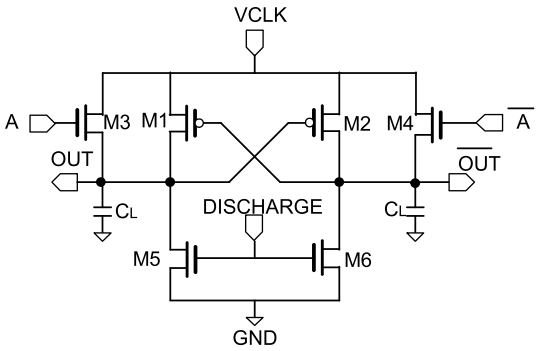

Fig. 5 SPGAL input/buffer configuration

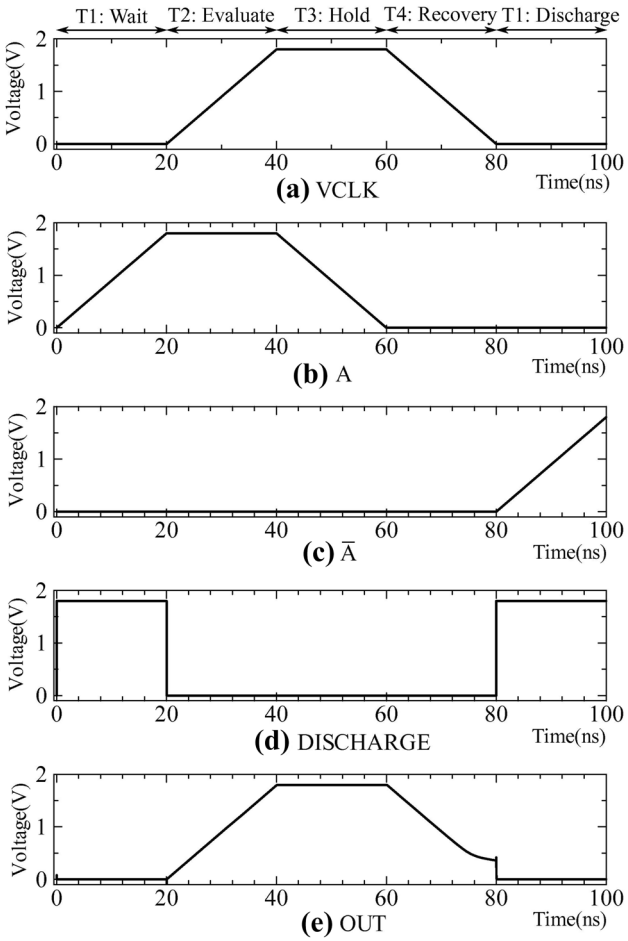

Fig. 6 Timing chart of SPGAL input/buffer

evaluate (T2), Hold (T3), and recovery (T4). To explain the functionality of SPGAL inverter/buffer, we assume that all the nodes are at ground (GND) level.

T1 (Wait phase) At T1, VCLK is at GND. Input A slowly increases from 0 to Vdd. In general, for NMOS to be turned on, Vgs must be greater than Vtn, where Vgs is the voltage across the gate and the source of the NMOS and Vtn is the threshold voltage of the NMOS. When the input A is greater than Vtn, the transistor M3 is turned on. Since the source and drain of M3 is at GND, there is no current flow through the transistor. In this phase, discharge signal causes the transistors M5 and M6 to be turned on thereby discharging the charges stored (from the previous cycle) in the load capacitor to ground. All other transistors are off in this phase.

T2 (Evaluate phase) At T2, input A is at Vdd. The discharge signal and $\overline{A}$ are at GND. VCLK slowly increases from 0 to Vdd slowly charges the output load capacitor. At any instant of time, the potential of the clock VCLK will be greater than the potential of the output node in this phase. Hence, the voltage at the output node will always follow the clock VCLK in this phase which makes the OUT node to act as the source and the clock to act as the drain of the M3 transistor. For M1, the clock VCLK acts as the source and the OUT node acts as the drain of the transistor.

T3 (Hold phase) At T3, the clock VCLK is at Vdd. The transistor M3 is turned off without non-adiabatic loss by slowly decreasing the inputs from Vdd to GND. The output in this phase will be same as that in T2.

