Secure Adiabatic Logic: a Low-Energy DPA-Resistant Logic Style

Mehrdad Khatir and Amir Moradi

Department of Computer Engineering,
Sharif University of Technology, Tehran, Iran
{khatir, a_moradi}@ce.sharif.edu

Abstract. The charge recovery logic families have been designed several years ago not in order to eliminate the side-channel leakage but to reduce the power consumption. However, in this article we present a new charge recovery logic style not only to gain high energy efficiency but also to achieve the resistance against side-channel attacks (SDA) especially against differential power analysis (DPA) attacks. Simulation results show a significant improvement in DPA-resistance level as well as in power consumption reduction in comparison with DPA-resistant logic styles proposed so far.

1 Introduction

Although the power minimization has become a primary concern in VLSI design methodologies, it is not the most important factor in many cases. For example, security is the main goal when designing cryptographic hardware. In one hand, cryptographic hardware are threatened strongly by several side-channel attack (SDA) scenarios especially by differential power analysis (DPA) attacks. On the other hand, cryptographic VLSI systems are energy consuming. This makes them to be limited and inefficient for power critical applications, particularly in portable battery-operated systems. Several techniques have been devised at cell level to make cryptographic VLSI systems resistant against these attacks. For example, Sense Amplifier Based Logic (SABL) [27], Wave Dynamic Differential Logic (WDDL) [28], Random Switching Logic (RSL) [26], Dual-Rail Random Switching Logic (DRSL) [8], Masked Dual-Rail Pre-charge Logic (MDPL) [24], and Three-phase Dual-Rail Pre-charge Logic (TDPL) [6] are cell level techniques proposed to counteract DPA attacks. All these techniques sacrifice the energy consumption factor to decrease the DPA vulnerability. Therefore, devising a technique to attain both low energy consumption and DPA-resistance seems to be very appealing and necessary.

Since DPA attacks rely on the fact that dynamic power consumption values can reveal key materials of a cryptographic hardware [12], one can improve the level of DPA-resistance by significantly decreasing the dynamic power consumption. For this purpose, amongst numerous approaches for dynamic power reduction, charge recovery techniques seem to be very attractive, since the different

type of charging they use yield a huge reduction in dynamic power consumption as compared with other techniques. In order to reduce the energy consumption of logic circuits, several charge recovery styles have been devised so far [19, 13, 21, 15, 29, 10]. Although they reduce the dynamic power consumption significantly, they have not been designed for security purposes, and thus they do not eliminate the side-channel leakages. Thus, a new charge recovery logic which is customized to reduce the information leakage and hence to improve DPA-resistance is proposed. To evaluate the level of DPA-resistance provided by our proposed logic style we compare it with some of the full-custom DPA-resistant logic styles such as SABL [27] and TDPL [6]. Parameters which are taken into account are those used in some previous security evaluation articles to make a sensible comparison between our technique and the previous DPA-resistant logic styles. The spice simulation results show significant improvements both in reducing energy consumption and in DPA-resistance.

The organization of the paper is a follows. In Sect. 2, the concept of charge recovery logics is illustrated. In Sect. 3, our proposed logic style is introduced and its characteristics are clarified. Sect. 4 illustrates the comparative security evaluation of our proposed logic style and other DPA-resistant styles. Finally Sect. 5 is devoted for conclusions.

2 Charge Recovery Logic

The principle of the adiabatic charging can be best explained by contrasting it with the conventional method during the charge of a capacitance in an RC circuit. To charge a node with the associated capacitance C from 0 to V_{dd} in conventional CMOS circuits (which use a DC power supply), $Q \cdot V_{dd} = C \cdot {V_{dd}}^2$ is taken from the supply voltage. Half of it is dissipated in the path resistors, and the rest is stored in the capacitor. Thus, the energy dissipation in each transition is given by

$$E_{Conventional} = \frac{1}{2} C {V_{dd}}^2. \tag{1}$$

On the other hand, consider a capacitance node of a circuit that is charged by a time-varying voltage source whose slope of transitions is slowed down. In this charging process the overall energy dissipated at each transition is reduced to:

$$E_{Adiabatic} = \xi \frac{RC}{T} C {V_{dd}}^2, \tag{2}$$

where T denotes the charging/discharging time, V_{dd} is the voltage swing value, and ξ is the shaping factor that supports the other shapes of power clock waveform in addition to the ramp waveform. Ideally, the charging energy tends to zero by increasing T. The adiabatic charging/discharging process is carried out by observing the adiabatic switching rules. Also, the logic gates must be driven by trapezoidal power-clock voltage waveforms to achieve the best energy efficiency [30]. Briefly, the charging through DC voltage source causes enormous energy dissipation because the charge experiences a potential drop on its way

from the supply node to the load. In contrast, in charge recovery circuits each capacitance node is charged steadily, and the voltage drops across the resistive elements are made small in order to reduce the energy dissipation during the charge/discharge of the capacitive loads via a power-clock signal.

