Low Power Bit-Parallel Cellular Multiplier Implemetation in Secure Dual-Rail Adiabatic Logic

Cancio Monteiro, Yasuhiro Takahashi, and Toshikazu Sekine

***Abstract*—The bit-parallel multiplier over Galois filed arithmetic algorithm and the circuit architecture have been widely studied and implemented in cryptosystem. In this paper, we implement the proposed secure and low-power dual-rail adiabatic logic circuit into the bit-parallel cellular multiplier over $GF(2^4)$. The full custom design of the layout has been designed in cadence virtuoso IC6.1 with the chip size of 172×155 μm^2, and the post-layout cyclical power consumption of 14pJ at 12.5MHz using 0.18μm CMOS technology has achieved; while, the well-known conventional TDPL logic in our work using the same technology occupied 183×173 μm^2 of the chip size and 123pJ per cycle. The thoroughly investigation results define that our proposed logic improve energy reduction and the circuit immunity to side-channel attack in the low frequency application, whereas, the TDPL shows the better security performance at high frequency range.**

***Index Terms*— Bit-parallel multiplier, adiabatic, low-power, side channel attack, cryptography.**

I. Introduction

In the recent cryptographic world, the finite field arithmetic plays an important role in modern coding theory and cryptographic system. The algorithm, architecture, and the circuit configuration have been extensively developed in finite field $GF(2^m)$ [1]–[3] for low complexity, computation time efficiency, and the low-power consumption. When it links to the cryptographic hardware implementation, one of the main issues is related to the security of processed information. Therefore, the side-channel analysis (SCA) attacks were introduced in [4] have become crucial challenges for cryptographers and hardware engineers to maintain the secrecy of private information in the cryptographic hardware, such as in smart card. Among other types of side-channel attacks, differential power analysis (DPA) attacks [5] and differential electromagnetic analysis (DEMA) [6] have been taken into consideration because of their technical measurement and statistical calculation efficiency to find the secret key and the applicability on various types of implementation.

The main factors of aforementioned attacks are related to CMOS logic power consumption and required operational time of cryptographic hardware itself. Regarding power consumption in cryptographic implementation such as smart card, logic design should be highly considered in order to mask the input logic values and also reduce the power consumption in the digital circuit level. In responding to the SCA attacks, several works on the cell level have been reported by the sense amplifier based logic (SABL) [7], three-phase dual-rail pre-charged logic (TDPL) [8]. Among those implemented logic styles in the cell library, majority of them applied conventional CMOS logic operation that causes the high spike current occurrence and huge energy consuming. As a result, the DPA and DEMA attacks are a bit difficult to avoid. Hence, our approach here is to design secure logic with low peak current transition and low energy consumption by exploiting an adiabatic switch principle [9]. In recent, few papers of secure adiabatic logic have been published which referred to this work, such as SAL [10], and SyAL [11]. The SAL and SyAL have achieved low power and high resistance to DPA attacks as stated, however, the throughout evaluation in our previous work [12] found out that they still perform certain different current values for every input transition.

In this work, the previous proposed logic is implemented in LSI design in a low complexity cellular multiplier over CF (2^4). The comparative post-layout SPICE simulation is conducted with the well-known conventional TDPL CMOS logic style.

II. Implementation of the Proposed Adiabatic Logic in The Bit-Parallel Cellular Multiplier over $GF(2^4)$.

A. Adiabatic Logic Technique

Adiabatic switching is commonly used in minimizing energy lost during charging/discharging period at all nodes of the circuit. The main idea of adiabatic switching is shown in Fig. 2(b), which indicates a transition that is considered sufficiently slow that heat is not significantly emitted. Adiabatic dissipated energy: $E_{\text{adiabatic}} = 2(RC/\tau)CV_{dd}^2$; where R is the effective resistance in driven device, C is the output node capacitance to be switched, τ is time over which the switching occurs, and the V_{dd} is the voltage to be switched across. Ideally, the charging $E_{\text{adiabatic}}$ tends to zero by increasing the length of the τ. In contrast, the conventional CMOS logic operation in Fig. 1(a) is the following equation: $E_{\text{conv.:}} = CV_{dd}^2/2$; where, it is possible to reduce the charging energy only by reducing V_{dd} or capacitor C. Fig. 1(c) shows a comparison of peak supply current for equivalent RC models of the conventional CMOS logic and the adiabatic logic. The instantaneous peak supply current of the adiabatic logic is significantly lower than that of the conventional CMOS logic

Manuscript received February 28, 2013; revised June 28, 2013.

