

A Comparison of Adiabatic Logic as a Countermeasures against Power Analysis Attacks

Yasuhiro Takahashi, Toshikazu Sekine
Department of Electrical and Electronic Engineering,
Gifu University,
1-1 Yanagido, Gifu-shi, 501-1193, Japan
e-mail: {yasut, sekine}@gifu-u.ac.jp

Michio Yokoyama
Department of Bio-system Engineering,
Yamagata University,
4-3-16 Jonan, Yonezawa-shi, 992-8510 Japan
e-mail: yoko@yz.yamagata-u.ac.jp

Abstract—This paper investigates the possibility of using adiabatic logic as a countermeasure against power analysis attacks. As the examples of adiabatic logic styles, we evaluate single- and dual-rail gates that are driven a single sinusoidal power clock. From simulation results, we conclude that adiabatic logic countermeasures, such as the single-rail logics, seem to be promising candidates, because they increase the resistance against power analysis attacks while at the same time lowering the power consumption of the pervasive device.

Keywords—power analysis attacks, adiabatic logic, low power

I. INTRODUCTION

Power analysis has become a threat to the security of cryptographic implementation such as smart card, and so researchers' works have resulted in several proposed countermeasures, particularly against Differential Power Analysis (DPA). These countermeasures can be roughly classified into the following two groups: Algorithmic level [1], [2] and Logic level [3], [4]. In [5] Saeki *et al.* have described that countermeasures at the logic level are the most fundamental techniques because these are related to power consumption and applicable to various cryptographic 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.

The adiabatic logics [6]–[18] are a very attractive solution for low power consumption. Few papers on adiabatic logic for DPA countermeasures have been reported to our knowledge [19]–[21], but these papers are not clear that the proposed adiabatic logic circuit achieves current equalization, and has certain current differences.

In this paper, we examine adiabatic logic circuits from the DPA-resistance point of view. As an example of adiabatic logic styles, ADL [9], ADCL [14], 2N-2N2D [8] and APDL [10] are evaluated with respect to current differences.

The rest of the paper is organized as follows. Section II summarizes the most important properties of the adiabatic logic, and also reviews the principles of adiabatic logic circuits. The security evaluation of adiabatic logics in the presence of DPA attacks is described in Section III. Finally the conclusions are given in Section IV.

II. ADIABATIC LOGIC

A. Conventional vis-a-vis Adiabatic Switching

The conventional switching can be understood by using a simple CMOS inverter. The CMOS inverter can be considered to consist of a pull-up and pull-down networks connected to a load (or internal) capacitance C . The pull-up and pull-down networks are actually MOS transistors in series with the same load C . Both transistors can be modeled by an ideal switch in series with a resistor which is equal to the corresponding channel resistance of the transistor in the saturation mode, as shown in Fig. 1(a). When a conventional CMOS inverter is set into a logical “1” state, a charge $Q = CV_{dd}$ is delivered to the load and the energy which the supply applies is $E_{applied} = QV_{dd} = CV_{dd}^2$, where V_{dd} is a DC power supply voltage. The energy stored into the load C is a half of the supplied energy:

$$E_{stored} = \frac{1}{2}CV_{dd}^2. \quad (1)$$

The same amount of energy is dissipated during the discharge process in the NMOS pull-down network because no energy can enter the ground rail $Q \times V_{gnd} = Q \times 0 = 0$. From the energy conservation law, a conventional CMOS logic emits heat and, in this way, it wastes energy in every charge-discharge cycle:

$$\begin{aligned} E_{total} &= E_{charge} + E_{discharge} \\ &= \frac{1}{2}CV_{dd}^2 + \frac{1}{2}CV_{dd}^2 \\ &= CV_{dd}^2. \end{aligned} \quad (2)$$