Several charge recovery styles have been proposed so far such as Efficient Charge Recovery Logic (ECRL) [19], 2N-2N2P [13], Pass-transistor Adiabatic Logic (PAL) [21], Clocked CMOS Adiabatic Logic (CAL) [15], Positive Feedback Adiabatic Logic (PFAL) [29], True Single-phase Energy recovery Logic (TSEL) [10], and Source-Coupled variant Adiabatic Logic (SCAL)'[10]. Each one has its own characteristics and efficiency, and non of them surpasses another. For example, some different efficiencies for adiabatic styles are observed in [4, 3]. Therefore, the best choice for the design depends on several parameters such as the application, fabrication technology, and frequency.

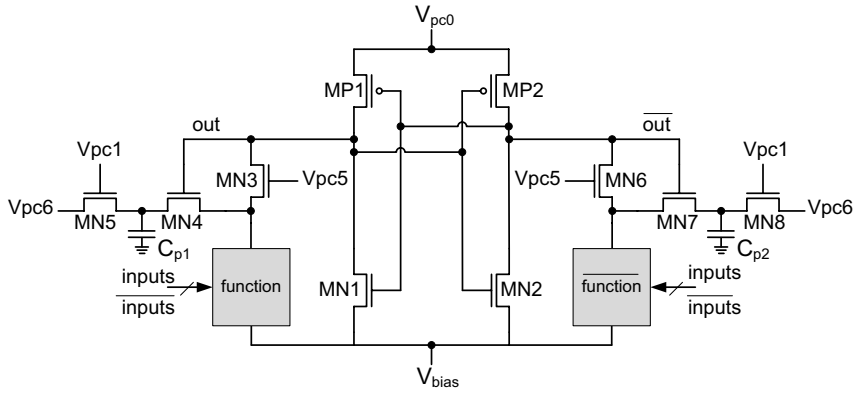
3 Secure Adiabatic Logic

Our proposed logic style aims at reducing the data-dependent energy dissipations. The basic structure of an SAL gate is shown in Fig. 1(a). It consists of three main parts:

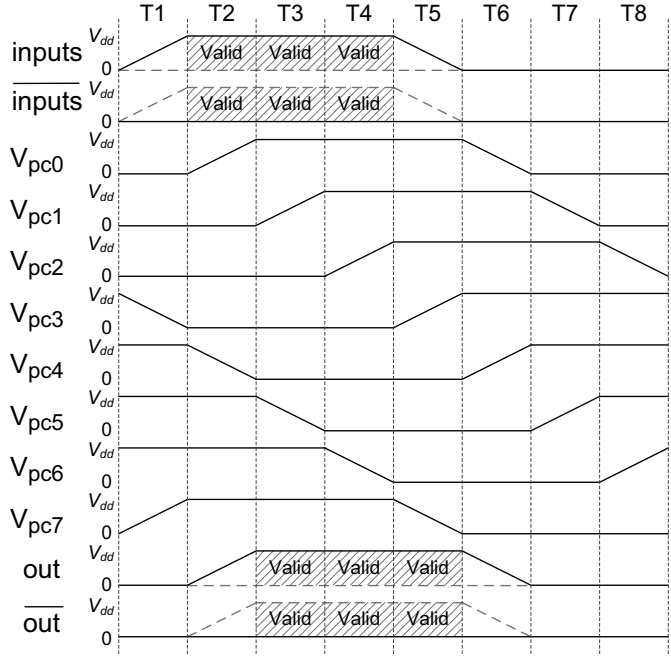
i) Two function blocks which construct the outputs. These functions are implemented by NMOS transistors.
ii) A latch which is made by two cross-coupled PMOS transistors, i.e., MP1 and MP2. Also, two cross-coupled NMOS transistors, i.e., MN1 and MN2, are inserted to cause that the outputs not to be float. This latch saves the value of out signals when the inputs fall down. Falling the inputs down before the outputs is unavoidable in all adiabatic logic styles [19, 13, 21, 15, 29, 10].
iii) Extra pass transistors, i.e., MN3 to MN8, that are responsible to discharge internal capacitances of the function blocks adiabatically. In fact, this part is added to recover the energies locked up in internal capacitances. Therefore, it leads to reduce the data-dependent dynamic power consumption. (This part will be explained more later).

