Investigating the DPA-Resistance Property of Charge Recovery Logics

Amir Moradi[1], Mehrdad Khatir[1], Mahmoud Salmasizadeh[2], and Mohammad T. Manzuri Shalmani[1]

[1] Department of Computer Engineering, Sharif University of Technology, Azadi St., Tehran, Iran
[2] Electronic Research Center, Sharif University of Technology, Azadi St., Tehran, Iran
{a_moradi,khatir}@ce.sharif.edu, {salmasi,manzuri}@sharif.edu

Abstract. The threat of DPA attacks is of crucial importance when designing cryptographic hardware. As a result, several DPA countermeasures at the cell level have been proposed in the last years, but none of them offers perfect protection against DPA attacks. Moreover, all of these DPA-resistant logic styles increase the power consumption and the area consumption significantly. On the other hand, there are some logic styles which provide less power dissipation (so called charge recovery logic) that can be considered as a DPA countermeasure. In this article we examine them from the DPA-resistance point of view. As an example of charge recovery logic styles, 2N-2N2P is evaluated. It is shown that the usage of this logic style leads to an improvement of the DPA-resistance and at the same time reduces the energy consumption which make it especially suitable for pervasive devices. In fact, it is the first time that a proposed DPA-resistant logic style consumes less power than the corresponding standard CMOS circuit.

1 Introduction

Cryptographic algorithms are usually strong against the known theoretical cryptanalysis attacks. However, the vulnerability of their practical implementations to side-channel attacks [9, 11] posed a great threat to the security. The most powerful and effective branch of side-channel attacks exploit the power consumption profile of the different data processed to detect the correlation between key materials of the attacked device and the dynamic switching power. This technique is referred to as Differential Power Analysis (DPA) [11].

Several methods in different ways have been proposed to counteract DPA attacks. DPA-resistant logic styles are the countermeasures proposed at the cell level. For instance, Sense Amplifier Based Logic (SABL) [26] and Wave Dynamic Differential Logic (WDDL) [27] are dual-rail pre-charge logic styles whose logic gates are driven by a pre-charge signal to prevent glitches, and each logic signal is represented by two complementary wires. The SABL needs a full-custom design tool to equalize the capacitances of the complementary wires. Data-dependent

time of evaluation of the WDDL and its memory effect made it vulnerable to DPA attacks [17]. Masked Dual-rail Pre-charge Logic (MDPL) [22] and Dual-rail Random Switching Logic (DRSL) [7] were introduced by combining the masking scheme and dual-rail pre-charge logic in order to use semi-custom design tools without routing constrains. Additionally, these logic styles need a random number/sequence generator to prepare the mask bits. In addition to the leakages found in MDPL [8, 23, 24], a practical evaluation done on a prototype chip [21] showed that early propagation of MDPL gates leads to a significant information leakage. Also, Three-phase Dual-rail Pre-charge Logic (TDPL) [4] has been proposed in such a way that each TDPL gate contains three control signals, and hardware implemented using TDPL style needs a separate unit to schedule control signals in order to prevent the glitches.

Although each DPA-resistant logic style has its own advantages and disadvantages, all of them have in common that they increase the power consumption in comparison to the corresponding CMOS circuit. The fact that all of these logic styles use the conventional charging method (and the major problem in DPA attacks is caused by the charging current of the capacitive loads) motivated us to utilize a different charging method called adiabatic charging [14, 2] to counteract DPA attacks. To the best of our knowledge it is the first attempt to utilize the charge recovery logic styles for DPA-resistance. The charge recovery logic styles, such as [10, 20, 16, 12] have been proposed to save the energy dissipation of logic circuits. They are designed to steadily inject the energy (charge) to the capacitances (capacitive loads). Therefore, the dynamic power consumption is reduced enormously. Thus, the signal-to-noise ratio (SNR) of the power consumption traces will be decreased significantly in comparison to corresponding circuits in other logic styles. Moreover, the pipelined structure of the charge recovery logic circuits causes the power consumption of each cycle to depend on the number and the values of the data which are currently in the pipeline. Consequently, it becomes more difficult for an adversary to discover the correlation between some specific processed data and the power consumption values. In this article, a simple charge recovery logic family 2N-2N2P [10] is taken into account to evaluate the resistance of charge recovery logic families against DPA attacks.