T4 (Recovery phase) At T4, the clock VCLK slowly decreases from Vdd to GND. The charge stored in the output load capacitor is slowly recovered back to the clock through M1. When the output voltage is reduced to Vtp, M1 is turned off and the output voltage will stay at Vtp at the end of this phase. Charge stored in the output node at the end of the first cycle (T1–T4) is discharged to the ground in the next phase of the clock (T5 = T1) through M5 or M6 transistor using the discharge signal. Resetting the output node to zero reduces the correlation between the current supplied and the data evaluated.

The disadvantage of the SPGAL logic is that the multi-input logic (e.g., AND/NAND) has source current fluctuation when input transition changes. Let us explain the individual processes in more detail. Figures 7 and 8 show the circuit configuration of SPGAL AND/NAND and the current pass model for various input transitions, respectively. From these figures, we found that SPGAL has a different current pass depending on the input transitions. For example,

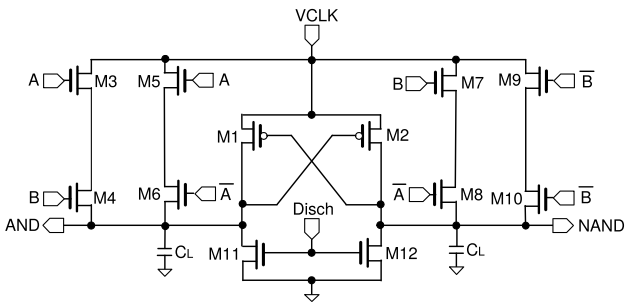

Fig. 7 SPGAL NAND/AND circuit

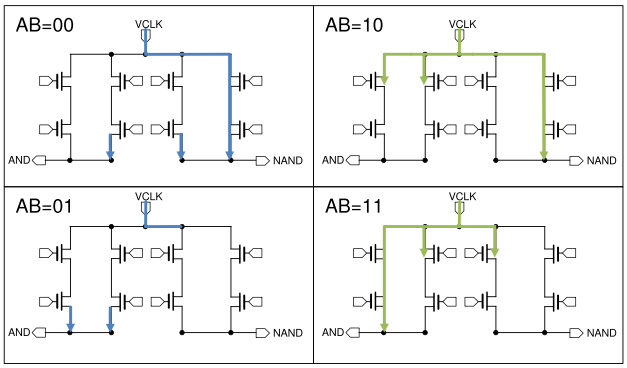

Fig. 8 SPGAL NAND/AND circuit

at AB = 00 input transition, two short current passes are generated on the "bottom-side" of the input function block, whereas, at AB = 10, two passes are generated on the "upper-side."

CPO-SPGAL

Figure 9 shows the proposed SPGAL based adiabatic logic, called as the current pass optimized SPGAL (CPO-SPGAL). This logic family uses 4-phase timing as with SPGAL. In the proposed circuit, the dummy pass section (which is constructed using cascode-connected MOS transistors) is added to the existing SPGAL's input function block. To add the dummy transistors, the proposed logic has a current pass that is independent of the input data, as shown in Fig. 10.

Figure 11 depicts the conventional and proposed supply current waveforms for various input transitions. The proposed circuit consumes uniform current irrespective of the input data being processed, when compared to the conventional circuit. Also, in Fig. 11, at 80 ns (or 160, 240, 320, ...), we can find that leakage current is appeared as small peak waveform. Compared with the conventional, leakage current of the proposed becomes uniform waveform.

S-Box Circuit Design for AES

To compare the performance of the conventional circuit and the proposed circuit, we simulated the S-box circuit, as shown in Fig. 12 [9]. Three sub-components of the conventional composite field S-box circuit were converted into the PPRM form: the pre-inversion section, the inversion section, and the post-inversion section, as depicted top side of in Fig. 12. In the adiabatic S-box circuit, we apply three power clock supplies for each section, which completely avoid the glitch current, consume uniform transitional energy, and ensure significant energy reduction in our comparative results. The bottom side of Fig. 12 shows multi-stage PPRM