Cancio Monteiro is with the Graduate School of Engineering, Gifu University, 1-1 Yanagido, Gifu-shi, 501-1193, Japan (corresponding author, e-mail: canciotimor@gmail.com).

Yasuhiro Takahashi and Toshikazu Sekine are with Faculty of Engineering, Gifu University, 1-1 Yanagido, Gifu-shi, 501-1193, Japan (e-mail: {yasut,sekine}@gifu-u.ac.jp).

style.

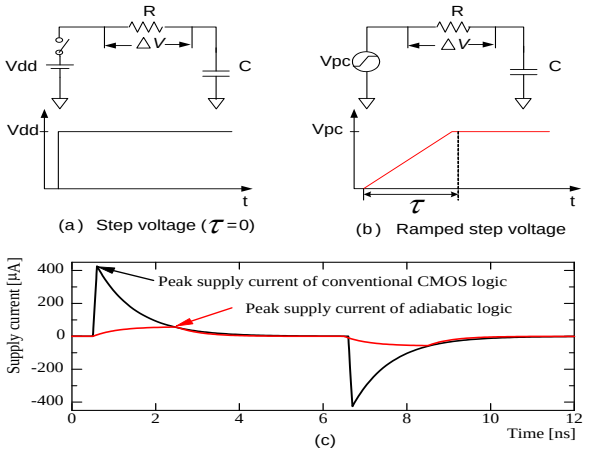

Fig. 1. Comparison of supply currents for equivalent RC models of CMOS logic (a) step voltage and adiabatic logic (b) ramped step voltage. (c) The peak supply current of adiabatic logic is significantly lower than the conventional CMOS logic under the same parameters and conditions.

B. Proposed Charge-Sharing Symmetric Adiabatic Logic

Detail proposed charge-sharing symmetric adiabatic logic (CSSAL) operation was described in [13]. We have presented here CSSAL NAND/AND logic in Fig. 2(a), and its equivalent RC model at pull-down network when the condition of (A,B) is (1,1), (0,1), (0,0), and (1,1), as labeled in Fig. 3(b), thus, to clarify that there are always same amount of charges for all possible input condition which is the merit of our proposed logic to consume uniform energy at any input condition (transition). The transistor schematic of CSSAL XNOR/XOR is similar to NAND/AND logic, the difference is only at the arrangement of input signals; hence, the internal equivalent RC model is also similar as shown in Fig. 2(b).

In contrast, the TDPL NAND/AND logic [8] in Fig. 3(a) was implemented using universal dual-rail pull-down network tree. The internal equivalent RC model in Fig. 3(b) indicates that there are some floating capacitors during charging and discharging process; however TDPL logic inserts discharged cells (MN1 and MN4) to discharge the output line that was not discharged during the evaluation phase. This phenomenon makes the TDPL logic avoid input/output data dependencies, and consumes almost constant energy for all input transitions; however, TDPL is the most energy consuming in comparing to the proposed logic.

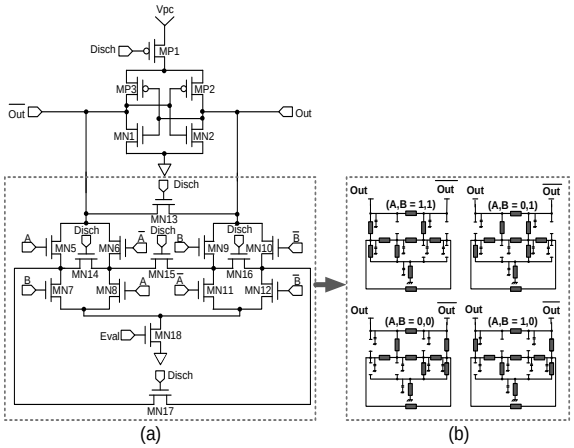

Fig. 2. Proposed CSSAL; (a) NAND/AND logic structure, (b) Internal equivalent RC model at pull-down network.