The rest of the paper is organized as follows. It starts with a summary of the most important properties of the charge recovery logics in Sect. 1. Also, Sect. 2 reviews the principles of 2N-2N2P logic and deals with its difficulties. The security evaluation of 2N-2N2P circuits in the presence of DPA attacks is presented in Sect. 3. Finally the conclusions are given in Sect. 4.

2 Charge Recovery Logic

The charging through DC voltage source causes enormous energy dissipation because the charge (the charging current) 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 or discharge of the capacitive loads via a power clock signal.

The principle of the adiabatic charging scheme 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, $Q \cdot V_{dd} = C \cdot {V_{dd}}^2$ is taken from the supply voltage source. Half of it is dissipated in the path resistors, and the rest is stored in the capacitor C. Thus, the energy dissipation in each transition is given by

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

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 for each transition is reduced to

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

where T denotes the charging/discharging time, V_{dd} is the voltage swing value, and ξ is the shaping factor that supports the other types of voltage source waveform in addition to the ramp waveform. Ideally, the charging energy tends to zero ($E_{\text{Adiabatic}} \rightarrow 0$) by increasing T ($T \rightarrow \infty$). 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 [28].

Several charge recovery styles have been proposed so far such as Efficient Charge Recovery Logic (ECRL) [15], 2N-2N2P [10], Pass-transistor Adiabatic Logic (PAL) [20], Clocked CMOS Adiabatic Logic (CAL) [16], True Single-phase Energy recovery Logic (TSEL) [12], and Source-Coupled variant Adiabatic Logic (SCAL) [12]. Each one has its own characteristic and efficiency. For example, different efficiencies for some of them are observed in [6] and [13] that shows the best choice for the design depends on several parameters such as the application, the fabrication technology, and the frequency. However, their fundamental structure does not differ much from each other. Due to the simplicity of the 2N-2N2P, it is taken into account to examine the DPA-resistance of charge recovery logics.

2.1 2N-2N2P

A 2N-2N2P gate consists of two main parts:

(*i*) two functional blocks whose duty is to construct the gate outputs out and $\overline{\text{out}}$ as shown in Fig. 1(a)
(*ii*) a latch which is made by two cross-coupled PMOS transistors.

Also, two cross-coupled NMOS transistors are inserted to prevent from the flotation of the output signals. In fact, it avoids the degradation of the voltage level at the output nodes. All 2N-2N2P gates operate at four different phases:

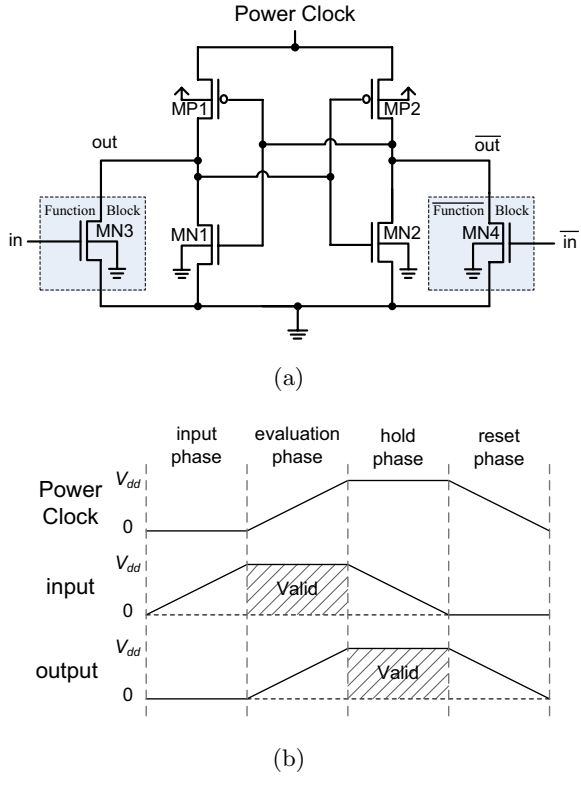

Fig. 1. (a) Structure of a 2N-2N2P buffer/inverter gate (b) Timing diagram in 2N-2N2P logic style

input phase, evaluation phase, hold phase, and reset phase. In order to clarify the specification of each phase, the operation of a 2N-2N2P buffer/inverter gate is explained for simplicity.