According to Fig. 1(b) each SAL gate operates in eight phases:

T1- In this phase, input signals can change and will be valid at the end of the phase. Thus, one of the function blocks turns on according to the input values. Also, in this phase V_{pc5} is HI and V_{pc1} is LO. So MN3 and MN6 are on; MN5 and MN8 are off. Thus, the output of function blocks are connected to out signals.
T2- During this phase V_{pc0} goes HI steadily, and out signals are evaluated. Other signals remain unchanged within this phase. At the end of this phase out signals take their valid values and remain valid for next three phases because cross-coupled PMOS transistors keep them while V_{pc0} is HI.
T3- Simultaneously V_{pc1} and V_{pc5} go steadily HI and LO respectively. Thus, MN5 and MN8 will be on. Also, MN3 and MN6 will be off, and it will be possible to recover the energy stored in the internal capacitances of function blocks without affecting the output validity.



(a)



(b)

Fig. 1. Secure Adiabatic Logic (a) structure (b) timing diagram.

T4- In this phase the energy stored in the internal capacitances of a function block is recovered. V_{pc6} goes LO steadily, and the stored energy is recovered via two transistors: "MN4 and MN5" or "MN7 and MN8". At the end of this phase, the capacitance of all nodes except one of out signals are discharged.
T5- During this phase, all of HI input signals go LO and turn function blocks off. All other signals remain unchanged during this phase.
T6- V_{pc0} goes LO, and the energy stored in one of load capacitances is recovered through a PMOS transistor, i.e., MP1 or MP2. As mentioned previously, the charge recovery process continues till V_{tp}.
T7- V_{pc1} and V_{pc5} go steadily LO and HI respectively. Thus, output of the function blocks are disconnected from V_{pc6}, and each one is connected to the corresponding out signal.
T8- V_{pc6} goes HI, and at the end of this phase all parts of the circuit will be as same as the start of the first phase.

At the first sight, our proposed style is similar to the other adiabatic styles. However, there are two major differences between SAL and the others that make it more suitable to counteract DPA attacks:

i) The function blocks and the two cross-coupled NMOS transistors are connected to a DC bias voltage equal to V_{tp} instead of GND. Note that the bulk of NMOS transistors are already connected to GND. It avoids the non-adiabatic energy dissipation due to incomplete discharge of C_{load}.
ii) A mechanism was employed to recover the energies stored in the internal parasitic capacitances of the function blocks. It was achieved by adding some extra pass transistors, i.e., MN3 to MN8, and applying some modifications on the timing of the circuit in comparison with other charge recovery logic styles. This mechanism aim at avoiding the data-dependent dissipation.

However, there are still some non-adiabatic dissipations. The remaining dissipation is due to a non-adiabatic charge of parasitic capacitances exist between MN4 and MN5 (i.e., C_{p1}) or that of between MN7 and MN8 (i.e., C_{p2}). Consider the start of T3 phase, and suppose that out signal is HI, and $\overline{\text{out}}$ is LO. Consequently, C_{p1} has been charged, and C_{p2} has been discharged previously. At the start of this phase V_{pc1} goes HI steadily. When MN8 is turned on, C_{p2} is charged non-adiabatically. The dissipated energy is given by

$$E_{in\_p} = \frac{1}{2} C_p {V_{dd}}^2. \tag{3}$$

Obviously, E_{in_p} is much less than the dynamic energy needed to charge a capacitance load. That is, the amount of energy dissipation in our proposed logic style is much less than that of in other logic styles.