If the logic is driven by a certain frequency f ($= 1/T$), where T is the period of the signal, then the power of the CMOS gate is determined as:

$$P_{total} = \frac{E_{total}}{T} = CV_{dd}^2 f. \quad (3)$$

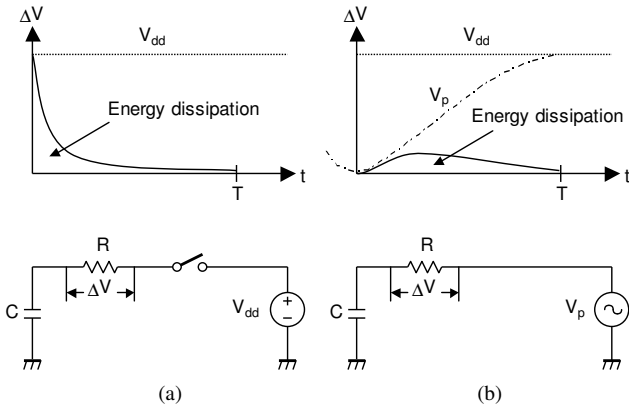


Fig. 1. RC tree model. (a) CMOS Charging. (b) Adiabatic Charging.

Adiabatic switching is commonly used to minimize energy loss during charging/discharging. The word “adiabatic” (Greek *adiabatos*, which means impassable) indicates a state change that occurs without heat loss or gain. During adiabatic switching, all the nodes are charged or discharged at a constant current in order to minimize power dissipation. This is accomplished by using AC power supplies to initially charge the circuit during specific adiabatic phases and then discharge the circuit to recover the supplied charge. The principle of adiabatic switching can be best explained by contrasting it with the conventional dissipative switching technique. The main idea in the adiabatic switching shown in Fig. 1(b) is that transitions are considered to be sufficiently slow so that heat is not emitted significantly. This is made possible by replacing the DC power supply by a resonance LC driver, an oscillator, a clock generator, etc. If a constant current source delivers the $Q = CV_{dd}$ charge during the time period ΔT , the energy dissipation in the channel resistance R is given by

$$\begin{aligned}
 E_{diss} &= \xi P \Delta T \\
 &= \xi I^2 R \Delta T \\
 &= \xi \left(\frac{CV_{dd}}{\Delta T} \right)^2 R \Delta T, \quad (4)
 \end{aligned}$$

where I is considered as the average of the current flowing to C , and ξ is a shape factor which depends on the shape of the clock edges [22]. It takes on the minimum value $\xi_{min} = 1$ if the charge of the load capacitor is DC modulated. For a sinusoidal current, $\xi = \pi^2/8 = 1.23$. The above equation indicates that when the charging period ΔT is indefinitely long, in theory, the energy dissipation is reduced to zero. This is called an adiabatic switching [16].

B. Single- and Dual-Rail Adiabatic Logics

In this subsection, we will explain diode based adiabatic logic circuits if we assume that the adiabatic logic is implemented on a cryptographic VLSI which is used as a smart card system [23]. The assumed adiabatic smart card is illustrated in Fig. 2, which comprises of a voltage limiter, an ASK demodulator, a clock recovery circuit, a base-band

digital circuit and a load modulator. The induced AC voltage at the coil directly powers the adiabatic smart card through a voltage limiter. As a result, the adiabatic smart card is more power efficient than conventional designs.

Figures 3 and 4 show the single-rail adiabatic 2-input nand (NAND2) logic circuits: ADL [9] and ADCL [14] respectively. ADL comprises two series connected controllable switches in the form of two NMOSs across a clock node V_p and an output node *out*. A precharge diode is connected across two NMOSs. The result of this logical operation appears on the output terminal. This logic causes an unavoidable energy loss due to the voltage drop across the diode when turned on. Therefore, the energy loss of ADL is $E_{ADL} = C_L V_p V_d$, where C_L is a load capacitance, V_p is a power supply voltage and V_d is the diode turn-on voltage. ADCL has the structure of static CMOS logic. The output voltage of ADCL gate is synchronized with the power supply voltage and so the operating speed of the ADCL circuits is determined by the frequency of V_p . This means that the larger the number of gate stages, the lower the operating speed of the ADCL. The energy loss is $E_{ADCL} = 2C_L (V_p - 2V_d) V_d$.

On the other hands, Figs. 5 and 6 show the dual-rail adiabatic NAND2 logic circuits: 2N-2N2D [8] and APDL [10]. 2N-2N2D consists entirely of NMOS and uses diodes for precharging the output nodes. This logic causes an unavoidable energy loss due to the voltage drop across the diode when turned on. The energy loss is given by $E_{2N2N2D} = C_L V_p V_d$. APDL is smaller input pin count compared to other adiabatic circuits that use differential signals. For APDL, an additional DC voltage supply V_{dd} is required, and therefore its energy loss is given by $E_{APDL} = C_L V_{dd} V_d$.