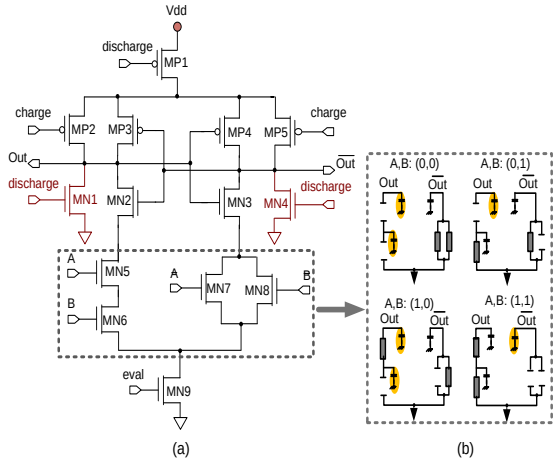

Fig. 3. Conventional TDPL; (a) NAND/AND logic structure, (b) Internal equivalent RC model at pull-down network. The yellow marked color is the floating capacitor at each pull-down network condition.

C. Implementation

The targeting logic cell in this work was proposed in a novel cellular architecture [1] which has explored inner-product multiplication algorithm to compute the function of $AB+C$ into low-complexity and less computation time cellular architecture in a class field GF(24). There are several definitions described and arithmetic calculation have been done to define cellular array multiplication :

$$AB^2 = \sum_{j=0}^{m} A^{(2^j)}[B^2]^{(-j)},$$

where m = 4 to calculate the function block of the bit-parallel multiplier over $GF(2^4)$.

The similar architecture proposed in [2] for computing AB^2+C which is also suitable for LSI implementation for cryptosystem; however, it has the drawback of high circuit complexity and requires more computation time per cell. The multiplier circuit architecture is depicted in Fig. 4. The complexity of inner cell includes one 2-input AND gate and 2-input XOR gate with the logic depth from each primary input line to the output line is symmetrically m + 1 basic cell. The complexity of cellular multiplier over $GF(2^4)$ includes $(m + 1)^2$ identical cells. For the purpose of comparison study, we have implemented both of the proposed CSSAL logic and the TDPL logic into the multiplier circuit in Fig. 4. Each circuit layout has designed in full custom design using cadence virtuoso IC6.1 with the chip size of the CSSAL multiplier is $172 \times 155 \mu m^2$ and the TDPL has $183 \times 173 \mu m^2$ as depicted in Fig. 5.

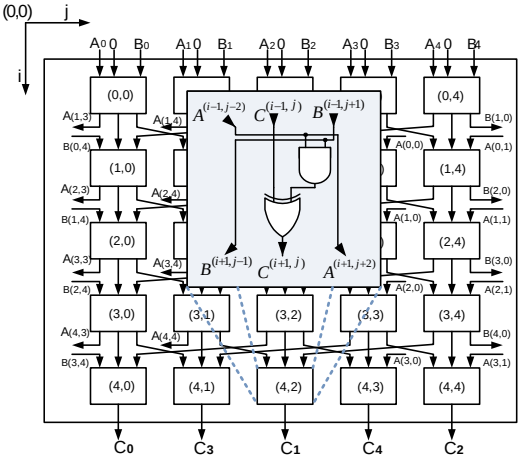

Fig. 4. Configuration of bit-parallel cellular multiplier over $GF(2^4)$.

