Power Analysis Attack on the Masking Type Conversion Algorithm Using Exponentiation

Young In Cho', Dong-Guk Han[g], Seokhie Hong', Young-Ho Park[a]

'LIST (Center for Information Security Technologies), Korea University, Anam-dong, Seongbuk-gu, Seoul, 136-713, South Korea.
[2]Department of Mathematics, Kookmin University, Seoul, South Korea.
[3]Department of Information Security Systems, Sejong Cyber University, Seoul, South Korea.
elowey@korea.ac.kr, christa@kookmin.ac.kr, shhong@korea.ac.kr, youngho@sjcu.ac.kr

Abstract. In the recent years, power analysis attacks were widely investigated, and so various countermeasures have been proposed. In the case of block ciphers, such as SEED and IDEA, masking methods that blind the intermediate results in the algorithm computations (encryption, decryption and key-schedule) are well-known. The masking type conversion is unavoidable since Boolean operation and arithmetic operation are performed together in block ciphers. Messerges proposed simple masking type conversion algorithms which are resistant to general power analysis. In this paper, we propose a new adversary model to break the Messerges's masking type conversion algorithm. Furthermore, we show that our adversary model can be a practical threat by mathematical proof and simulation results.

Keywords: Power analysis attack, Masking method, Masking type conversion, DPA, CPA

1 Introduction

Side channel attack was first introduced by Kocher et al. in 1996 [5]. Since side channel attack has been introduced, it is well known that careless implementation can leak information about the secret key through the execution time and electrical power consumption of smart cards and smart phones or the other secure cryptographic devices. Therefore, to be resistant against side channel attacks, various countermeasures have already been proposed. The masking method [1][3][4][6] is known to be one of the most general countermeasures against differential power analysis (DPA) [6][7] and correlation power analysis (CPA) [2] the most powerful attacks of side channel attacks. The masking method is a algorithmic countermeasure to prevent the first-order DPA and CPA attacks and it is more adequate for low cost smart cards that have small RAM size than hardware countermeasures like jitter and cycle stealing.

In case of block ciphers, many of them combine Boolean and arithmetic functions, such as IDEA or several of AES candidates and SEED. Thus a way to convert back

and forth between Boolean masking and arithmetic masking is needed. Messerges proposed two conversion algorithms between Boolean masking and arithmetic masking which are resistant against DPA [8].

In this paper, we propose a new adversary model which is able to make a relation between the guessed value and the power consumption obtained. We show that the proposed methods are practical threats to Messerges ' s countermeasure by mathematical proof and simulation results.

This paper is organized as follows. In section 2, we introduce the masking type conversion algorithm. Our new first-order DPA and CPA attacks on the masking type conversion algorithm and the simulation results of these are given in section 3. Finally, section 4 is our conclusion.

2 Related work

2.1 The masking type conversion algorithm

Many of the block ciphers such as SEED and IDEA combine Boolean and arithmetic functions, thus a way to convert back and forth between Boolean masking and arithmetic masking is needed. The conversion from one type of masking to another needs to be done in such a way to prevent from the DPA attack. The conversion from Boolean masking to arithmetic masking as described in [8] works as Algorithm 1.

Algorithm 1 BooleanToArithmetic [8]

Input: $x'(= x\ r_x)$, r_x
Output: A(= x — rx)
stepl : randomly select : $C = 0$ *or* $C = —1$
2: $B = Cierx; I*B = rx$ *or* $B = f^{-}{}_{x}*1$
3: $A = Belx'; 1*A = x$ *or* $A = *1$
4: $A = A—B; I*A = x—r_x$ *or* $A = -7.^{-}{}_{x}*1$
5: $A = A + C; I\ *A = x—r_s$ *or* $A = -77_{x}-1*1$
6: A=AEDC;/*A=x¬rx*/ 7 :
Return A;

The previous algorithm takes as input a tuple (x', r) such that $x = .x^{1}C)\ r$. The unmasked data is x and the masked data is x' . The algorithm works by unmasking x' with XOR operation and then remasking it with addition operation. The conversion from the arithmetic masking to Boolean masking can be done with a similar way as Algorithm 2.

The issue is that the variable x or X is computed during the execution of the algorithm. Depending on the random value C, x or x is exposed with equal probability where x is the one's complement of x . Therefore a single-bit DPA attack cannot break Algorithm 1.