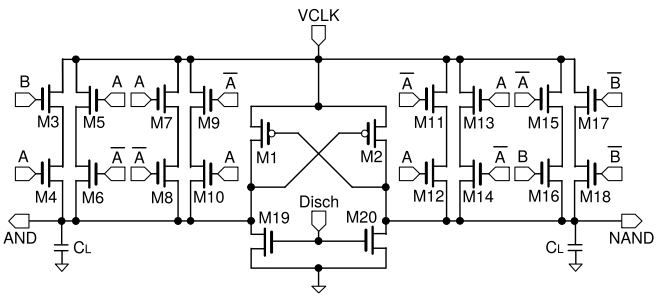

Fig. 9 Proposed logic: CPO-SPGAL-NAND/AND

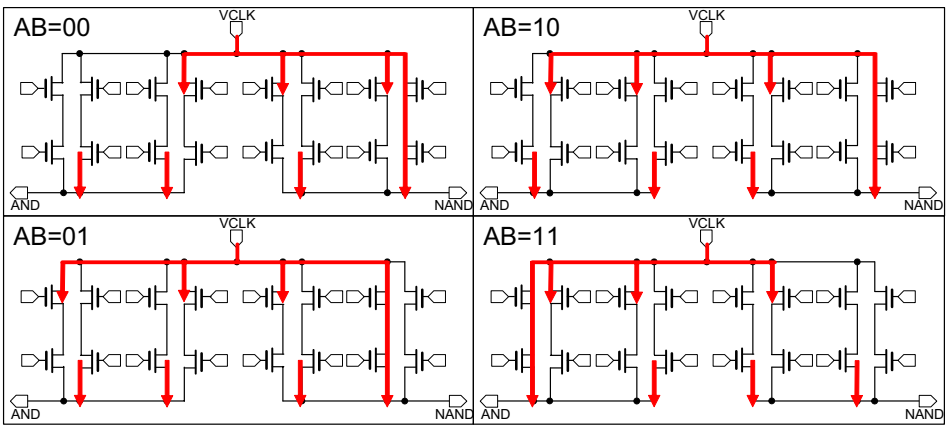

Fig. 10 Current pass of each CPO-SPGAL-NAND/AND transitions

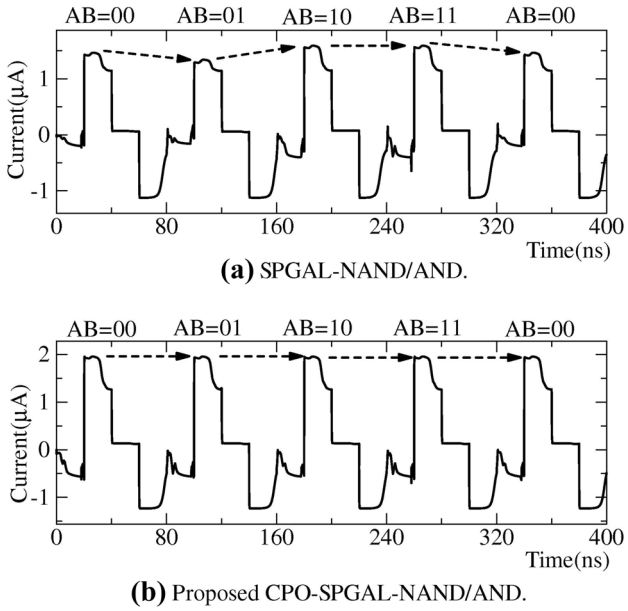

Fig. 11 Supply current waveforms for various input transitions

representation with the implementation of the adiabatic 8-bit S-box circuit.

The S-box circuit is a substitution table circuit that converts input data according to a certain rule into an output. This conversion is called SubBytes conversion of Advanced Encryption Standard (AES). The processing in AES is divided into four blocks: AddRoundKey, SubBytes, ShiftRows, and MixColumns, as shown in Fig. 13. In hardware AES, SubBytes conversion is the more complex.

This S-box circuit is designed and simulated in SPICE, such that the results are from the forward annotation simulation. Figure 14 shows a DUT S-box circuit. To evaluate index (see, Sect. 6.2), we measure the current, voltage, and power waveforms through SPICE. To evaluate CPA resistance (see, Sect. 6.4), their obtained hamming weight power consumption is calculated using Visual Basic for applications on Excel for the post-processing.

Simulation Results

Conventional Adiabatic Logics: CSSAL and SQAL

To evaluate the adiabatic logic performance compared with the different designs, we briefly describe the conventional adiabatic logics: charge-sharing symmetric adiabatic logic (CSSAL) [3] and DPA-secured quasi-adiabatic logic (SQAL) [4]. All results are evaluated in a SPICE simulation with 0.18-μm, 1.8-V standard CMOS process technology. The widths and the lengths of the transistors are 0.6 μm and 0:18 μm, respectively, for both the PMOS and NMOS transistors.

