A-7-6

Investigation Study of Inner-cell Bit-Parallel Multiplier over $GF(2^m)$ Using Secure Adiabatic Logic Style

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 investigates the logic security of inner cell bit-parallel multiplier over $GF(2^m)$ using secure logic styles. We evaluate the logic ability for resistance against DPA attack from the view point of instantaneous supply current regarding to the possible input transitions. The investigation results using our proposed logic has its ability for DPA attack compare to other investigated adiabatic logic, and is more power efficient in comparison to well-known conventional secure TDPL logic style.

1 Introduction

Differential power analysis (DPA) attacks are the most popular type of power analysis attacks to reveal the secret information in cryptosystem, such as smart card. A DPA attack seeks to crack the secret key of a smart card by statistically analyzing power fluctuations that occurs while the device encrypts and decrypts large blocks of data. Apart from DPA attack, electromagnetic radiation attack (DEMA) and other side-channel attacks on cryptographic hardware has been extensively studied. DEMA attack described that, current flow during the switching of the CMOS gates causes a variation of the electro-magnetic field surrounding the chip that can be monitored by inductive probes which are particularly sensitive to the related impulse. Hence, we are encouraged to design a robust secure logic for those aforementioned attacks for application in advanced encryption standards (AES) hardware architecture targeted for smart card.

2 Simulation and results

We investigate our proposed logic [1] with other previously published secure logic styles [2]–[4] in bit-parallel cellular multiplies over $GF(2^m)$ using SPICE simulation with a 0.18 μm, 1.8 V standard CMOS process technology. The comparison of inner cell cellular multiplier is depicted in Fig. 1 [5]. The evaluation logics are investigated under the same frequency operation: the power supplies of adiabatic logics are all trapezoidal waveform, power clock frequency is 12.5MHz, and inverter input frequency are set to 6.25 MHz for all instigated logics.

We calculate the normalized energy deviation (NED) and normalized standard deviation (NSD) of bit-parallel multiplier using A-cell and B-cell separately as shown in Table 1. The merit of NED and NSD is to measure the ability of the logic against power analysis attack. The more small value of NES and NSD, the consumed energy is more constant for different input transition. Observing the Table 1, our proposed logic is suitable for A-cell circuit in bit-parallel cellular multiplier over $GF(2^m)$ for AES hardware architecture design.

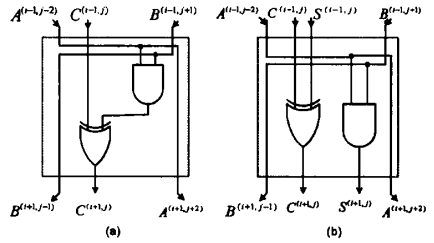

Fig. 1 Investigation of inner cell circuit; (a) A-cell circuit, (b) B-cell circuit.

Table 1 Simulation and calculation results for B-cell circuit and bit-parallel cellular multiplier over $GF(2^4)$.

		$GF(2^4)$ using A-cell			
		SAL	SyAL	Proposed	TDPL
E_{min}	fJ	337.15	311.64	310.28	3957.84
E_{max}	fJ	628.92	418.25	350.74	4112.35
$\overline{E}$	fJ	506.78	382.02	333.86	4042.54
σ_E	fJ	95.42	31.02	11.15	40.77
NED	%	50.65	25.49	11.54	3.76
NSD	%	18.83	8.12	3.32	1.01
		$GF(2^4)$ using B-cell			
E_{min}	fJ	345.70	318.12	342.01	3892.87
E_{max}	fJ	842.90	427.27	435.56	4053.52
$\overline{E}$	fJ	592.63	396.04	392.11	3943.42
σ_E	fJ	142.56	34.25	32.21	44.47
NED	%	58.98	25.55	21.48	3.96
NSD	%	24.06	8.65	8.47	1.12

3 Conclusion

The investigation and comparison results show that our proposed logic in A-cell circuit structure has ability for DPA and DEMA attacks, because it balances the transitional currant traces and lowers peak supply current values 36-times small compare to the conventional TDPL logic style. The power analysis model and the complete logic implementation using our proposed logic for AES architecture in smart card are addressed in future work.

References

[1] C. Monteiro, Y. Takahashi and T. Sekine,"A comparison of cellular multiplier cell using secure adiabatic logics," in *Proc. ITC-CSCC'12*, Sapporo, Jul. 15-18, 2012 (*accepted*).

[2] M. Khatir, and A. Moradi, "Secure adiabatic logic: A low-energy DPA-resistant logic style," in *IACR Eprint archive* (Available URL: http://eprint.iacr.org/2008/123).

[3] B.-D. Choi, K.E. Kim, K-S. Chung, and D.K. Kim, "Symmetric adiabatic logic circuits against differential power analysis," in *ETRI Journal*, vol. 32, no. 1, pp. 166–168, Feb. 2010.

[4] M. Bucci, L. Giancane, R. Luzzi and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. CHES'06*, LNCS, vol. 4249, pp. 232–241, 2006.

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