IPSJ Transactions on System LSI Design Methodology Vol.12 50–52 (Feb. 2019)

[DOI: 10.2197/ipsjtsldm.12.50]

Short Paper

Current Pass Optimized Symmetric Pass Gate Adiabatic Logic for Cryptographic Circuits

Hiroki Koyasu[1,a)] Yasuhiro Takahashi[1,b)]

Received: May 28, 2018, Revised: August 22, 2018,
Accepted: October 22, 2018

Abstract: We propose a new adiabatic logic for cryptographic circuits, called as the Current Pass Optimized Symmetric Pass Gate Adiabatic Logic (CPO-SPGAL). The proposed circuit realizes a flat current waveform by considering the current path. The simulation results demonstrate that the proposed circuit can reduce the current fluctuation by approximately 84% and reduce the energy consumption fluctuation by approximately 79% as compared to the existing SPGAL circuits. This shows that it is more resistant to differential power analysis attacks than conventional circuits.

Keywords: adiabatic logic, dual rail logic, secure, current trace

1. Introduction

Power analysis attacks (PAA) have become a special threat for cipher designers, software developers, and hardware engineers working to secure private information stored in cryptographic devices such as smart cards, RFID tags, and wireless sensors. In cryptographic devices, there are cases requiring countermeasures at the cell/gate level design that are resilient to PAA. In the past two decades, numerous designs of PAA resistant logic, e.g., SABL [1] have been presented. In addition, adiabatic switching based on energy efficient PAA resistant logics have been proposed [2], [3], [4]. Among these, Symmetric Pass Gate Adiabatic Logic (SPGAL) [4] is a particularly more efficient PAA resistant adiabatic logic family; however, it still suffers from information leakage in the form of current consumption.

This short paper proposes a new adiabatic logic for cryptographic circuits, called as the Current Pass Optimized Symmetric Pass Gate Adiabatic Logic (CPO-SPGAL). The proposed logic is based on the SPGAL and includes on dummy transistors that offer an optimal path for current while logic switching.

2. Basic Theory of Adiabatic Switching

Adiabatic logic uses slowly rising/falling AC power supply, i.e., sinusoidal or trapezoidal clock signal, to reduce the dynamic power dissipation in LSIs. **Figure 1** shows the RC model of the conventional CMOS and adiabatic logic, 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 (shown on the left side of Fig. 1), the dissipated energy in the R is $E_{CMOS} = \frac{1}{2}CV_{dd}{}^2$. Conversely, the energy dissipation in the channel resistance R of an adiabatic logic (shown on the right side of Fig. 1) is given by $E_{Adia} = \xi\left(\frac{CV_{dd}}{\Delta T}\right)^2 R\Delta T$, where T is the time period of the clock supply and ξ is a shape factor that depends on the shape of the clock edges. The aforementioned adiabatic logic equation indicates that when the charging period ΔT is indefinitely long, the energy dissipation is, in theory, reduced to zero. This is called adiabatic switching.

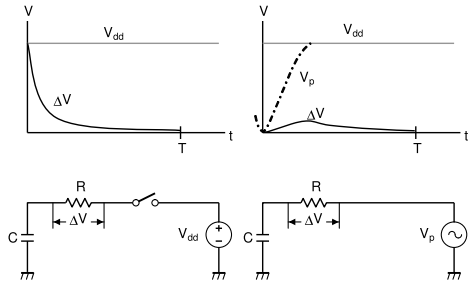

Fig. 1 *RC* tree model. Left: CMOS charging, Right: Adiabatic charging.

3. Proposed Logic

Figure 2 shows the circuit structure of the conventional adiabatic SPGAL NAND/AND. This SPGAL consists of three parts: a data-hold block that is PMOS cross-coupled pairs (M1 and M2), a function block that are all NMOS input transistors (M3–M10), and a discharge circuit (M11 and M12). **Figure 3** shows the current pass model for various input transitions. From this figure, we discover that SPGAL has a different current pass depending on the input transitions. For example, 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."