Figure 15 shows a CSSAL inverter/buffer circuit. The logic operation of CSSAL is described in the right side of Fig. 15 that at A(=In), Eval, Discharge ≥ Vt of the MOS transistor in the charge-sharing phase, all internal nodes are discharged to ground level before evaluation. This load balancing is the reason why CSSAL has uniform energy dissipation for all possible input transitions. Therefore, CSSAL logic's supply current transition has the same peak values and is able to consume uniformly low power for various input transitions.

Figure 16 shows an SQAL inverter/buffer circuit. The SQAL has a same circuit topology like the CSSAL. By optimally controlling discharge signal, SQAL has also uniform energy dissipation for all possible input transitions. However, as the output gate consists of two cross-coupled PMOS

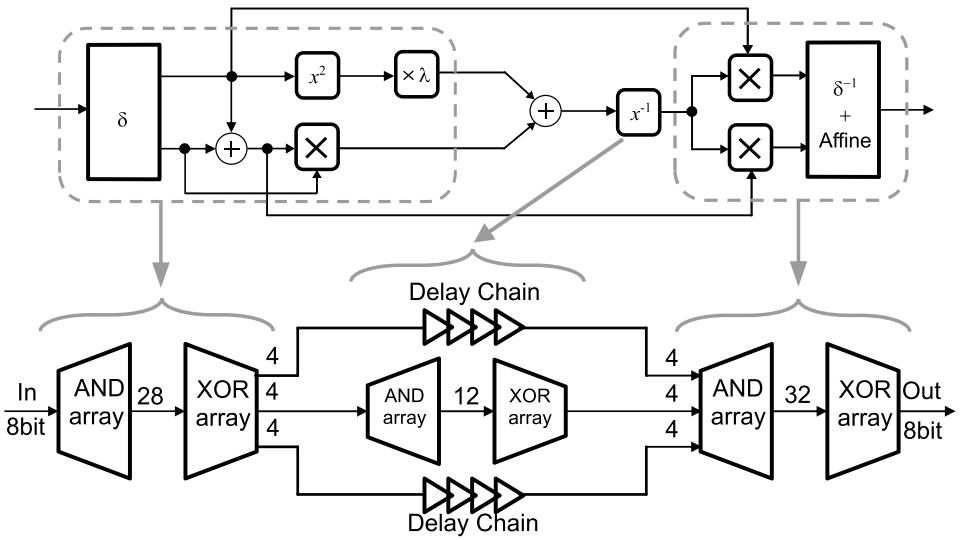

Fig. 12 Components of the composite field S-box circuit and PPRM representation. Top side: conventional composite field AES S-box architecture [9]. Bottom side: multi-stage PPRM representation with the implementation of the adiabatic 8-bit S-box circuit