Algorithm 2 ArithmeticToBoolean [8]

Input: A(= x — r_x), rx
Output: A(= $x@r_x$)
stepl : randomly select : $C = 0$ *or* $C = —1$
2 : $B=CEBr_x; I*B=r_x$ *or* $B=r^{-}{}_x*I$
3 : $A = A @ C ; I * A = x — r_x$ *or* $A = -1 * 1$
4 : A = $A—C; I*A=x—r_x$ *or* $A=x—r_x$ */
5 : $A=A+B; I*A=x$ *or* $A=^{-}\pm\cdot*I$
6: A=AEBB;/*A=x@rx*/ 7 :
Return A;

3 New power analysis attack

In this section, we introduce two new power analysis attacks on the masking type conversion algorithm. We also show that this attack really works successfully by a simple mathematical approach and the simulation result.

3.1 Weight squaring CPA attack

The new CPA attack applies the trace squaring map and the weight squaring map below. Weight squaring map gives a strong relation. We consider the power consumption model given by Messerges. Messerges's power consumption model is as follows;

$$C = offset + eHW(x) + N$$

Here, the power consumption at time when x is processing is represented by C, *offset* represents the additive constant portion of the total power, e represents the incremental amount of power for each extra 1 in the Hamming weight, $HW(x)$ represents the Hamming weight of the guessed value x and N represents the Gaussian noise.

Denition 3. A function 0, maps a set A to the set of all rational numbers Q is the trace squaring map if $0_{7,}(a)_{\cdot}\ a^2$ where a E A.

Denition 4. A function O_w maps a set B to the set of all rational numbers Q is the weight squaring map if $O_w\ (13) = (8^2 + (v — fi)^2)/ 2$ where $_{l}$a e B.

The v -bit (2 5 v 8) weight squaring CPA attack process is as follows;

1. We use $2n$ plaintexts and let the set of power samples of the guessed value x be X' then the trace squaring map over X' is as bellow.

$$OT(X) = \{(offset + et_i + N_i)^2 \; lt_i = HW(x_j)(1in'')\},$$
$$t = 8 — HW(x_i)\,(n''+ 1\; i\; 2n)\}\,.$$

Here, $n''1\,2n$ •-=-*1* 0.5 .

2. Let the Hamming weight of the i-th guessed value x_i be Iv, and calculate the range of the weight squaring map o_w of W . For example, the range of the weight squaring map o_w of W for 8-bit attack is represented in Table 1.
3. Calculate the correlation coefficient $p_{T,w}$ between $0_{7,}(X')$ and $O_w(W)$.
4. Choose the corresponding key which has the biggest correlation coefficient.

Theorem 1. The correlation coefficient between 0_7,(X and $O_w(W)$ converges to where

$$v = 2\,.$$
$$\overline{2'2(offset + 6)^2 + 0.256^2}$$

Proof Its detailed description is given at http://youngincho.com/cnsi_appendix.

Table 1. The range of the weight squaring map o_w of W where v = 8 .

W	Ow(w1)
0,8	32
1 7	25
2 6	20
3 5	17
4	16

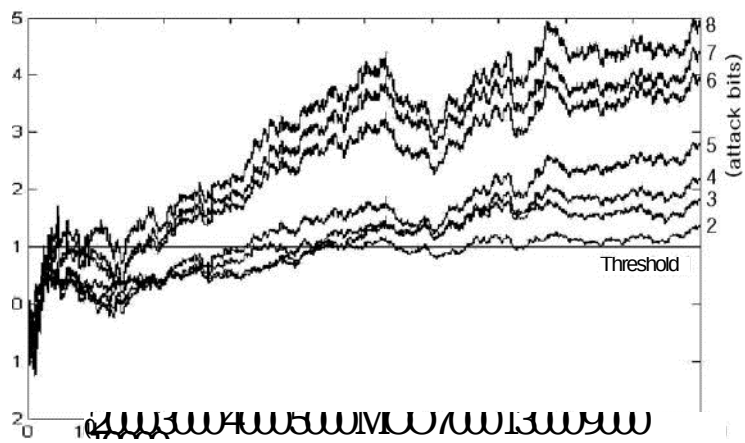

Fig. 1. The simulation result of the weight squaring CPA attack on the masking type conversion algorithm.