The basic structure of a 2N-2N2P buffer/inverter gate is shown in Fig. 1(a). During the input phase the power clock is LO, and inputs can change. At the end of this phase inputs have taken their own valid values. Suppose that in=HI and $\overline{\text{in}}$=LO; therefore, MN3 is closed, and MN4 is open. In other words, the function block which prepares out signal is closed, and the complementary function block which prepares $\overline{\text{out}}$ signal is open.

At the start of the evaluation phase both of out and $\overline{\text{out}}$ are LO. As shown in Fig. 1(b), power clock steadily increases towards HI; thus, $\overline{\text{out}}$ is charged through MP2. In contrast, out node remains LO since it is connected to GND through the function block. Finally, MN1 is closed and outputs are latched by the cross-coupled transistors. Note that during this phase inputs must remain unchanged.

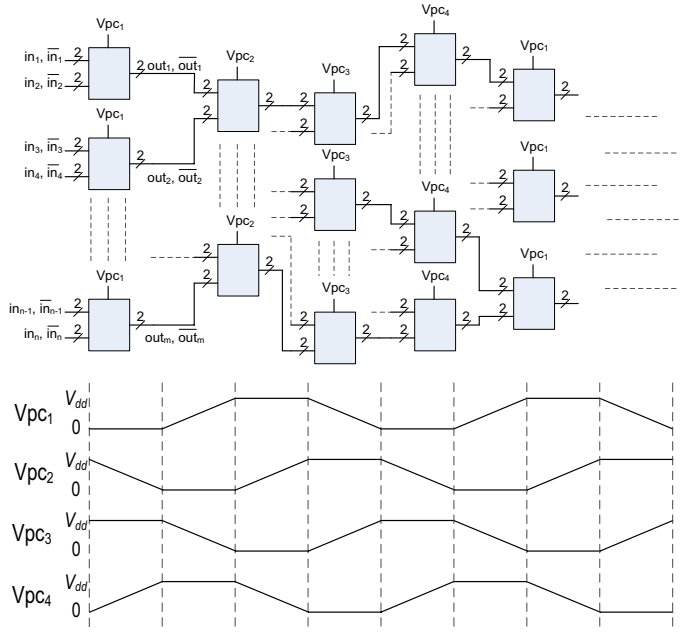

Fig. 2. A block diagram and a timing diagram of a 2N-2N2P circuit.

In hold phase, inputs switch to LO, and both of the function blocks are switched off. In this situation output values are held by the cross-coupled transistors. Note that during this phase output values are valid and can be used as input at the next stage.

Finally, during the reset phase power clock steadily decreases towards LO. By falling power clock, $\overline{\text{out}}$ goes LO via MP2 until it reaches V_{tp0}. Then, MP2 becomes open and $\overline{\text{out}}$ remains unchanged. The remaining charge of $\overline{\text{out}}$ is dissipated non-adiabatically at the next cycle if new inputs cause the complementary function block to switch on.

A complex 2N-2N2P gate can be easily implemented using an NMOS function block instead of MN3 and its complementary function block instead of MN4. See [10] for more detailed information about 2N-2N2P logic family.

To establish a complex system using 2N-2N2P style, four trapezoidal power clock signals which have 90 degree in advance of each other are employed. Each stage of the circuit is connected to a power clock that has one phase latency in terms of the 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 a block diagram and a timing diagram of a 2N-2N2P circuit.

Note that the performance of an n-stage cascaded adiabatic circuit is similar to a pipeline with n stages. It operates at the frequency of the power clocks.

The phase latency to prepare the outputs is equal to the number of the circuit stages.