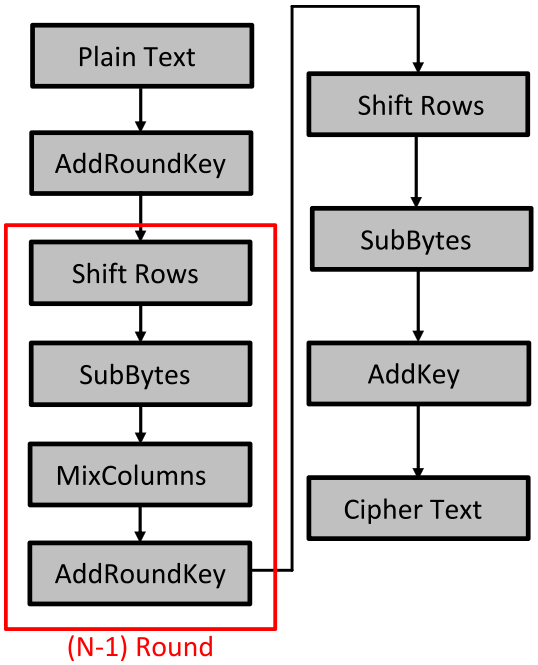

Fig. 13 AES chart

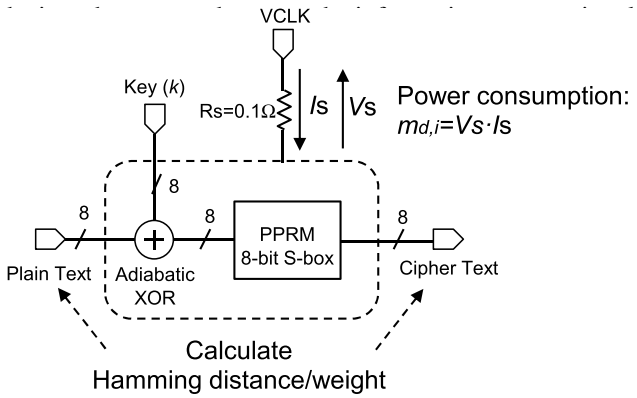

Fig. 14 DUT S-box circuit

Evaluation Index of Cryptographic Logic Circuit

The resistance of the cryptographic logic gate is evaluated using the following index [2]:

$$\sigma E\ [\mathrm{J}] = \sqrt{\frac{\sum_{i=E_1}^{E_n}(E_i - \bar{E})^2}{n}} \tag{3}$$

$$\mathrm{NED}\ [\%] = (E_{\max} - E_{\min})/E_{\max} \times 100, \tag{4}$$

$$\mathrm{NSD}_E\ [\%] = \frac{\sigma E}{\bar{E}} \times 100, \tag{5}$$

where σE is the standard deviation of energy consumption, $\bar{E}$ is the average energy consumption, NED is the normalized energy deviation, and NSD_E is the normalized standard deviation of energy. The NED shows the difference between the maximum value and the minimum value of energy consumption for all possible input transitions. NSD_E shows the variation of energy consumption based on input transition.

In this paper, we also introduce the following current indicators and evaluate resistance with regard to both energy and current. The current index is as follows:

$$\sigma I\ [A] = \sqrt{\frac{\sum_{i=I_1}^{I_n}(I_i - \bar{I})^2}{n}}, \tag{6}$$

$$\mathrm{NCD}\ [\%] = (I_{\max} - I_{\min})/I_{\max} \times 100, \tag{7}$$

$$\mathrm{NSD}_I\ [\%] = \frac{\sigma I}{\bar{I}} \times 100, \tag{8}$$

where σI is the standard deviation of the peak current, $\bar{I}$ is the average peak current, NCD is the normalized current deviation, and NSD_I is the normalized standard deviation of the peak current. NCD indicates the difference between the maximum value and the minimum value of the peak current for all possible input transitions. NSD_I represents the peak current fluctuation based on the input transition. Therefore, it can be stated that the smaller the values are, the smaller the current variation becomes.

Table 1 summarizes the comparison of simulation and calculation results of 12.5 MHz operating S-box circuit for 256 cyclical energy data samples. Comparing the conventional and proposed S-box, to add the dummy transistor in input section, the average current and energy of the proposed circuit are increased compared with the SQAL and SPGAL. On the other hand, current and energy fluctuations of the proposed can be reduced as shown $\%\mathrm{NSD}_\mathrm{I}$, $\%\mathrm{NSD}_\mathrm{E}$. Hence, the proposed CPO-SPGAL-based S-box is more secure than the existing adiabatic S-boxes.

Energy Dissipation Comparison

Figure 17 shows the comparison between the conventional and proposed energy dissipation of the S-Box. Upon adding the dummy transistor, the number of transistors of the proposed S-box increases; hence, the energy dissipation at low-frequency operation increases. On the other hand, at high-frequency operation region, the proposed Sbox has the lowest energy dissipation; hence, the proposed adiabatic logic is suitable for 100 MHz order operated IoT devices.