III. COMPARISON AND EVALUATION

To evaluate current differences of adiabatic logic circuits, the 2-input nand (NAND2) of each adiabatic logic was tested by SPICE simulation using an 0.18 μm , 1.8 V CMOS standard process technology. The transistor size W/L is 0.6 $\mu\text{m}/0.18 \mu\text{m}$ for both of the PMOS and NMOS transistors. In the simulation, the frequency of V_p was 13.56 MHz because ISO/IEC 14443 system uses ASK carrier frequency at 13.56 MHz.

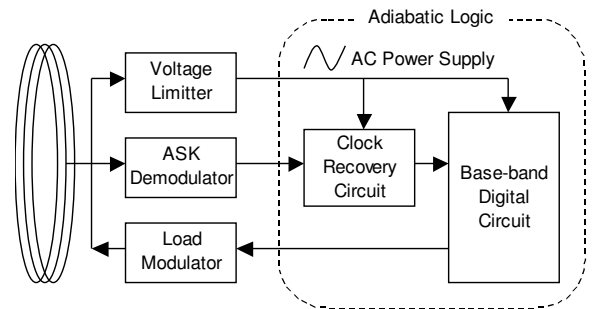


Fig. 2. Block diagram of an adiabatic smart card.

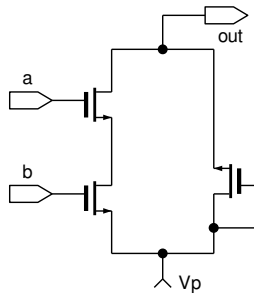


Fig. 3. ADL NAND2.

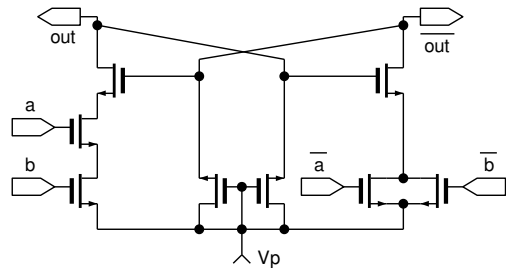


Fig. 5. 2N-2N2D NAND2.

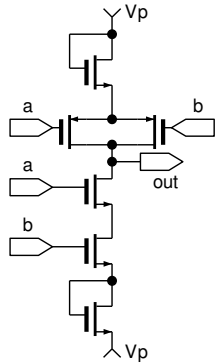


Fig. 4. ADCL NAND2.

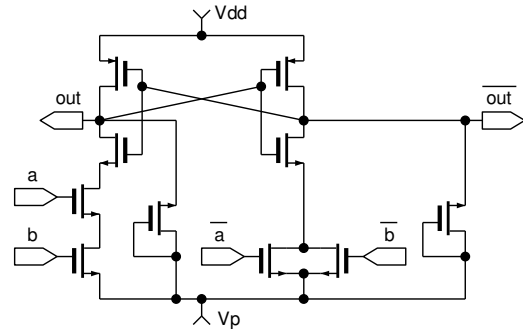


Fig. 6. APDL NAND2.

The SPICE simulation results obtained for the ADL NAND2 are shown in Fig. 7. Figure 7(a) shows the driving voltage of the sinusoidal supply clock, Figs. 7(b) and (c) demonstrate the input signals which is a CMOS compatible rectangular pulses, and Fig. 7(d) shows the output waveform. Figure 7 (e) also displays the trace showing supply current through the NAND2 logic. The point of divergence is at clock cycle four (that is $a = 0 \rightarrow 1$, $b = 0 \rightarrow 1$) and is clearly visible.