Since charge recovery styles usually use trapezoidal power clock (PC) signals, several techniques have been devised to provide this type of PCs. These techniques can be categorized into electronic power clock generators (PCG) and Micro-Electro-Mechanical System (MEMS) PCGs. Electronic PCGs can operate at high frequencies (e.g., 100MHz or higher) but have rather low energy efficiency. For instance, energy transformed in a trapezoidal waveform is 61% of overall energy injected to the best presented PCG in [1]. In contrast, MEMS PCGs operate at low frequency but have very high energy efficiency (e.g., 98% of the injected energy is transformed to the trapezoidal power clock in a frequency of 500KHz). Since details of PCGs are beyond the scope of this article, we refer the interested reader to [1, 3]. Note that since these PCGs can be placed into the chip, the adversary is only able to measure the total injected energy and is unable to measure the energy injected by each power clock signal.

3 Comparison and Evaluation

3.1 Area Consumption

Since the 2N-2N2P is a full-custom logic style, it is not possible to compute the gate equivalence for its logic cells. Thus, similar to [18] the transistor cost[3] is considered to compare the 2N-2N2P to other full-custom logics SABL and TDPL. As shown in Table 1, the transistor cost of all 2N-2N2P logic cells is less than the corresponding SABL and TDPL cells. Note that the area needed to implement the PCG is not included in the results.

Table 1. Transistor cost of 2N-2N2P vs. SABL and TDPL

cell	SABL		TDPL		2N-2N2P		ratio $\frac{\text{2N-2N2P}}{\text{SABL}}$	ratio $\frac{\text{2N-2N2P}}{\text{TDPL}}$
	N	P	N	P	N	P		
Inverter/Buffer	8	6	9	7	4	2	0.43	0.37
AND/NAND (2-in) OR/NOR (2-in)	12	6	11	7	6	2	0.44	0.44
XOR/XNOR (2-in)	12	6	13	7	10	2	0.67	0.60

3.2 Power Consumption

From a power consumption point of view there is a large difference between charge recovery logics and other logic styles. This is the effect of the frequency. In fact, the peak of power consumption traces in DPA-resistant logic styles does

[3] Number of transistors without attention to their difference in type(N or P) and in W/L ratio

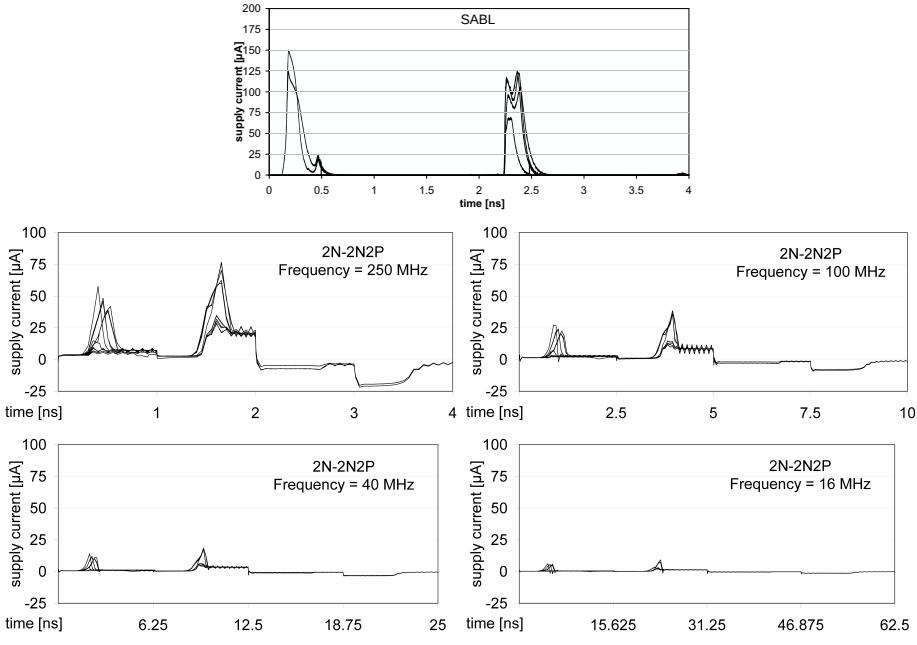

Fig. 3. AND/NAND - superimposition of the supply current traces: SABL vs. 2N-2N2P (for different frequencies)

not depend on the frequency but in charge recovery logic families it does. A comparison between the superimposition of supply current traces of an AND/NAND gate in SABL and 2N-2N2P styles is shown in Fig. 3. Obviously, the peak of the power traces decreases for low power clock frequencies. It should be noted that all results have been obtained using HSPICE simulation in 0.18μm technology and 1.8V supply voltage.