Figure 4 shows the proposed SPGAL based adiabatic logic, called as the current pass optimized SPGAL (CPO-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

[1] The authors are with the Graduate School of Natural Science and Technology, Gifu University, Gifu 501–1193, Japan
a) x4526034@edu.gifu-u.ac.jp
b) yasut@gifu-u.ac.jp

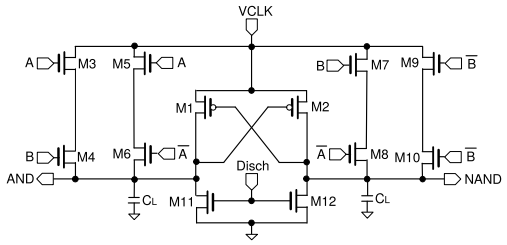

Fig. 2 SPGAL-NAND/AND.

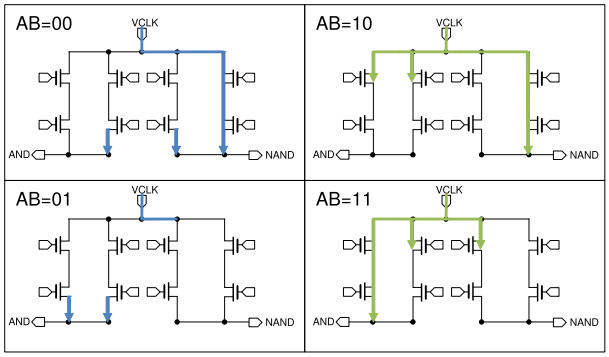

Fig. 3 Current pass of each SPGAL-NAND/AND transitions.

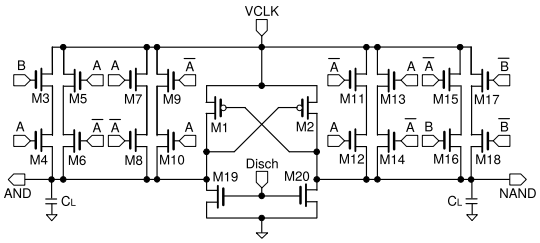

Fig. 4 Proposed logic: CPO-SPGAL-NAND/AND.

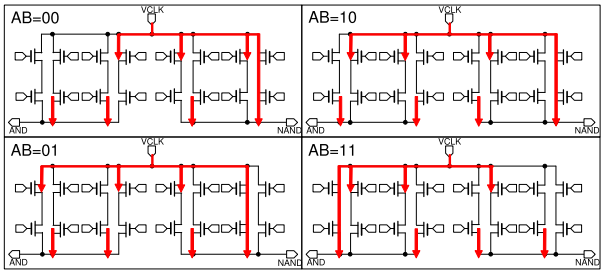

Fig. 5 Current pass of each CPO-SPGAL-NAND/AND transitions.

transistors, the proposed logic has a current pass that is independent of the input data, as shown in **Fig. 5**. **Figure 6** 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 compared to the conventional circuit.

4. Simulation Results

To evaluate the power traces of the secure adiabatic logic, the bit-parallel cellular multiplier over GF(2^4) [5] was simulated in SPICE software with Rohm 0.18-μm, 1.8-V standard CMOS process technology. The widths and lengths of all transistors were 0.6 μm and 0.18 μm, respectively. Then, we calculated the normalized energy/current deviation (NED/NCD), normalized standard deviation of energy/current (NSD$_E$/NSD$_I$), and standard deviations (σ_E, σ_I) according to the following equations: NED = $\frac{E_{max}-E_{min}}{E_{max}} \times 100\,[\%]$, NCD = $\frac{I_{max}-I_{min}}{I_{max}} \times 100\,[\%]$, NSD$_x$ = $\frac{\sigma_x}{\bar{x}} \times 100\,[\%]$, and $\sigma_x = \sqrt{\frac{\sum_{i=x_1}^{x_n}(x_i-\bar{x})^2}{n}}$ [J or A], where x becomes E when computing the fluctuations in energy, while x is I when computing current. From the aforementioned index values, we find that the smaller the difference between the maximum and minimum energy (or current) values, the smaller the value of %NED and %NSD$_E$ (or %NCD and %NSD$_I$) and hence the lower the cell's vulnerability to power analysis attacks.

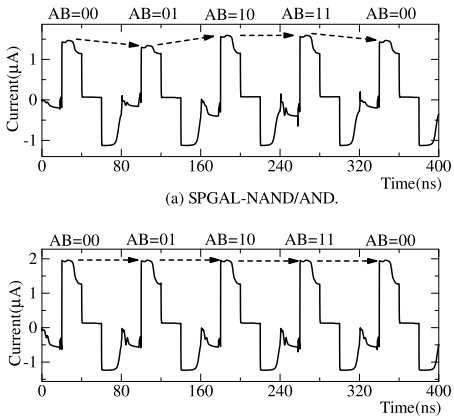

Fig. 6 Supply current waveforms for various input transitions.