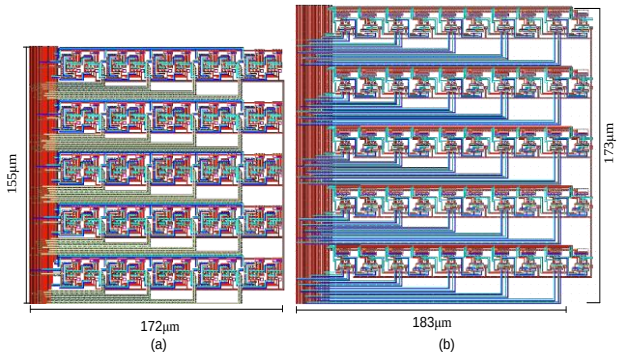

Fig. 5. Full custom layout design of the circuit structure in Fig. 4; (a) CSSAL multiplier, (b) TDPL multiplier.

III. Simulation and Results

A. Simulation Condition

The evaluation provided in this paper was made using SPICE simulation with a 0.18μm, 1.8V standard CMOS technology. We have done the post-layout simulation for the CSSAL multiplier in comparison to the TDPL multiplier using the same parameters and under the same condition. The input signals of our proposed CSSAL multiplier circuit are all trapezoidal waveforms with adiabatic power clock frequency range from 1.25-50MHz. On the other hand, the TDPL is supplied with constant 1.8V of V_{dd}, and the input discharge, charge, evaluation signals' dynamic frequency are 1.25–50MHz as well. The previous work in [12] reported the pre-layout simulation with active power clock frequency range is 1.25–125MHz. However, the more accurate information provided in this optimization work shown that the maximum speed of our proposed CSSAL multiplier is 50MHz. Moreover, the DPA attacks analyze the peak current differences to reveal the secret-key during encryption and decryption; hence, our job is to analyze the various instantaneous peak supply current and the various energy consumption per input transition which will be summarized in the following subsection.

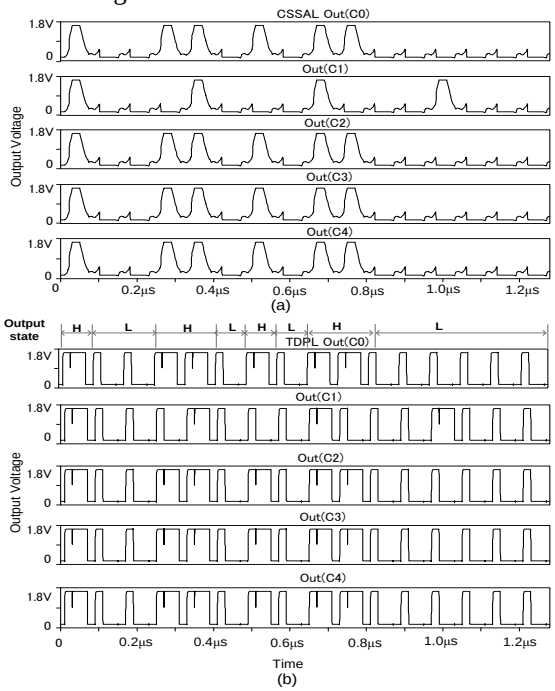

Fig. 6. The post-layout output voltage; CSSAL multiplier (top) and the TDPL multiplier (bottom).

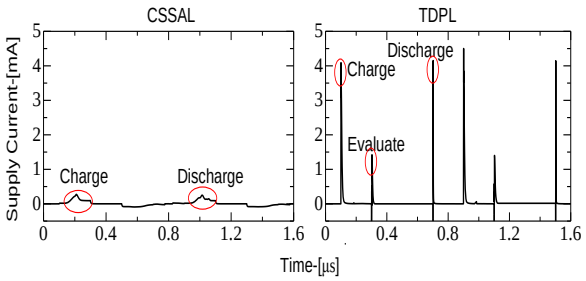

Fig. 7. The comparison of the peak supply current of the CSSAL and the TDPL multiplier when complementary dual output states are shifted for charging and discharging process.

B. Results

The simulation result of output voltage is depicted in Fig. 7(a) and (b) for the CSSAL multiplier and the TDPL multiplier, respectively. The TDPL logic was implemented using pre-charged logic style; hence, the pre-charged signals at the complementary L (low) voltage is appeared as H (high); however, in comparing to CSSAL, we consider them as Low level, which is indicated as L and H on the top of the TDPL Out(C0).