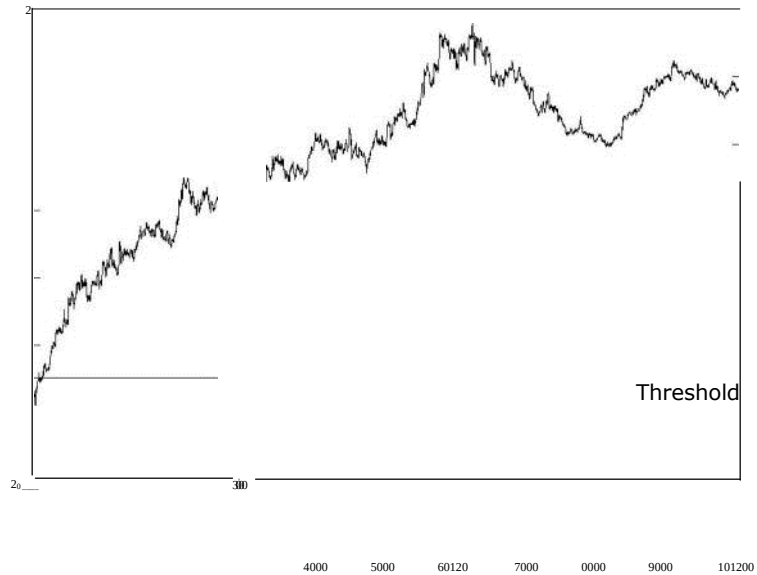

Fig. 2. The simulation result of the extended CPA attack on the masking type conversion algorithm.

Theorem 3 states that the weight squaring CPA attack works successfully since the correlation coefficient *C'* corresponding to the correct key is positive. In other words, the proper key hypothesis would have a visible peak for the power analysis trace. Let C'_w be the biggest one among the differences *C'* for all wrong key guesses and be the correlation coefficient for the correct key guess. The simulation result in Figure 2 presents *C'* / C'_w w of the new v -bit CPA attack. The value of CyC'_w of the new v -bit CPA attack is bigger than 1. Moreover, when v becomes bigger, the value of $c_{aw}^{'}$ also becomes bigger.

Corollary 1. The correlation coefficient has the maximum value when *offset* = —*s* .

Corollary **1** is trivial by Theorem 3. Corollary 1 states that adjusting offset help us to find a visible peak for the power analysis trace more clearly. In our case, subtracting the average power consumption *offset* + *s* from power samples would be helpful to analyze.

4 Conclusion

We provided theoretical analysis about the security of Messerges's algorithm with Messerges's power consumption model and introduced a new adversary model. The new adversary model which is able to make a relation between the guessed value and the recorded power consumption. To generate this relation, we proposed two kinds of maps. Moreover, we gave the mathematical proof and the simulation results to

confirm our analysis. Also we presented a new direction for the power analysis attack on the masking type conversion algorithm.

Acknowledgments. This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2011-0004395)

References

1. Blomer, J., Guajardo, J., Krummel, V.: Provably Secure Masking of AES, SAC 2004, LNCS 3357, pp.69-83(2004)
2. Brier, E., Clavier, C., Olivier, F.: Correlation Power Analysis with a Leakage Model, CHES 2004, LNCS 3156, pp.16-29(2004)
3. Oswald, E., Mangard, S., Pramstaller, N., Rijmen, V.: A Side-Channel Analysis Resistant Description of the AES S-box, FSE 2005, LNCS 3557, pp.413-423(2005)
4. Oswald, E., Schramm, K • An Efficient Masking Scheme for AES Software Implementations WISA 2005, LNCS 3786, pp. 292-305(2005)
5. Kocher, P., Jaffe, J., Jun, B.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Others Systems, CRYPTO 1996, LNCS1109, pp.104-113(1996)
6. Kocher, P., Jaffe, J., Jun, B.: Introduction to differential power analysis and related attacks http://www.cryptography .com/dpa/technical(1998)
7. Messerges, T., Dabbish, E., Sloan R.: Power analysis attacks on modular exponentiation in Smart cards Workshop on CHES 1999, pp.144-157(1999)
8. Messerges, T.: Securing the AES Finalists Against Power Analysis Attacks FSE 2000, pp. 150-164(2000)