Symmetric Adiabatic Logic Circuits against Differential Power Analysis

Byong-Deok Choi, Kyung Eun Kim, Ki-Seok Chung, and Dong Kyue Kim

We investigate the possibility of using adiabatic logic as a countermeasure against differential power analysis (DPA) style attacks to make use of its energy efficiency. Like other dual-rail logics, adiabatic logic exhibits a current dependence on input data, which makes the system vulnerable to DPA. To resolve this issue, we propose a symmetric adiabatic logic in which the discharge paths are symmetric for data-independent parasitic capacitance, and the charges are shared between the output nodes and between the internal nodes, respectively, to prevent the circuit from depending on the previous input data.

Keywords: Side channel attack (SCA), differential power analysis (DPA), adiabatic logic, low power consumption.

I. Introduction

Differential power analysis (DPA) is a type of attack that can reveal the secret key of a cryptographic device by statistically analyzing the correlation between the processed data and power traces [1]. They are regarded as the most powerful of all side channel attacks on cryptographic devices because they can successfully extract secret keys even when measured power traces are very noisy.

There are numerous countermeasures against DPAs, such as algorithm and architecture level approaches [2], [3], but the circuit level countermeasure is very attractive because it consumes constant currents for each computation, irrespective of employed security algorithms. Therefore, researchers have proposed various logic styles that can protect against key extraction through power consumption. However, previous secure logic styles used to protect against DPAs commonly consume higher power than conventional CMOS logics in order to make the supply currents constant or independent of the data. This can be a critical issue if a cryptographic device works under power-limited circumstances as in battery-operated systems. An adiabatic logic is a very attractive solution for low power consumption [4], but few papers on adiabatic logic for DPA countermeasures have been reported to our knowledge [5]. Moreover, it is not clear that the logic circuit in [5] achieves current equalization because the transistor-level circuit is not completely shown, and certain current differences are still found in [5]. Also, the circuit requires eight-phase clocked power to cascade the logics, which complicates the construction of a cryptographic device. This letter aims to provide a new adiabatic logic style for DPA countermeasures with low power consumption.

II. Symmetric Adiabatic Logic Circuits

The efficient charge recovery logic (ECRL) [6] has a very simple structure, but its discharge circuits are asymmetric as shown in Fig. 1(a). Thus, currents from the clocked power in the evaluation phase differ, depending on the input data. For example, when the input data of both A and B is '1,' transistor MYb turns on, and the supply current only charges the capacitance at node Yb. However, when input data A is '1' and B is '0,' the supply current charges the capacitance at node N1 as well as that at node Y. This dependence of the supply current on the input data must be eliminated to make the adiabatic logic effective against DPA. For this purpose, we propose modifying the discharge circuits of the ECRL to obtain the circuits shown in Fig. 1(b). The principal idea of the circuits is

Manuscript received June 9, 2009; revised Nov. 6, 2009; accepted Nov. 19, 2009.

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2009-C1090-0902-0003).

Byong-Deok Choi (phone: +82 2 2220 2311, email: bdchoi@hanyang.ac.kr) Kyung Eun Kim (email: kekim@esslab.hanyang.ac.kr), Ki-Seok Chung (corresponding author, email: kchung@hanyang.ac.kr), and Dong Kyue Kim (email: dqkim@hanyang.ac.kr) are with the Department of Electronics and Communications Engineering, Hanyang University, Seoul, Rep. of Korea.

doi:10.4218/etrij.10.0209.0247

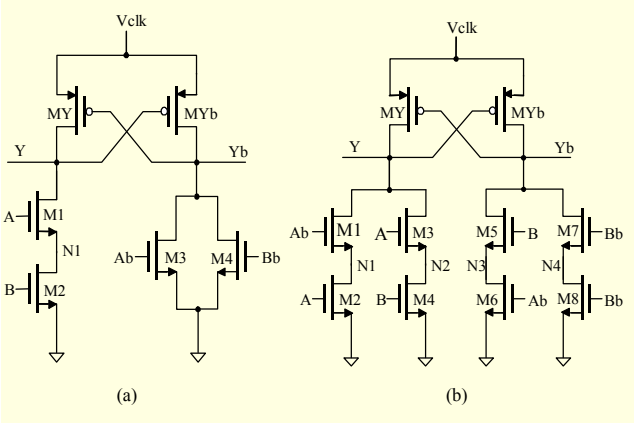

Fig. 1. Schematic diagrams of adiabatic logic circuits: (a) efficient charge recovery logic (ECRL) and (b) symmetric adiabatic logic (SyAL), ver. 1.

Table 1. States of discharge circuits in SyAL, ver. 1, with input data.

