Measurement of CSSAL Multiplier over $GF(2^4)$ LSI Implemented in 0.18μm CMOS Technology

Cancio Monteiro[1] Yasuhiro Takahashi[2] Toshikazu Sekine[2]

Graduate School of Engineering, Gifu University[1] Faculty of Engineering, Gifu University[2]

Abstract

This paper presents a measurement result of the charge-sharing symmetric adiabatic logic (CSSAL) multiplier over $GF(2^4)$ LSI implemented in 0.18μm CMOS process technology. Supply current traces regard to input-output transitions are measured at 1.25 MHz of power clock frequency, and achieved 1.13 μW of power consumption.

1 Introduction

Finite field arithmetic plays an important role in modern coding theory and practical application of cryptographic system. From the view point of the cryptographic hardware implementation, one of the main issues is related to the security of processed information by a differential power analysis (DPA) attacks. As a contribution for counteracting DPA, we have designed a new secure logic style that is based on the adiabatic switching principle [1]. In this work, the fabricated LSI multiplier over $GF(2^4)$ in 0.18 μm CMOS process using the proposed charge-sharing symmetric adiabatic logic (CSSAL) is measured, and the LSI chip immunity for resistance against DPA attack is discussed.

2 LSI Measurement Result

The circuit schematic of the bit-parallel cellular multiplier over $GF(2^4)$, the LSI photomicrograph, and the measurement setup are shown in Figs. 1. The inner cell of the bit-parallel cellular multiplier over $GF(2^4)$ composes of dual-input AND and XOR logic, where those individual logic's transistor schematic can be found in [1]. The features of the fabricated LSI of the CSSAL multiplier are summarized in 1. In this measurement technique, we combined the connection of the input signals $In1 = \{A0, A1, A2, A3, A4\}$, $\bar{In1} = \{\bar{A0}, \bar{A1}, \bar{A2}, \bar{A3}, \bar{A4}\}$, $In2 = \{B0, B1, B2, B3, B4\} = 1$ (constant V_{dd}) and $\{\bar{B0}, \bar{B1}, \bar{B2}, \bar{B3}, \bar{B4}\} = 0$ (connected to ground); accordingly, the output voltage of a cellular multiplier $\{C0, C1, C2, C3, C4\}$ are correctly produced as $In1 \times In2 = \text{Out} = 1$ when the $In1 =$ "1". To the best of our knowledge, the DPA attack reveals the secure information by a hypothetical probe measurement on smart card, and then statistically analyzing the peak current/power differences at certain interval time during cryptographic hardware operation. Therefore, in this work, we have measured the supply current trace by inserting a small shunt resistance $R_s = 1\ \Omega$ between V_{ss} pin of the multiplier chip and the true source (ground), as shown in Fig. 1. The Vpc supply current in Fig. 2 is plotted as (a) Transition of $In1 = 0\rightarrow1$, $1\rightarrow0$ when $In2 = 0\rightarrow0$; (b) Transition of $In1 = 0\rightarrow1$, $1\rightarrow0$ when $In2 = 1\rightarrow1$; (c) Transition of $In2 = 0\rightarrow1$, $1\rightarrow0$ when $In1 = 0\rightarrow0$; (d) Transition of $In2 = 0\rightarrow1$, $1\rightarrow0$ when $In1 = 1\rightarrow1$. Results of this transitions in Fig. 2 indicate that the peak current is uniformly plotted which may resistive to DPA attacks.

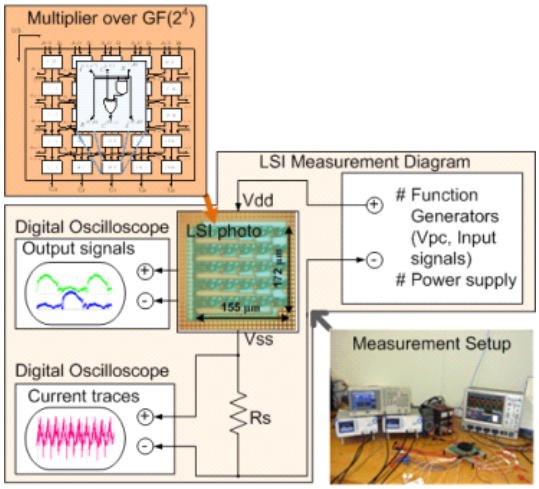

Fig. 1 The diagram of the equipment used for LSI chip measurement.

Table 1 CSSAL multiplier chip feature summary

Feature	Value
Technology	0.18 μm CMOS process
Power Voltage	1.8 V
Core Size	155(W) $\times$ 172(H) μm^2
No. of Transistor	950
Dynamic Operating Frequency	0.5–5 MHz
Power Dissipation	1.13 μW @ 1.25 MHz

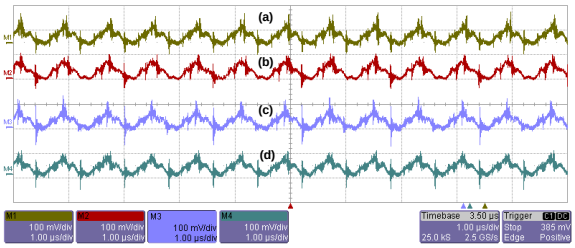

Fig. 2 Supply current traces of a representation input transition. Vertical scale: 100 mV/div. Horizontal scale: 1 μV/div.

3 Conclusion

The CSSAL multiplier chip performs a uniform power trace that is securely applicable for low-power and low frequency devices, such as smart cards, RFID tags and wireless sensors.

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.