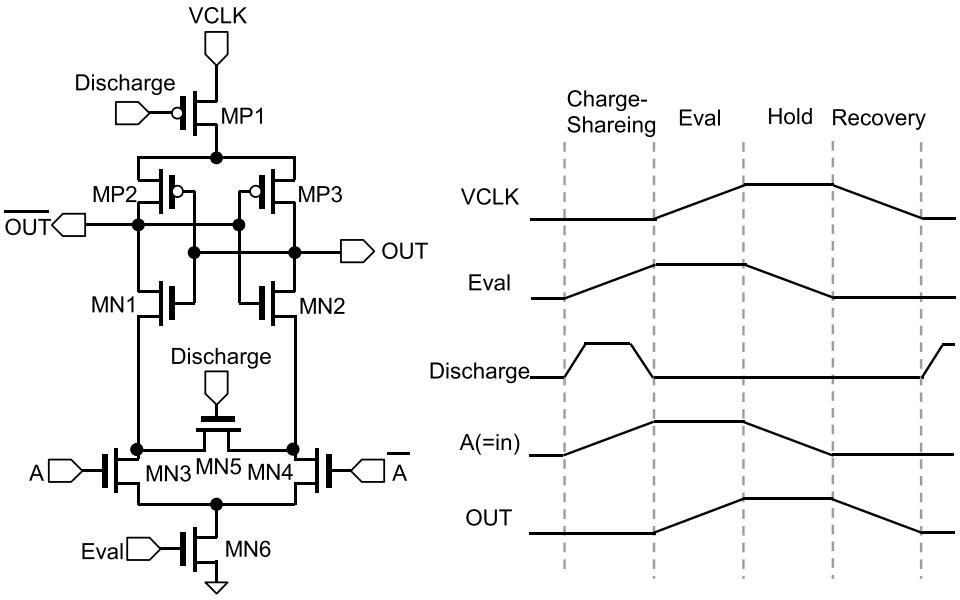

Fig. 15 CSSAL input/buffer configuration and its timing chart

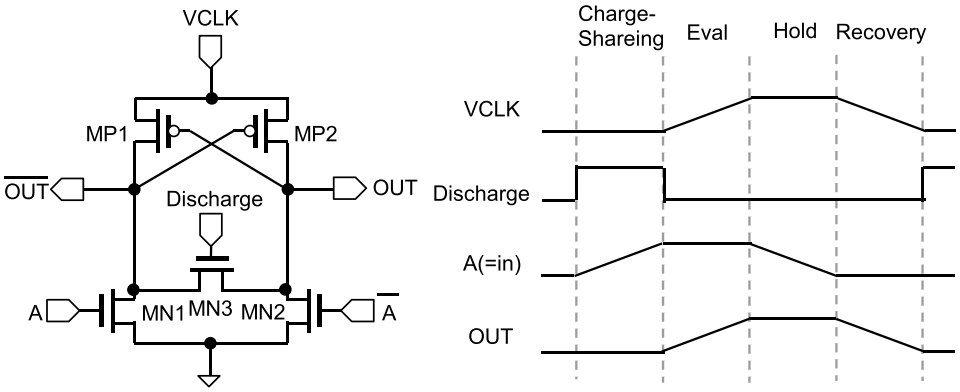

Fig. 16 SQAL input/buffer configuration and its timing chart

Correlation Power Analysis (CPA) Attack

Secret data in the devices will be revealed by power analysis attacks, such as Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis

Table 1 Comparison of simulation and calculation results of 12.5 MHz operating S-box circuit

	CSSAL [3]	SQAL [4]	SPGAL [6]	Proposed
I_{avg} [μA]	1020.60	961.90	397.72	457.59
σ_I [μA]	7.156	216.667	3.412	1.894
NCD [%]	4.902	64.970	4.659	2.556
NSD_I [%]	0.701	22.525	0.858	0.414
E_{avg} [pJ]	5.17	4.52	1.61	2.46
σ_E [pJ]	0.018	0.291	0.022	0.020
NED [%]	5.829	65.143	28.071	11.115
NSD_E [%]	1.043	19.713	6.832	2.549
#of transistor	8115	4517	5748	6940

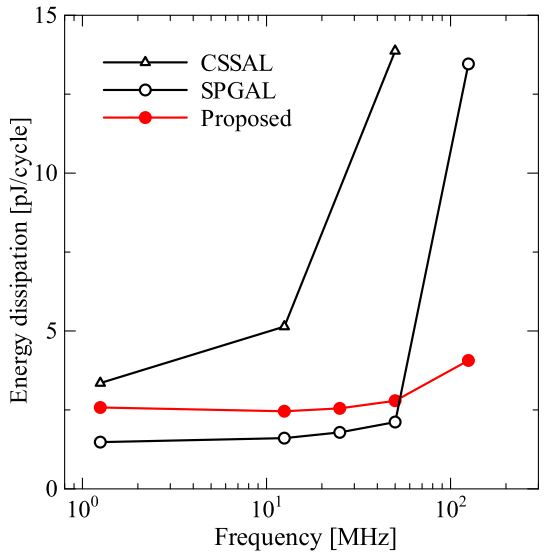

Fig. 17 Comparison of energy dissipation of S-box circuit

(CPA). Especially, CPA attack is a powerful analysis, requiring fewer number of power consumption measurements needed to recover the secret key than differential power analysis [10]. In a CPA attack, we calculate the Pearson correlation coefficient between the modeled and actual power consumption. The correlation between the Hamming distance and the power consumption is calculated by the following equation [11]:

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i})(m_{d,j} - \overline{m_j})}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i})^2 \times \sum_{d=1}^{D}(m_{d,j} - \overline{m_j})^2}}, \quad (9)$$

where D is the number of the power consumption traces, $h_{d,i}$ is the Hamming distance value with key k_i, $m_{d,j}$ is the power consumption at time j, $\overline{h_i}$ is the mean value of $h_{d,i}$, and $\overline{m_j}$ is the mean value of $m_{d,j}$.

For CPA, we set the key as $(33)_{10}$, and prepare 2048 random plain-texts, and therefore, we obtain 2048 power consumption traces in one round simulation. In this SPICE simulation for CPA, 200 round experimentals are set; hence, 409,600 (= 2048 texts × 200 round) power consumption traces are obtained. Finally, the hamming distance/weight is calculated using Visual Basic on Excel for key-guess.

Figures 18, 19, and 20 show the correlation coefficient values of the hypothetical key guesses for the successful CPA attack in the conventional S-box circuits. From the simulation results, we found that the correlation coefficient value is at the peak for key guess as $(33)_{10}$. On the other hand, Figure 21 shows the non-successful CPA attack performed on the 8-bit S-box circuit implemented using the proposed CPO-SPGAL gates. The correlation coefficient value is maximum for key guess as $(81)_{10}$. Hence, against CPA attack, the proposed CPO-SPGAL-based S-box is also

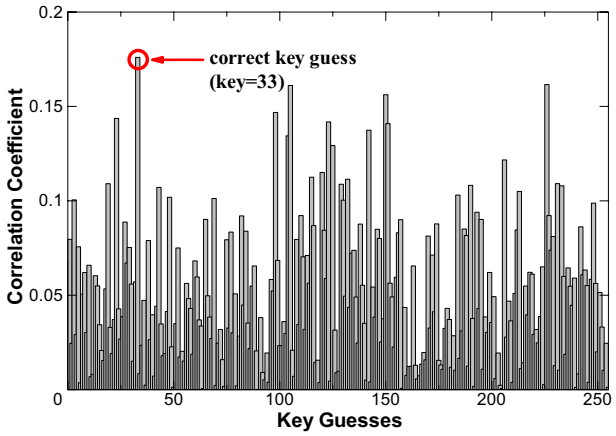

Fig. 18 CPA attack on S-box circuit implemented using the CSSAL gates with key=33

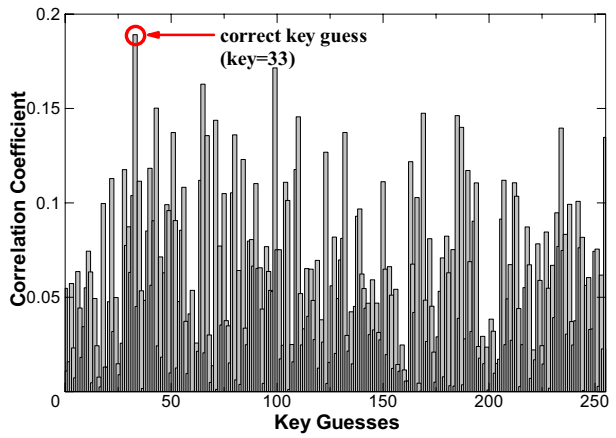

Fig. 19 CPA attack on S-box circuit implemented using the SQAL gates with key=33

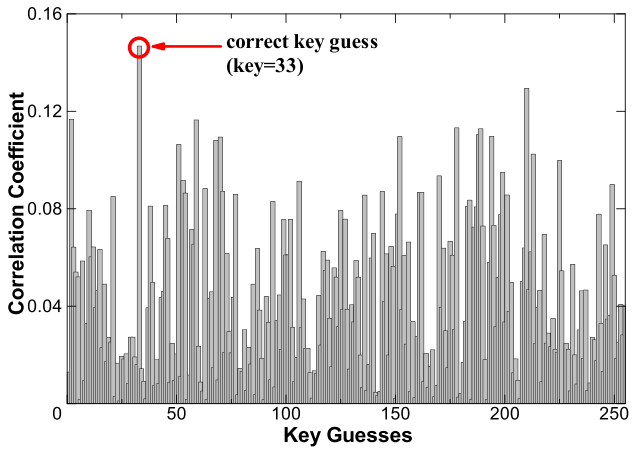

Fig. 20 CPA attack on S-box circuit implemented using the SPGAL gates with key=33

