

C-12-41

LSI Implementation of a Bit-Parallel Cellular Multiplier over $GF(2^4)$ using Charge-Sharing Symmetric Adiabatic Logic.

Cancio Monteiro¹Yasuhiro Takahashi²Toshikazu Sekine²Graduate School of Engineering, Gifu University¹Faculty of Engineering, Gifu University²

Abstract

This paper presents a verification of the operating speed in a bit-parallel cellular multiplier over $GF(2^4)$ using a secure dual-rail charge-sharing symmetric adiabatic logic. The multiplier LSI chip measured in this work was fabricated using $0.18\ \mu\text{m}$ CMOS process technology. Maximum power clock frequency for chip measurement is 5 MHz, whereas the post-layout simulation is up to 50 MHz and the pre-layout simulation reaches 125 MHz using the same individual logic.

1 Introduction

Finite field arithmetic has played an important role in modern coding theory, computer algebra, and cryptographic system. From the view point of the cryptographic hardware implementation, one of the main issues is related to the security of processed information. Apart from the secure logic ability to withstand side channel analysis attacks, the power efficiency is also a demand of our society. To the best of our knowledge, many works on secure logic design in the simulation level and further in the LSI implementation have been done in the conventional CMOS logic operation. As a result, the high dynamic power consumption becomes a challenge and the motivation in our work. In our approach for secure and low-power logic implementation, we have designed a new secure logic style that is based on the adiabatic switching principle [1]. The full custom layout was designed in cadence virtuoso IC6.1 with the chip size of $172 \times 155\ \mu\text{m}^2$ [2]. In this work, the fabricated LSI chip measurement is conducted. The operating speed of the multiplier in the LSI is checked and compared with the pre-layout and the post-layout simulation result.

2 LSI Measurement Result

The circuit schematic of the bit-parallel cellular multiplier over $GF(2^4)$ and the photomicrograph are shown in Figs. 1(a),(b), respectively. As shown in Fig. (a) that the inner cell composes of dual-input AND and XOR logic, where those individual logic's transistor schematic can be found in [1]. The LSI measurement result of the input and output signals at 1.25 MHz power clock frequency is shown in Fig. 2. In this measurement, the input signals of the $In1 = \{A0, A1, A2, A3, A4\}$, $In2 = \{B0, B1, B2, B3, B4\} = "1"$, thus the output voltage of a multiplier $\{C0, C1, C2, C3, C4\}$ are currently produced as $Out = "1"$. The V_{pc} supply current in the bottom of Fig. 2 indicates that the peak current is uniformly plotted which may resistive to side channel analysis attacks.

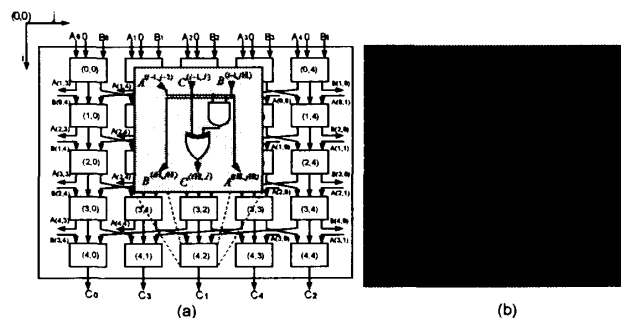


Fig. 1 (a) Circuit structure of the bit-parallel cellular multiplier over $GF(2^4)$, (b) Photomicrograph of the bit-parallel cellular multiplier over $GF(2^4)$.

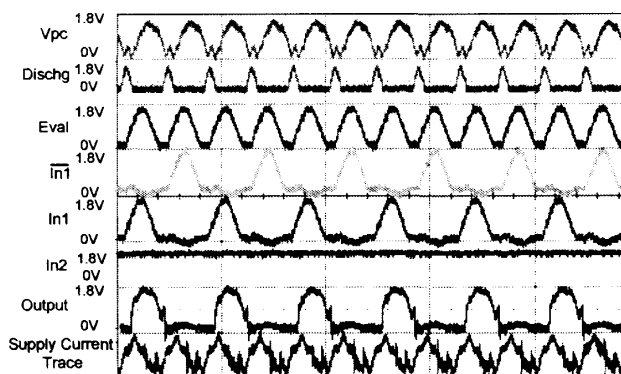


Fig. 2 Input and output signals of the bit-parallel cellular multiplier over $GF(2^4)$ from the measurement result.

3 Conclusion

We have verified a multiplier logic functionality in the LSI measurement that, the output voltages are correctly measures. The maximum operating power clock frequency in the measurement is 5 MHz, which is slow down from 50 MHz in the post-layout simulation and a hundred times speed down from pre-layout simulation using the same individual logic.

References

- [1] C. Monteiro, Y. Takahashi, and T. Sekine, "Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level," *Microelectronics Journal*, vol.44, no.6, pp.496–503, June 2013.
- [2] C. Monteiro, Y. Takahashi, and T. Sekine, "Low power secure CSSAL bit-parallel multiplier over $GF(2^4)$ in $0.18\mu\text{m}$ CMOS technology," in *Proc. IEEE ECCTD*, Dresden, Germany, Sept. 8-12, 2013. (Accepted)