3.1 How to Cascade the SAL Gates

To establish a complex system using SAL style, eight trapezoidal power-clock which have 45 degree in advance of each other is employed. Each stage of the

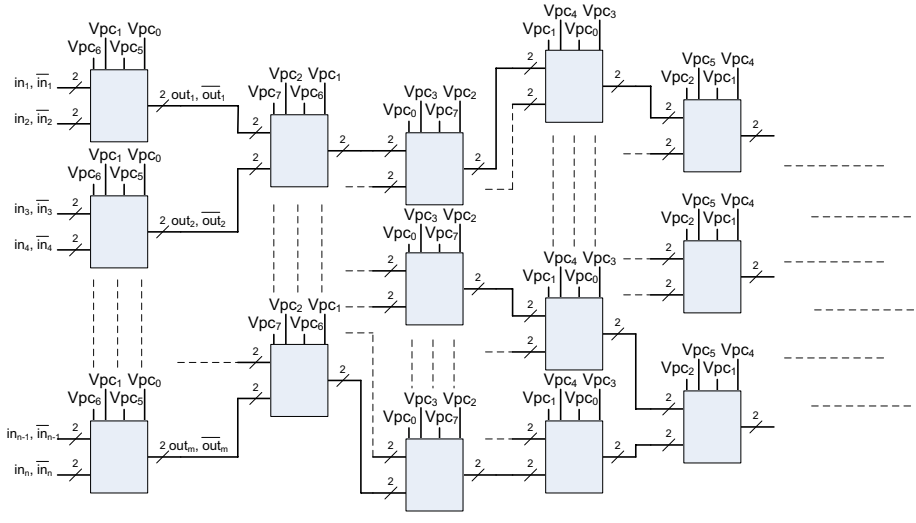


Fig. 2. The block diagram and a SAL circuit.

circuit is connected to a power-clock that has one phase latency in terms of previous stage. Note that the output of each gate is valid one phase later than its input phase. Therefore, it is possible to connect the outputs of each stage to the input of the consecutive stage. Fig. 2 shows the block diagram of a SAL circuit.

Since charge recovery styles usually use trapezoidal power clock (PC) signals, several techniques have been proposed to provide this type of PCs. These techniques can be categorized into electronic Power Clock Generators (PCG) and MEMS PCGs. Electronic PCGs can operate at high frequencies (e.g., 100MHz or higher) but have rather low energy efficiency (e.g., the energy transformed in a trapezoidal waveform is 61% of the overall energy injected to the best PCG presented in [2]). However, MEMS PCGs operate just at low frequencies but have very high energy efficiency (e.g., 98% of the injected energy is transformed to the trapezoidal power clock in the frequency of 500KHz). Since details of PCGs are beyond the scope of this work, they are not included in the article. More details can be found in [1, 2]. Note that since these PCGs can be placed inside the chip, the adversary is only able to measure the total injected energy, and it is not possible to measure the energy injected by each power clock signal.

4 Security Evaluation

Since first DPA-resistant logic styles were proposed, several evaluation criteria have been introduced to quantify their effectiveness [24, 27]. Similar to [6] we use

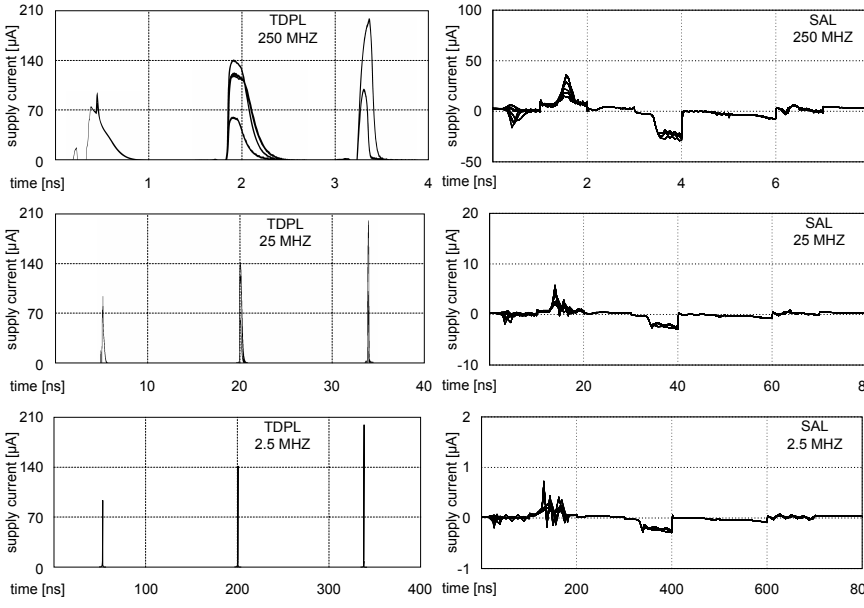


Fig. 3. AND/NAND - superimposition of supply current traces: SAL vs. TDPL (for different frequencies)

supply current traces, and energy deviation to present a sensible comparison of our proposed style with some DPA-resistant logic styles (e.g., SABL and TDPL). It should be noted that all results have been obtained using HSPICE simulation with 0.18μm technology model and 1.8v supply voltage.