Moreover, in order to examine the energy variation, a 2N-2N2P full adder has been simulated and compared to the corresponding SABL and TDPL circuits. A histogram of the observed energies per cycle presented in Fig. 4 shows that not only the energy consumption of 2N-2N2P circuits is less than other logic styles, but also their energy deviation decreases for low frequencies.

3.3 Security

The pipelining structure of 2N-2N2P (and other charge recovery logic families) causes the circuit to process multiple data simultaneously. Therefore, the power consumption at each cycle depends on several data which are being processed. Obviously, a pipeline does not provide an effective countermeasure against DPA attacks, and it can be viewed as a noise generator that has the advantage of decreasing the correlation between predictions and measurements [25].

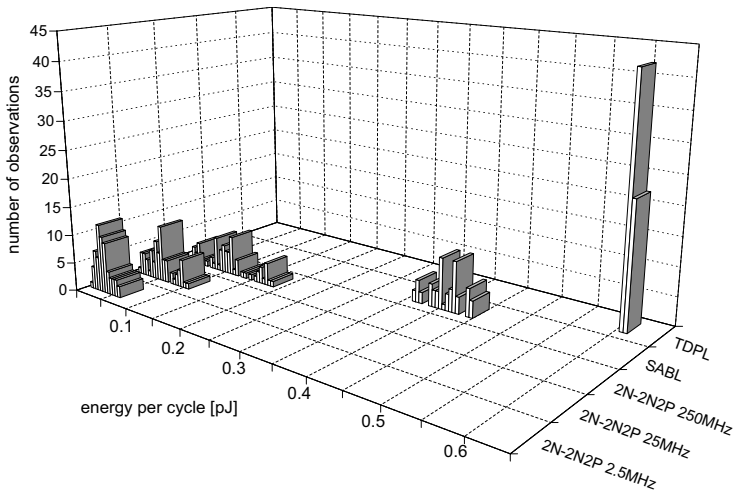

Fig. 4. FullAdder - energy consumption per cycle: TDPL and SABL vs. 2N-2N2P

As described in [19], Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) are heuristic metrics used in a number of works to evaluate the security of a logic style according to the variance of the power consumption over different keys. Also, comparing the difference-of-mean-energies which directly relates to the classical DPA attack [11] has been suggested to evaluate the security of the MDPL cells. However, in order to determine the amount of information leaked by a given logic style independently of a particular attack, an information theoretic metric, mutual information, has been introduced in [19].

$$\mathrm{I}\left(S_g; \mathrm{L}^q_{s_g}\right) = \mathrm{H}\left[S_g\right] - \mathrm{H}\left[S_g | \mathrm{L}^q_{s_g}\right], \tag{3}$$

where S denotes any possible candidate value of the correct signal S_g in a side-channel attack, and $\mathrm{L}^q_{s_g}$ is a vector of side-channel traces generated by the correct key class s_g. Also, $\mathrm{H}[\cdot]$ and $\mathrm{H}[\cdot|\cdot]$ are entropy and conditional entropy, respectively.

Since 2N-2N2P logic can be viewed as a pre-charged and not masked logic style, we apply their definition [19] to evaluate 2N-2N2P logic gates. As illustrated in Sect. 2.1, charges that remain on the capacitances of the function and complementary function blocks are discharged non-adiabatically. These discharges may repeat for each stage of the pipeline constructed by 2N-2N2P structure, and hence each secret s_g can give rise to different leakage traces, corresponding to the different values, v, existing in the pipeline. Therefore, the following definition is used to compute the conditional entropy for an 2N-2N2P circuit.