Table I summarizes the supply current peak values of each logic function and the average values of current. As can be seen from this table, the supply current difference of single-rail logic (ADL or ADCL) is smaller than that of dual-rail (2N-2N2D or APDL). In [24], Chen and Zhou have described that when comparing the total power leakage from SPICE simulation, Dual-rail Random Switching Logic's (DRSL) which is constructed from CMOS static logic has shown better performance compared with single-rail logic. However, in the adiabatic logic families, we conclude that adiabatic logic countermeasures, such as the single-rail logics, seem to be promising candidates, because they increase the resistance against power analysis attacks while at the same time lowering the power consumption of the pervasive device. To create a power model of adiabatic logic is our job in the future.

IV. CONCLUSION

In this paper we have compared how adiabatic logic styles can be used to implement cryptographic hardware that is secure against power analysis attacks. We have found that the information leakage of single-rail adiabatic logic is smaller than that of dual-rail adiabatic logic style.

REFERENCES

- [1] J. -S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," *Lecture Notes in Computer Science (LNCS)*, vol. 1717, pp. 292–302, Springer-Verlag, 1999.
- [2] M. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," *LNCS*, vol. 2162, pp. 309–318, Springer-Verlag, 2001.
- [3] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. 28th European Solid-State Circuits Conf. (ESSCIRC '02)*, Florence, Italy, Sept. 24–26, 2002, pp. 403–406.
- [4] K. Tiri and I. Verbauwhede, "Securing encryption algorithms against DPA at the logic level: Next generation smart card technology," *LNCS*, vol. 2779, pp. 125–136, Springer-Verlag, 2003.

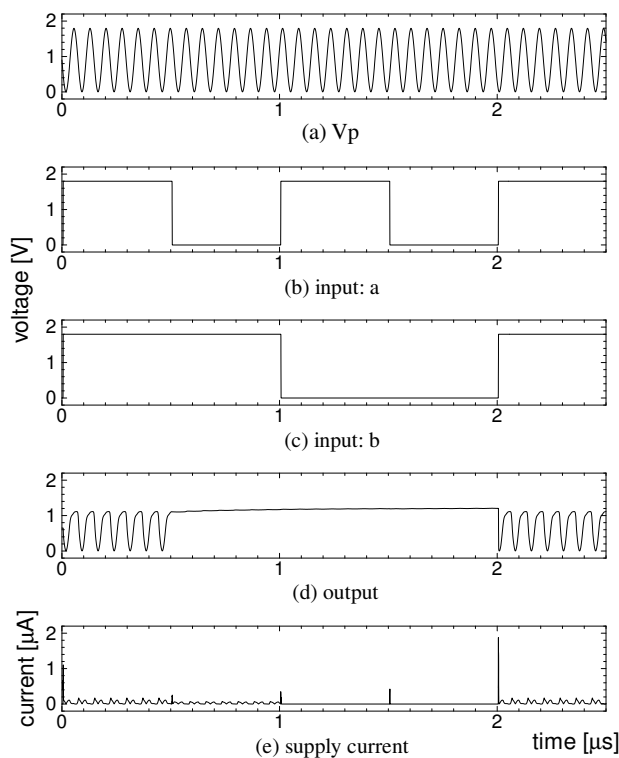


Fig. 7. Input/output waveforms and supply current trace of ADL NAND2.

TABLE I

COMPARISON OF SUPPLY CURRENT DEPENDENCE ON INPUT PATTERNS OF NAND2 GATE

input (a&b)	CMOS	ADL	ADCL	2N-2N2D	APDL
00	8.30	0.42	0.19	0.36	0.41
01	16.9	0.35	0.68	0.48	0.52
10	1.70	0.26	0.53	0.37	0.39
11	12.0	1.74	2.06	2.70	2.60
Avg.	9.73	0.70	0.87	0.98	0.98

(unit: μA)