Using semi-custom(and even full-custom) design tools to place and route the dual-rail circuits leads to unbalanced capacitances at the complementary wires. This phenomenon affects the security of DPA-resistant logic styles such as the leakages shown in [8] for WDDL and MDPL gates. In order to examine the resistance of our proposed logic style in a real condition, two unbalanced parasitic interconnection capacitances(which are chosen like [6]) have been supposed for each complementary wires in our simulations. First, a NAND/AND gate is taken into account. Fig. 3 shows its supply current traces for SAL and TDPL in different frequencies.

In order to evaluate the dependency of power consumption traces on the processed data, the difference of mean traces is examined. In fact, according to the classical DPA [12], power traces are divided into two groups based on the data processed, e.g., gate output value. The existence of a visible peak in the difference trace in the presence of noise indicates the information leakage of the power traces [16]. In order to compare our proposed logic style with MDPL from this point of view, Fig. 4 presents the difference of mean traces for the NAND/AND gate in SAL and MDPL. Clearly, our proposed logic style leads to

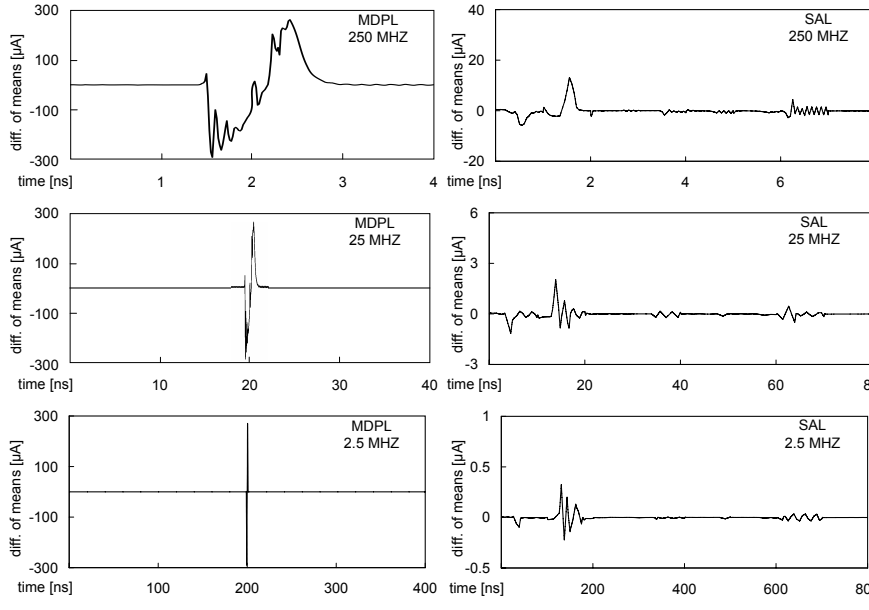


Fig. 4. AND/NAND - difference of means of supply current traces with unbalanced capacitances: SAL vs. MDPL(for different frequencies)

less information leakage. Moreover, the frequency of power clock supplies affects the information leakage too.

On the other hand, since a charge recovery circuit inherently create a pipeline, its power consumption at each cycle depends on several data which are being processed. Although a pipeline does not provide an effective countermeasure against DPA attacks, it can be viewed as a noise generator, which has the advantage of decreasing the correlation between predictions and measurements [25].

As is in [27], the energy per cycle is adopted as a figure of merit to evaluate the resistance against power analysis attacks. Thus, in order to evaluate SAL form this point of view, an SAL full-adder has been simulated. Similar to [6], the implementation was based on XOR/XNOR and NAND/AND gates, and all possible transitions which may occur in the charge recovery pipeline have been taken into account. Fig. 5 compares its energy deviation and that of SABL, and TDPL in different frequencies. As a result, not only the energy consumption of SAL but also its energy deviation is decreased in low frequencies.