The comparative results from the security view point are summarized in Table I. The data of power consumption of each circuit are drawn as: $E_{diss.} = \int_0^{\tau} V(t)I(t)dt$, which is adopted as figure of merit to measure the resistance against power analysis attacks. The calculation for normalized energy deviation (NED) is defined as $(E_{max}\text{-}E_{min})/E_{max}$ and normalized standard deviation (NSD) is σ_E/E [8]. The $\bar{E}$ is the average of energy dissipation over every respective transition, and standard deviation is defined as: $\sigma_E = \sqrt{\sum_{i=E1}^{En}(Ei-\bar{E})^2/n}$.

TABLE I: Simulation and Calculation Results of the Bit-Parallel Cellular Multiplier over $GF(2^4)$ at 1.25-50MHz Input Clock Frequency

Frequency	1.25MHz		12.5MHz		50MHz	
	CSSAL	TDPL	CSSAL	TDPL	CSSAL	TDPL
Emin[pJ]	0.4	7.04	0.65	6.9	0.94	6.79
Emax[pJ]	0.46	35.44	1.24	9.61	2.63	7.44
$\bar{E}$[pJ]	0.43	14.31	0.88	7.67	1.52	7.04
σE[pJ]	0.015	8.4	0.21	0.79	0.58	0.18
NED[%]	12.04	80.13	47.33	28.18	64.19	8.7
NSD[%]	3.49	58.71	24.48	10.27	38.06	2.49

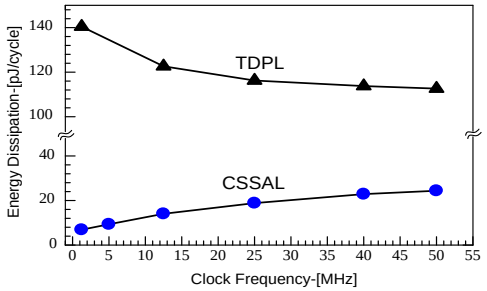

Fig. 8. The comparison of the simulated post-layout energy dissipation of the bit-parallel cellular multiplier over $GF(2^4)$ in respect to the different input clock frequencies.

We measure the parameters of NED and NSD which means the ability of the logic resistance against power

analysis attack. An important property of NES and NSD explain the consumed energy is more constant for different input transition if we achieve more small values. Hence, by observing the result in Table I, the proposed logic exhibits its ability at low frequency range, because it has smallest values of NED and NSD. Conversely, the TDPL multiplier is performing its ability at high frequency band. In our knowledge, the DPA and DEMA attacks reveal the secret information by statistically analyzing the power fluctuations and the current amplitude of attacked hardware, such as smart card. In this case, the proposed CSSAL is stronger to thwart DEMA attack because the peak supply current comparison in Fig. 7 shows that CSSAL is much lower that the TDPL.

Apart from the logic ability for resistance against SCA attacks, the power reduction is also one of the research targets. It is obviously described by the graphical information in Fig. 8 that our proposed CSSAL multiplier has significant energy reduction about nine times lower than that of the TDPL multiplier at 12.5MHz.

IV. Conclusion

In this paper, we have presented the post-layout of the proposed CSSAL and the conventional TDPL in the bit parallel cellular multiplier over $GF(2^4)$. Thoroughly investigation and comparative study on the logic ability and power reduction has been carried out; whereas, the optimum results have shown that the proposed logic consumes uniform energy at low frequency, and is more power efficient compare to the conventional TDPL CMOS logic style. Base on the logic speed, security performance and low-power requirement, we deduce that our proposed logic is applicable for contactless smart cards, RFID tags, and wireless sensors.

Acknowledgment

The custom circuits discussed in this paper have been implemented with Cadence and Synopsys tools through the chip fabrication program of the VLSI Design and Education Centre (VDEC) at the University of Tokyo in collaboration with ROHM Corporation.