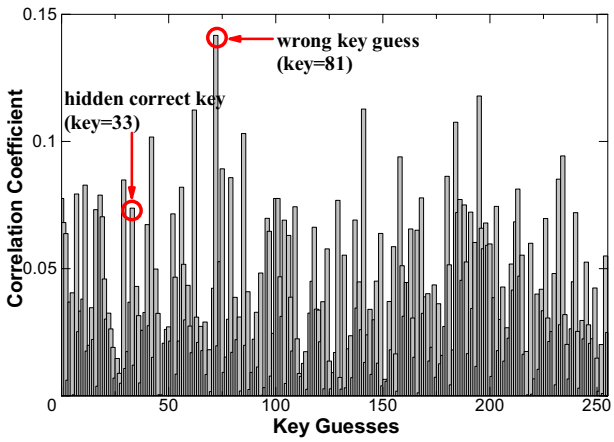

Fig. 21 CPA attack on S-box circuit implemented using the proposed CPO-SPGAL gates with key=33

more secure than the existing adiabatic S-boxes. Because, to control current pass in input section, the proposed circuit consumes uniform current irrespective of the input data being processed when compared to the conventional circuit.

Conclusion

This paper has been presented a secure S-box using our previously proposed Current-Pass Optimized Symmetric Pass Gate Adiabatic Logic (CPO-SGPAL). The security of CPO-SPGAL against CPA attacks was validated by implementing a S-box circuit and performing CPA attacks through SPICE simulations. As CPO-SPGAL is energy-efficient and secure against CPA attacks, the cryptographic circuits based on it can be employed in IoT-based portable electronic devices that can be used in fields with restricted power budget and where security is a major concern.

Compliance with ethical standards

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

References

1. Tiri K, Akmal M, Verbauwhede I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power. Proc ESSCIRC. 2002;2002:403–6.
2. Bucci M, Giancane L, Luzzi R, Trifiletti A. Three-phase dual-rail precharge logic. Proc Cryptogr Hardw Embed Syst (CHES). 2006;2006:232–41.
3. Monteiro C, Takahashi Y, Sekine T. Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level. Microelectron J. 2013;44(6):496–503.
4. Avital M, Dagan H, Levi I, Keren O, Fish A. DPA-secured quasi-adiabatic logic (SQAL) for low-power passive RFID tags employing S-boxes. IEEE Trans Circuits Syst I. 2015;62(1):149–56.
5. Monteiro C, Takahashi Y, Sekine T. Low-power secure S-box circuit using charge-sharing symmetric adiabatic logic for advanced encryption standard hardware design. IET Circuits Devices Syst. 2015;9(5):362–9.
6. Kumar SD, Thapliyal H, Mohammad A, Perumalla KS. Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware. Integr VLSI J. 2017;58:369–77.
7. Koyasu H, Takahashi Y. Current pass optimized symmetric pass gate adiabatic logic for cryptographic circuits. IPSJ Trans Syst LSI Des Methodol. 2019;12(1):50–2.
8. Athas WC, Svensson LJ, Koller JG, Tzartzains N, Chou EY-C. Low-power digital systems based on adiabatic-switching principles. IEEE Trans Very Large Scale Integr Syst. 1994;2(4):398–407.
9. Morioka S, Satoh A. An optimized s-box circuit architecture for low power AES design. Proc CHES. 2002;2002:172–86.
10. Le TH, Clediere J, Robisson B, Serviere C, Lacoume JL. A proposition for correlation power analysis enhancement. Proc CHES. 2006;2006:174–86.
11. Wu J, Shi Y, Choi M. Measurement and evaluation of power analysis attacks on asynchronous s-box. IEEE Trans Instrum Meas. 2012;61(10):2765–75.