5 Conclusions

In this paper, we have proposed a novel DPA-resistant logic style. It employs the concept of adiabatic charging to decrease dynamic power consumption and two extra mechanisms to reduce the data-dependent power consumptions: i) the

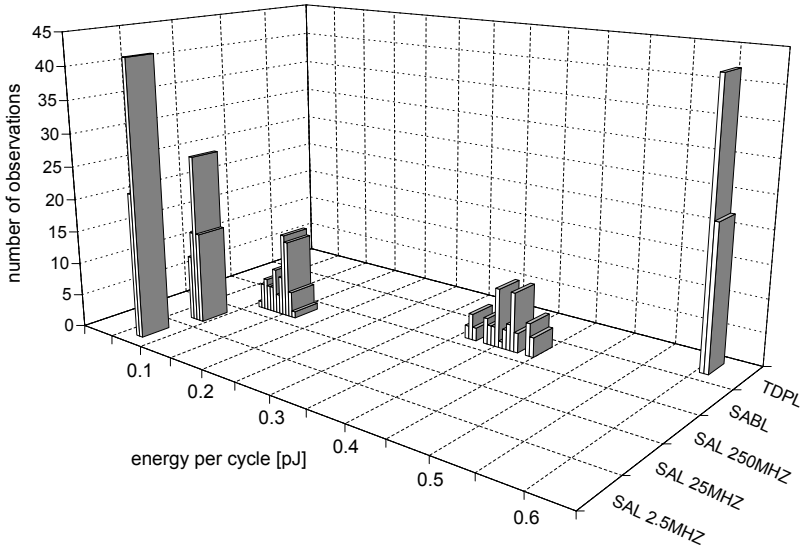


Fig. 5. FULLADDER - energy consumption per cycle: SAL vs. SABL and TDPL (for different frequencies)

usage of a DC bias voltage instead of GND in source of some NMOS transistors to avoid the non-adiabatic discharge of load capacitances and ii) the addition of some pass transistors to discharge the internal parasitic capacitances of function blocks.

The security level of our proposed logic style has been evaluated and compared with the other DPA-resistant logic styles (SALB and TDPL). The spice simulation results showed that making use of our proposed logic style leads to increase the level of DPA-resistance and to decrease the power consumption significantly. Moreover, the effect of frequency on DPA-resistance of our proposed logic was investigated. It is observed that extra DPA-resistance level is achieved by decreasing the frequency. As a result, SAL is especially suitable in low throughput applications such as passive RFID tags in which the power consumption is limited seriously.

References

1. V. Anantharam, M.P. Frank, H. Xie, M. He, and K. Nataraian, "Driving Fully Adiabatic Logic Circuits Using Custom High-Q MEMS Resonators," In *International Conference on Embedded Systems and Applications – CSREA 2004, Proceedings,* pp. 5-11, 2004.