- [5] M. Saeki, D. Suzuki, and T. Ichikawa, "Leakage analysis of DPA countermeasures at the logic level," *IEICE Trans. Fundamentals.*, vol. E90-A, no. 1, pp. 169–178, Jan. 2007.
- [6] L. J. Svensson, and J. G. Koller, "Adiabatic charging without inductors," in *Proc. IEEE Int. Workshop Low Power Design, (IWLDP '94)*, Napa Valley, CA, April 22–27, 1994, pp. 159–164.
- [7] S. G. Younis and T. G. Knight, "Asymptotically zero energy split-level charge recovery logic," in *Proc. IWLDP '94*, pp. 177–182.
- [8] J. S. Denker, S. C. Avery, A. G. Dickinson, A. Kramer, and T. R. Wik, "Adiabatic computing with 2N-2N2D logic family," in *Proc. IWLDP '94*, pp. 183–187.
- [9] A. G. Dickinson and J. S. Dencker, "Adiabatic dynamic logic," *IEEE J. Solid-States Circuits.*, vol. 30, no. 3, pp. 311–315, April 1995.
- [10] K. T. Lau and F. Liu, "Adiabatic pseudo-domino logic," *Electron. Lett.*, vol. 31, no. 23, pp. 1982–1983, Nov. 1995.
- [11] Y. Moon, D.K. Jeong, "An efficient charge recovery logic circuit," *IEEE J. Solid-States Circuits.*, vol. 31, no. 4, pp. 514–522, April 1996.
- [12] S. Kim and M. C. Papaefthymiou, "True single-phase energy-recovering logic for low-power, high-speed VLSI," in *Proc. IEEE Int. Symp. Low-Power Electronics and Design*, Monterey, CA, Aug. 10–12, 1998, pp. 167–172.
- [13] D. Maksimović, V. G. Oklobdžija, B. Nikolić, and K. W. Current, "Clocked CMOS adiabatic logic with integrated single-phase power-clock supply," *IEEE Trans. VLSI Syst.*, vol. 8, no. 4, pp. 460–463, Aug. 1998.
- [14] K. Takahashi and M. Mizunuma, "Adiabatic dynamic CMOS logic circuit," *Electronics and Communications in Japan Part II*, vol. 83, no. 5, pp. 50–58, April 2000 [*IEICE Trans. Electron.*, vol. J81-CII, no. 10, pp. 810–817, Oct. 1998].
- [15] Y. Ye and K. Roy, "QSERL: Quasi-static energy recovery logic," *IEEE J. Solid-States Circuits.*, vol. 36, no. 2, pp. 239–248, Feb. 2001.
- [16] S. Nakata, "Adiabatic charging reversible logic using a switched capacitor regenerator," *IEICE Trans. Electron.*, vol. E87-C, no. 11, pp. 1837–1846, Nov. 2004.
- [17] Y. Takahashi, T. Sekine, and M. Yokoyama, "VLSI implementation of a 4×4-bit multiplier in a two phase drive adiabatic dynamic CMOS logic," *IEICE Trans. Electron.*, vol. E90-C, no. 10, pp. 2002–2006, Oct. 2007.
- [18] Y. Takahashi, T. Sekine, and M. Yokoyama, "Two-phase clocked CMOS adiabatic logic," *Far East J. Electronics and Communications*, vol. 3, no. 1, pp. 17–34, April 2009.
- [19] M. Khatir and A. Moradi, "Secure adiabatic logic: A low-energy DPA-resistant logic style," *Cryptology ePrint Archive*, Report 2008/123, 2008. [Online] Available URL: <http://eprint.iacr.org/2008/123>
- [20] A. Moradi1, M. Khatir1, M. Salmasizadeh, and M. T. M. Shalmani, "Investigating the DPA-resistance property of charge recovery logics," *Cryptology ePrint Archive*, Report 2008/192, 2009. [Online] Available URL: <http://eprint.iacr.org/2008/192>
- [21] B. -D. Choi, K. E. Kim, K. -S. Chung, and D. K. Kim, "Symmetric adiabatic logic circuits against differential power analysis," *ETRI Journal*, vol. 32, no. 1, pp. 166–168, Feb. 2010.
- [22] M. Alioto, and G. Palumbo, "Power estimation in adiabatic circuits: A simple and accurate model," *IEEE Trans. VLSI Syst.*, vol. 9, no. 5, pp. 608–615, Oct. 2001.
- [23] K-K. Mok, *et al.*, "adiabatic smart card," in *Proc. IEEE Asia-Pacific Conf. Circuits Syst. (APCCAS 2006)*, Singapore, Dec. 4-7, 2006, pp. 287–290.
- [24] Z. Chen and Y. Zhou, "Dual-rail random switching logic: A countermeasure to reduce side channel leakage," *LNCS*, vol. 4249, pp. 242–254, Springer-Verlag, 2006.