A	B	M1-M2	M3-M4	M5-M6	M7-M8
0	0	on-off	off-off	off-on	on-on
0	1	on-off	off-on	on-on	off-off
1	0	off-on	on-off	off-off	on-on
1	1	off-on	on-on	on-off	off-off

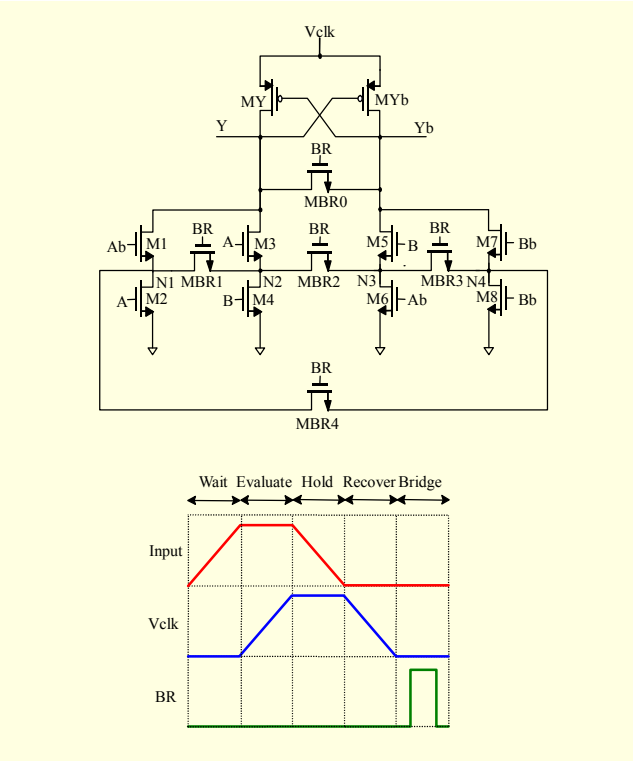

Fig. 2. Schematic diagram of SyAL, ver. 2.

that each output node has two discharge paths, and input data is assigned to the discharge paths such that on- and off-transistors are configured equally for all cases. That is, as shown in Table 1, the transistors at each discharge path are in either on-on, on-off, off-on, or off-off states, so the capacitances that supply current charges are equal for all cases of input data. We call these circuits symmetric adiabatic logic (SyAL), ver. 1.

The configuration of the discharge paths shown in Fig. 1(b) is very similar to that found in the symmetric discharge logic [7]. However, there is another important point we should emphasize in adiabatic logics. An adiabatic logic uses clocked power to recover the charge supplied to the circuits to save power. Therefore, when Vclk of the SyAL, ver. 1, shown in Fig. 1(b) ramps down for energy recovery, the charge on node Y or Yb is discharged according to Vclk. Note that node Y or Yb is not fully discharged to the ground level; rather, it is only discharged to a voltage level, corresponding to the threshold voltage of transistor MY or MYb because discharging occurs through the PMOS transistors as already described in [6]. This indicates that the supply current from Vclk in a clock period varies with the charge stored on node Y or Yb in the previous clock period, which in turn depends on the input data. Therefore, we further modify the SyAL, ver. 1, to produce the circuits shown in Fig. 2. Nodes Y and Yb are connected, and nodes N1, N2, N3, and N4 are connected by a BR signal after the recovery phase for charge sharing. As a result, the supply current is not affected by the previous input data. Transistor MBR4 is only added for the internal nodes, N1 to N4, to have the same parasitic capacitance. This circuit is named SyAL, ver. 2.

III. Simulations

HSPICE simulations were performed to validate the proposed SyALs using the model parameters of a 0.18 μm standard CMOS process. The supply currents of a conventional ECRL and the proposed SyAL, ver. 1, are compared in Fig. 3. While the ECRL requires different supply currents depending on the input data, the SyAL, ver. 1, requires the same supply current for all cases of input data. However, it should be noted that this is true only when all nodes are initially discharged. As the circuit operation repeats, output and internal nodes have charges as described in the previous section. The simulation results involving this effect are presented in Fig. 4(a). In the first clock period, the two supply currents with input data of '00' and '11' are equal because all of the nodes of the SyAL, ver. 1, are assumed to be initially discharged. In the second clock period, however, the supply current shows a difference because charges stored on the nodes are different from the previous input data. On the other hand, as shown in Fig. 4(b),