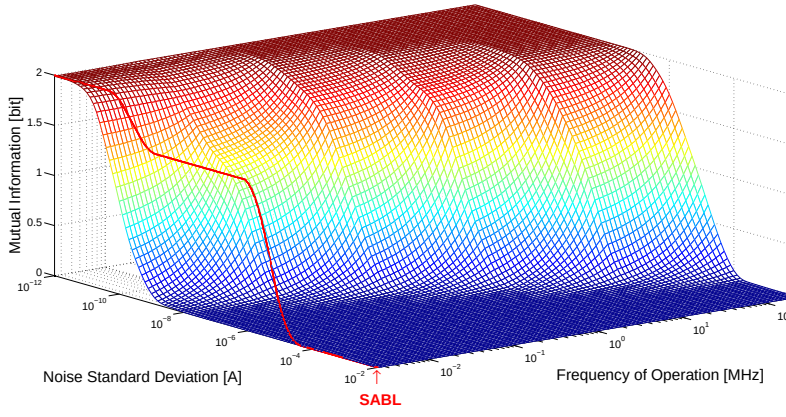

Fig. 5. Information leakage of 2N-2N2P AND/NAND gate

Note that a single 2N-2N2P gate is viewed as a pipeline with one stage.

$$\mathrm{H}\left[S_g|\mathrm{L}^q_{s_g}\right] = -\sum_{s_g}\Pr\left[s_g\right]\sum_{v}\Pr\left[v\right]\int \Pr\left[\mathrm{l}^q|s_g,v\right]\cdot\log_2\Pr\left[s_g|\mathrm{l}^q\right]dl, \qquad (4)$$

where $\Pr\left[s_g|\mathrm{l}^q\right] = \frac{\Pr[\mathrm{l}^q|s_g]}{\sum_s \Pr[\mathrm{l}^q|s]}$ and $\mathrm{l}^q_{s_g}$ is a realization of random vector $\mathrm{L}^q_{s_g}$. Since the consecutive values existing in the pipeline, v, are known by the adversary (or can be guessed), the probability $\Pr\left[\mathrm{l}^q|s_g\right]$ can be directly computed as $\Pr\left[\mathrm{l}^q|s_g,v\right]$.

According to the illustrated way in [19], we evaluate the mutual information for 2N-2N2P circuits with respect to the amount of noise in the side-channel measurements. In other words, we determine the noise threshold for different frequencies in order to compare the results with other full-custom logic styles (especially SABL). Similar to their assumption [19] to include various types of noise that effect the side-channel leakages, a Gaussian distribution is considered to model the overall effect of all the noise sources. In the following, we present the mutual information of different 2N-2N2P circuits for various operation frequencies in the presence of normally distributed noise. In order to consider the parasitic interconnection capacitances in simulations, two randomly chosen capacitances with a maximum amount of $10fF$ have been inserted on each 2N-2N2P gate output.

Since simulations were done in a high time resolution, each power trace consisted of millions of points (especially for low frequencies). We computed the mutual information for each point of the traces independently of the other points and then took the maximum information leakage for the given noise standard deviation. Fig. 5 shows the amount of information leakage of an 2N-2N2P AND/NAND gate vs. the noise standard deviation and the frequency of operation. Note that among all full-custom logic styles evaluated in [19], SABL