2. M. Arsalan and M. Shams, "Charge-Recovery Power Clock Generators for Adiabatic Logic Circuits," In *International Conference on VLSI Design, Proceedings,* pp. 171-174, 2005.
3. V.S.K. Bhaaskaran, S. Salivahanan, and D.S. Emmanuel, "Semi-Custom Design of Adiabatic Adder Circuits," In *International Conference on VLSI Design held jointly with International Conference on Embedded Systems Design, Proceedings,* pp. 745-748, 2006.
4. A. Blotti and R. Saletti, "Ultralow-Power Adiabatic Circuit Semi-Custom Design," *IEEE Transactions on VLSI Systems,* vol. 12, no. 11, pp. 1248-1253, 2004.
5. E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," In *Cryptographic Hardware and Embedded Systems – CHES 2004*, vol. 3156 of LNCS, Springer, pp. 16-29, 2004.
6. M. Bucci, L. Giancane, R.O Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Precharge Logic," In *Cryptographic Hardware and Embedded Systems – CHES 2006,* vol. 4249 of LNCS, Springer, pp. 232-241, 2006.
7. D. Canright, "A Very Compact S-Box for AES," In *Cryptographic Hardware and Embedded Systems – CHES 2005*, vol. 3659 of LNCS, Springer, pp. 441-455, 2005.
8. Z. Chen and Y. Zhou, "Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage," In *Cryptographic Hardware and Embedded Systems – CHES 2006,* vol. 4249 of LNCS, Springer, pp. 242-254, 2006.
9. S. Kim and S.I. Chaie, "A Bootstrapped Switch for nMOS Reversible Energy Recovery Logic for Low-Voltage Applications," *IEICE Transactions on Electronics,* vol. E89-C, no. 5, pp. 649-652, 2006.
10. S. Kim and M.C. Papaefthymiou, "True Single-Phase Adiabatic Circuitry," *IEEE Transactions on VLSI Systems,* vol. 9, no. 1, pp. 52-63, 2001.
11. P.C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," In *Advances in Cryptology – CRYPTO 96*, vol. 1109 of LNCS, Springer, pp. 104-113, 1996.
12. P.C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," In *Advances in Cryptology – CRYPTO 99*, vol. 1666 of LNCS, Springer, pp. 388-397, 1999.
13. A. Kramer, J.S. Denker, B. Flower, and J. Moroney, "2nd Order Adiabatic Computation with 2N2P and 2N-2N2P Logic Circuits", In *International Symposium on Low Power Design, Proceedings,* pp. 191-196, 1995.
14. R. Landauer, "Irreversibility and Heat Generation in the Computational Process," *IBM Journal of Research and Development*, vol. 5, pp. 183-191, 1961.
15. D. Maksimovic, V.G. Oklobdzija, B. Nikolic, and K.W. Current, "Clocked CMOS Adiabatic Logic with Integrated Single-Phase Power-Clock Supply," *IEEE Transactions on VLSI Systems,* vol. 8, no. 4, pp. 460-463, 2000.
16. S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks, *Revealing the Secrets of Smart Cards*," Springer, 2007. ISBN 0-387-30857-1.
17. S. Mangard, T. Popp, and B.M. Gammel, "Side-Channel Leakage of Masked CMOS Gates," In *Topics in Cryptology – CTRSA 2005, The Cryptographers Track at the RSA Conference*, vol. 3376 of LNCS, Springer, pp. 351-365, 2005.
18. T.S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software," In *Cryptographic Hardware and Embedded Systems – CHES 2000,* vol. 1965 of LNCS, Springer, pp. 238251, 2000.
19. Y. Moon and D.-K. Jeong, "An Efficient Charge Recovery Logic Circuit," *IEEE Journal of Solid State Circuits,* vol. 31, pp. 514-522, 1996.
20. A. Moradi, M. Salmasizadeh, and M.T. Manzuri Shalmani, "Power Analysis Attacks on MDPL and DRSL Implementations," In *International Conference of Security and Cryptology – ICISC 2007,* vol. 4817 of LNCS, Springer, pp. 259272, 2007.

21. V.G. Oklobdzija and D. Maksimovic, "Pass-Transistor Adiabatic Logic Using Single Power-Clock Supply," *IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing,* vol. 44, no. 10, pp. 842846, 1997.
22. E. Peeters, F.-X. Standaert, Nicolas Donckers, and Jean-Jacques Quisquater, "Improved Higher-Order Side-Channel Attacks with FPGA experiments," In *Cryptographic Hardware and Embedded Systems – CHES 2005,* vol. 3659 of LNCS, Springer, pp. 309-323, 2005.
23. T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the Masked Logic Style MDPL on a Prototype Chip," In *Cryptographic Hardware and Embedded Systems – CHES 2007*, vol. 4727 of LNCS, Springer, pp. 81-94, 2007.
24. T. Popp and S. Mangard, "Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints," In *Cryptographic Hardware and Embedded Systems – CHES 2005*, vol. 3659 of LNCS, Springer, pp. 172-186, 2005.
25. F.-X. Standaert, S.B. Örs, and B. Preneel, "Power Analysis of an FPGA," In *Cryptographic Hardware and Embedded Systems – CHES 2004*, vol. 3156 of LNCS, Springer, pp. 3044, 2004.
26. D. Suzuki, M. Saeki, and T. Ichikawa, "Random Switching Logic: A Countermeasure against DPA based on Transition Probability," Cryptology ePrint Archive (http://eprint.iacr.org/), Report 2004/346, 2004.
27. 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 *European Solid State Circuits Conference, Proceedings*, pp. 403-406, 2002.
28. K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," In *Design, Automation and Test in Europe Conference and Exposition – DATE 2004, Proceedings*, pp. 246-251, 2004.
29. A. Vetuli, S.D. Pascoli, and L.M. Reyneri, "Positive feedback in adiabatic logic," *Electronics Letters,* vol. 32, pp. 1867-1869, 1996.
30. B. Wang and P. Mazumder, "On Optimality of Adiabatic Switching in MOS Energy-Recovery Circuit," In *International Symposium on Low Power Electronics and Design – ISLPED 2004, Proceedings*, pp. 236-239, 2004.