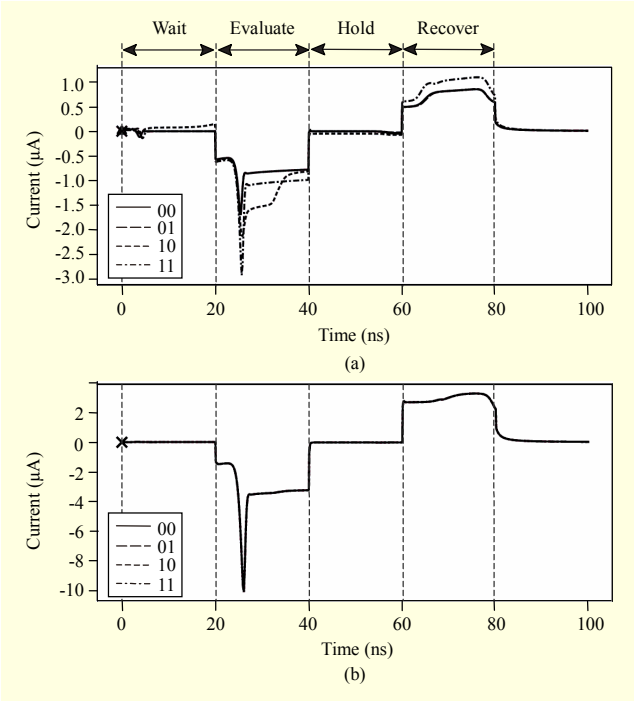

Fig. 3. Comparison of supply currents with input data for ECRL vs. SyAL, ver. 1: (a) supply current of ECRL with input data and (b) supply current of SyAL with input data.

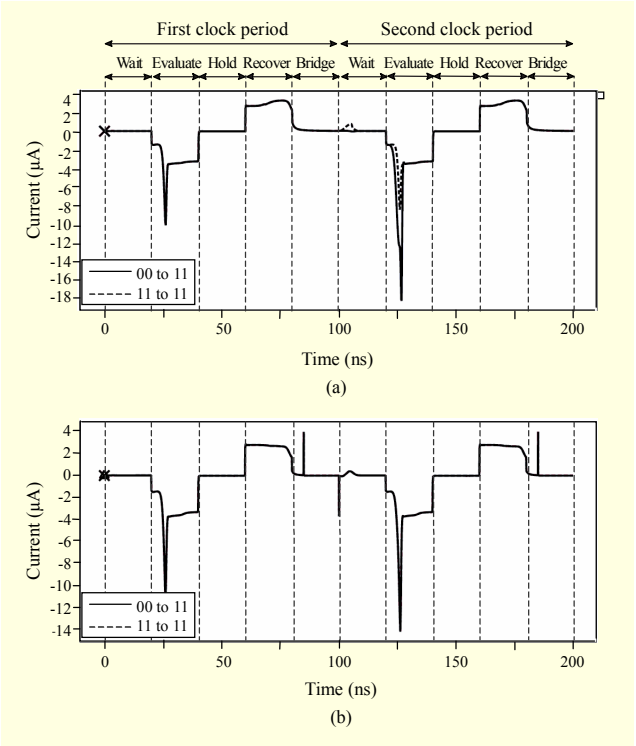

Fig. 4. Comparison of supply currents with input data for SyAL, ver. 1 vs. ver. 2: (a) supply current of SyAL, ver. 1 with input data transition from '00' and '11' to '11' and (b) supply current of SyAL, ver. 2 with input data transition from '00' and '11' to '11.'

the SyAL, ver. 2, is free from this difference in the supply current even with the input data transition due to the charge sharing between the nodes. Although not presented here, we observed that the supply currents match for all cases of data transition (00, 01, 10, and 11 to 00, 01, 10, and 11, respectively) through the simulations.

IV. Conclusion

An adiabatic logic, ECRL, is very attractive for low-power applications. However, an adiabatic logic by itself is inadequate as a countermeasure against DPA because it is dependent on the supply currents to the input data. To make the adiabatic logic independent of the input data, in addition to the symmetric discharge paths, we provide a charge-sharing feature to equalize the voltage between the output nodes and between the internal nodes, respectively, before the next clock period starts. A supply current that is independent of input data in the proposed symmetric adiabatic logic (SyAL) was verified by HSPICE simulations.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *Proc. Advances in Cryptography*, Santa Barbara, CA, USA, Aug. 1999, pp. 388-397.

[2] C. Herbst, E. Oswald, and S. Mangard, "An AES Smart Card Implementation Resistant to Power Analysis Attacks," *Proc. Appl. Cryptography and Network Security*, Singapore, June 2006, pp. 239-252.

[3] D. May, E.L. Muller, and N.P. Smart, "Random Register Renaming to Foil DPA," *Proc. Cryptographic Hardware and Embedded Systems*, Paris, France, May 2001, pp. 28-38.

[4] W.C. Athas et al., "Low-Power Digital Systems Based on Adiabatic-Switching Principles," *IEEE Trans. VLSI Systems*, vol. 2, no. 4, Dec. 1994, pp. 398-407.

[5] M. Khatir et al., "A Secure and Low-Energy Logic Style Using Charge Recovery Approach," *Proc. Int. Symp. Low Power Electron. Design*, Bangalore, India, Aug. 2008, pp. 259-264.

[6] Y. Moon and D.K. Jeong, "An Efficient Charge Recovery Logic Circuit," *IEEE J. Solid-State Circuits*, vol. 31, no. 4, 1996, pp. 514-522.

[7] J.S. Lee, J.W. Lee, and Y.H. Kim, "Symmetric Discharge Logic against Differential Power Analysis," *IEICE Trans. Fundamentals*, vol. E90-A, no. 1, Jan. 2007, pp. 234-240.