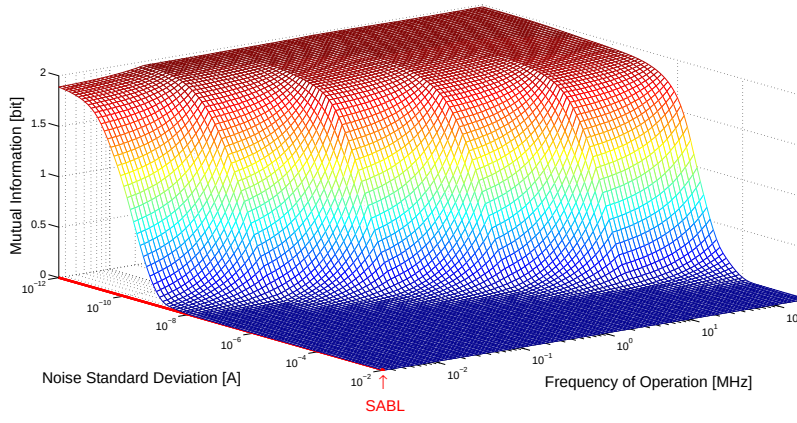

Fig. 6. Information leakage of 2N-2N2P XOR/XNOR gate

achieves the best result, i.e., 10^{-5}A for the threshold of the noise standard deviation. In case of 2N-2N2P, the noise threshold is the same for high frequencies (around 100MHz), but it is decreased significantly for lower frequencies (around 100KHz). As a result, contrary to the existing DPA-resistant logic styles, the vulnerability of 2N-2N2P circuits depends on the frequency of operation.

Since in the SABL XOR gate certain different inputs lead to identical leakages, and similarly, certain inputs give rise to very close leakages, the SABL XOR is much more secure than the SABL AND gate. However, in the case of 2N-2N2P, the leakage of the XOR gate is approximately similar to the AND gate. Fig. 6 shows the amount of information in the side-channel leakages for an 2N-2N2P XOR/XNOR gate. Therefore, the leakage of 2N-2N2P linear cells is higher than the SABL even in low frequencies. Note that DPA-resistant logics are invented to implement cryptographic algorithms which usually employ at least one high non-linear function.

The evaluation is limited to these two logic gates since the gate structures for the 2N-2N2P OR/NOR gate is completely similar to the AND/NAND gate and thus they lead to generate the same current curves. However, in order to evaluate a more complex non-linear circuit, an S-box of the PRESENT cipher [5] is taken into account to examine the capability of 2N-2N2P to construct DPA-resistant cryptographic hardware. Similarly, the amount of information leakage is reduced in low frequencies, and the threshold of the noise standard deviation is around 10^{-9} for the frequency of 10KHz. Its diagram is shown in the Appendix.

4 Conclusions

In this paper we have discussed how charge recovery logic styles can be used to implement cryptographic hardware that is secure against DPA attacks. Charge

recovery logic families have been introduced to implement low power circuits. On the other hand, several logic styles have been proposed to resist DPA attacks, but none of them can perfectly counteract DPA attacks. All of them increase the needed area and the power consumption significantly. To the best of our knowledge it is the first article dealing with the utilization of a charge recovery logic style as DPA-countermeasure.

We have shown that a simple charge recovery logic, so called 2N-2N2P, prevents information leakage even better than the DPA-resistant logic styles proposed so far. An important difference between charge recovery and other DPA-resistant logics is that the side-channel leakage of charge recovery circuits is frequency-dependent. Indeed, the information leakage is reduced in low frequencies. Consequently, the usage of these logic families in order to resist DPA attacks is more suitable in low-throughput pervasive devices such as passive RFID tags and wireless sensor networks where area and energy constrains are the major challenges that make other DPA-resistant logic styles impossible. On the other hand, these pervasive devices require DPA-resistance because they are not operated in a controlled environment.

Since the currently existing charge recovery logics have not been designed to prevent the information leakage, a novel full-custom logic style by observing the charge recovery rules should be designed.

References

1. 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.
2. W.C. Athas, L.J. Svensson, J.G. Koller, and E. Chou, "Low Power Digital Systems based on Adiabatic-Switching Principles," *IEEE Transactions On VLSI Systems*, vol. 2, no. 4, pp. 398-407, 1994.
3. 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.
4. 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.
5. A. Bogdanov, G. Leander, L.R. Knudsen, C. Parr, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT - An Ultra-Lightweight Block Cipher," In *Cryptographic Hardware and Embedded Systems – CHES 2007,* vol. 4727 of LNCS, Springer, pp. 450-466, 2007.
6. A. Blotti, R. Saletti, "Ultralow-Power Adiabatic Circuit Semi-Custom Design," *IEEE Transactions on VLSI Systems,* vol. 12, no. 11, pp. 1248-1253, 2004.
7. 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.
8. B. Gierlichs, "DPA-Resistance Without Routing Constraints?," In *Cryptographic Hardware and Embedded Systems – CHES 2007,* vol. 4727 of LNCS, Springer, pp. 107-120, 2007.