Table 1 Comparison of simulation and calculation results of bit-parallel cellular multiplier for GF(2^4) at 12.5 MHz.

	CSSAL [2]	SQAL [3]	SPGAL [4]	Proposed
I_{avg} [μA]	81.0	159	170	189
NCD [%]	17.3	39.4	3.12	0.49
NSD$_I$ [%]	4.53	15.4	0.89	0.14
E_{avg} [pJ]	0.47	0.43	0.22	0.27
NED [%]	3.03	64.4	10.7	2.50
NSD$_E$ [%]	0.76	26.7	2.99	0.59
# of Transistors	1155	595	900	1100

Table 1 summarizes the comparison of simulation and calculation results at an operating frequency of 12.5 MHz. Compared with SPGAL, the proposed circuit can reduce the current fluctuation by approximately 84% and reduce the energy consumption fluctuation by approximately 79%. Moreover, the %NSD$_E$ and %NSD$_I$ of the proposed CPO-SPGAL are smaller than those of the conventional adiabatic logics. Therefore, the proposed circuit counteracts PAA attacks at the circuit level.

On the other hand, from Fig. 6 and Table 1, the proposed logic has the obvious disadvantages that it has a large number of transistor and has a large peak current compared to the conventional SPGAL. Hence we may find it a bit inconvenient if we implement a low-power cryptographic LSI chip, such as a smart card. In the near future, we will design an improved low-power CPO-SPGAL.

5. Conclusion

In this short paper, we have proposed a dual-rail type adiabatic logic for cryptographic circuits. By adding dummy transistors in the input function part, the proposed circuit consumes uniform current irrespective of the input data being processed. The simulation results of GF(2^4) multiplier demonstrates that the normalized energy and current standard deviations of the proposed CPO-

SPGAL are smaller than those of conventional adiabatic logics.

References

[1] Tiri, K., Akmal, M. and Verbauwhede, I.: A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power, *Proc. ESSCIRC 2002*, pp.403–406 (2002).

[2] Monteiro, C., Takahashi, Y. and Sekine, T.: Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level, *Microelectronics J.*, Vol.44, No.6, pp.496–503 (2013).

[3] Avital, M., Dagan, H., Levi, I., Keren, O. and Fish, A.: DPA-secured quasi-adiabatic logic (SQAL) for low-power passive RFID tags employing S-boxes, *IEEE Trans. Circuits and Syst. I.*, Vol.62, No.1, pp.149–156 (2015).

[4] Kumar, S.D., Thapliyal, H., Mohammad, A. and Perumalla, K.S.: Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware, *Integr. VLSI J.*, Vol.58, pp.369–377 (2017).

[5] Liu, C.-H., Huang, N.-F. and Lee, C.-Y.: Computation of AB^2 multiplier in GF(2^m) using an efficient low-complexity cellular architecture, *IEICE Trans. Fundamentals*, Vol.E-83A, No.12, pp.2657–2663 (2000).

Hiroki Koyasu received his B.E. degree in electronic engineering from Gifu University, Japan in 2018. He is currently working toward the M.S. degree in energy engineering at the same university. Since 2017, he has been engaged in the fields of cryptographic systems. His research interests include the areas of high-performance digital logic for cryptography integrated circuit.

Yasuhiro Takahashi was born in Yamagata, Japan, in July, 1977. He received his B.E., M.E., and Ph.D. degrees in electronic engineering from Yamagata University, Japan in 2000, 2002, and 2005, respectively. He was a research associate at the Department of Electrical and Electronic Engineering, Faculty of Engineering, Gifu University, from April 2005 to March 2007. He was an assistant professor there from April 2007 to November 2014 and is currently an associate professor. His research interests include low-power VLSI design, with a particular emphasis on digital logic, CAD techniques for implementing high-performance DSP functions, and a new approach to nonlinear circuits design using memristors. He has published 130+ papers in refereed journals and conference papers in these and related areas. He is a member of IEEE, IEEJ, and IEICE.

(Recommended by Associate Editor: *Masayuki Hiromoto*)