References

[1] C. H. Liu, N. F. Huang, and C. Y. Lee, "Computation of AB^2 multiplier in CF(2^4) using an efficient low-complexity cellular architecture," *IEICE Trans. Fundamentals*., vol. E83-A, no. 12, pp. 2657–2663, Dec. 2000.

[2] C. Y. Lee, E. H. Lu, and L. F. Sun, "Low-complexity bit-parallel systolic architecture for computing AB^2 + C in a class of finite field $GF(2^4)$," *IEEE Trans. on Circuit and System—II: Analog and Digital Signal Processing*, vol. 48, no. 5, pp. 385-393, May 2001.

[3] H. S. Kim and K. Y Yoo, "Multiplier for public-key cryptosystem based on cellular automata," in *Proc. MMM-ACNS 2003*, vol. 2776, 2003, pp. 436–439.

[4] P. Kocher, "Timing attacks on implementation of Diffie-Hellman, RSA, DSS and other system," in *Proc. Advances in Cryptology-CRYPTO*'96, vol. 1109, 1996, pp. 104–113.

[5] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. of 19th Int'L Advances in Cryptology Conf. – CRYPTO'99*, 1999, pp. 388–397.

[6] E. D. Mulder, S. B. Ors, B. Preneel, and I. Verbauwhede, "Differential electromagnetic attack on an FPGA implementation of elliptic curve cryptosystems," in *Proc. of WAC'06*, Budapest, 24–26 July 2006, pp. 1–6.

[7] 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. European Conf. Solid-State Circuits*, Firenze, Italy, Sept. 24–26, 2002, pp. 403–406.

[8] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dualrail pre-charge logic," in *Proc. Workchop on Cryptographic Hardware and Embedded Systems*, Yokohama, Japan, Oct. 10–13, 2006, pp. 232–241.

[9] W. C. Athas, L. J. Svesson, J. G. Koller, N. Traztzanis, and E. Y. C. Chuo, "Low power digital system based on adiabatic-switching principles," *IEEE Trans. VLSI System*, vol. 2, no. 4, pp. 398–406, Dec. 1994.

[10] M. Khatir and A. Moradi. (2008). Secure adiabatic logic: A low-energy DPAresistant logic style. *Cryptology ePrint Archive*, [Online]. Available: http://eprint.iacr.org/2008/123

[11] 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.

[12] C. Monteiro, Y. Takahashi, and T. Sekine, "DPA resistance of charge-sharing symmetric adiabatic logic," in *Proc. of IEEE ISCAS*, Beijing, China, May 19–23, *2013*.

[13] C. Monteiro, Y. Takahashi, and T. Sekine, "A comparison of cellular multiplier cell using secure adiabatic logics," in *Proc. of Int. Conf. Circuit/ System, Computers and Communications*, Sapporo, Japan, July 14–18, 2012, pp. 4.

Cancio Monteiro was born on March 2, 1981 in Lospalos, Timor-Leste. He received his B.E. in National University of East Timor (UNTL) in 2005. He obtained his M.Eng. degree in the Graduate School of Engineering, Gifu University in 2012, where he is currently working toward his Ph.D. degree in the same university.

His research interests include low power VLSI design for information security systems. He is a student member of IEICE, IEEE.

Yasuhiro Takahashi was born in 1977. He received his B.E., M.E., and Ph.D. degrees from Yamagata University in 2000, 2002, and 2005 respectively. From 2005 to 2007, he was a Research Associate at the Department of Electrical and Electronic Engineering, Gifu University, where he is currently an Assistant Professor. His research interests include the design of low-power circuits and high-performance DSP functions. He is a member of IACSIT, IAEAG, IEEE, IEEJ, and IEICE.

Toshikazu Sekine received his B.E., M.E. and Ph.D. degrees from Yamagata University in 1974, 1976, and 2002, respectively. Since 1976, he has been with the Faculty of Engineering, Gifu University and is currently an Associate Professor. His current research interests include electro-magnetic compatibility (EMC) analysis, lossy transmission line modeling, and microwave system and high-speed PCB signal integrity analysis. He is a member of IEEE and IEICE.