9. 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.
10. 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.
11. 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.
12. S. Kim, M.C. Papaefthymiou, "True Single-Phase Adiabatic Circuitry," *IEEE Transactions on VLSI Systems,* vol. 9, no. 1, pp. 52-63, 2001.
13. V.S. Kanchana Bhaaskaran, S. Salivahanan, and D.S. Emmanuel, "Semi-Custom Design of Adiabatic Adder Circuits," In *the 19th International Conference on VLSI Design held jointly with 5th International Conference on Embedded Systems Design, Proceedings,* pp. 745-748, 2006.
14. S. Kim, C.H. Ziesler, and M.C. Papaefthymiou, "Charge-Recovery Computing on Silicon," *IEEE Transactions On Computers,* vol. 54, no. 6, pp. 651-659, 2005.
15. Y. Moon and D.-K. Jeong, "An Efficient Charge Recovery Logic Circuit," *IEEE Journal of Solid State Circuits,* vol. 31, pp. 514-522, 1996.
16. 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.
17. S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks, *Revealing the Secrets of Smart Cards*," Springer, 2007. ISBN 0-387-30857-1.
18. F. Mace, F.-X. Standaert, I. Hassoune, J.-J. Quisquater, and J.-D. Legat, "A Dynamic Current Mode Logic to Counteract Power Analysis Attacks," In *Conference on Design of Circuits and Integrated Systems – DCIS 2004, Proceedings,* pp. 186-191, 2004.
19. F. Macé, F.-X. Standaert, and J.-J. Quisquater, "Information Theoretic Evaluation of Side-Channel Resistant Logic Styles," In *Cryptographic Hardware and Embedded Systems – CHES 2007,* vol. 4727 of LNCS, Springer, pp. 427-442, 2007.
20. 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.
21. 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.
22. 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.
23. D. Suzuki and M. Saeki, "Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style," In *Cryptographic Hardware and Embedded Systems – CHES 2006,* vol. 4249 of LNCS, Springer, pp. 255-269, 2006.
24. P. Schaumont and K. Tiri, "Masking and Dual-Rail Logic Don't Add Up," In *Cryptographic Hardware and Embedded Systems – CHES 2007,* vol. 4727 of LNCS, Springer, pp. 95-106, 2007.
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. K. Tiri, M. Akmal, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Anal-

ysis on Smart Cards," In *European Solid State Circuits Conference, Proceedings*, pp. 403-406, 2002.
27. 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.
28. B. Wang and P. Mazumder, "On Optimality of Adiabatic Switching in MOS Energy-Recovery Circuit," In *International Symposium on Low Power Electronics and Design, Proceedings,* pp. 236-239, 2004.

Appendix: 2N-2N2P PRESENT S-box

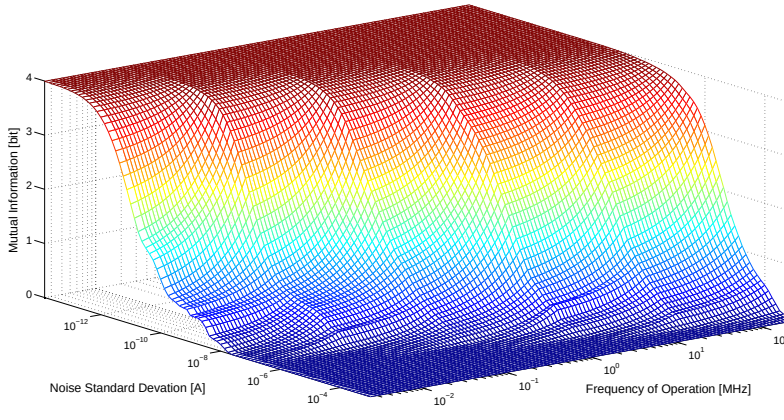

Fig. 7. Information leakage of 2N-2N2P PRESENT S-box