A Novel SPA Attack on ECC Using MMM's Conditional Subtraction

Lihui Wang, Qing Li, Zhimin Zhang, Weijun Shan
Central Research Institute
Shanghai Fudan Microelectronics Group Company Limited
Shanghai, 200433, China
E-mail: wanglihui@fmsh.com.cn

David Wei Zhang
School of Microelectronics, Fudan University
Collaborative Innovation Center of IC Design & manufacturing in Yangtze River Delta (2011)
Shanghai, 200433, China
E-mail: dwzhang@fudan.edu.cn

***Abstract*—Elliptic curve cryptosystems (ECCs) are becoming more popular because of the reduced number of key bits required in comparison to other cryptosystems such as RSA. They are especially suited to smartcards because of the limited memory and computational power available on these devices. However, the side-channel attacks especially simple side-channel analysis (SPA) can obtain information about the cryptosystem by measuring power consumption and processing time. To resist this attack there appear a number of countermeasures and the most widely used methods are Montgomery ladder and double-and-add-always algorithm. This paper proposes a novel simple power analysis attack to these countermeasures. Experimental results on smart cards demonstrate that this attack method can retrieve secret keys by distinguishing the conditional subtraction of Montgomery modular multiplication (MMM). Several countermeasures that can resist this kind of SPA attack are also demonstrated in this paper.**

Keywords—ECC; cryptography; SPA; Montgomery modular multiplication

I. INTRODUCTION

Elliptic curve cryptosystems become more and more popular. With much shorter key lengths they (presumably) offer the same level of security than older cryptosystems. This advantage is especially attractive for small cryptographic devices, like the smart cards.

However, a new class of attacks was exploited to retrieve some secret information embedded in a cryptographic device: the so-called side-channel attacks [1, 2]. By monitoring some side-channel information (e.g., the power consumption) it is possible, in some cases, to deduce the inner workings of an (unprotected) crypto-algorithm and thereby to recover the secret keys. To counteract these attacks, a variety of countermeasures have been proposed [2, 3, 4, 5, 6, 7, 8, 9].

This paper only deals with simple side-channel analysis (SPA) because it is made easier for elliptic curve algorithms because the operations of doubling and addition of points are intrinsically different. There are a number of countermeasures for ECC against SPA attacks, and the most widely used as so far are Montgomery method [10] of the point multiplication and double-and-add-always algorithm [11]. They are all regular point multiplication algorithm that the operations of point doubling and addition are always executed whatever the key bit is. However, the above countermeasures can't ensure the absolute security of point multiplication when there is more powerful simple power analysis. The main contribution of this paper is the development of a novel and more powerful simple power analysis attack.

Here, to make the details concrete and quantifiable, this is considered for a specific choice of the algorithms and form of side channel leakage, namely point multiplication using the standard double-and-add-always algorithm, together with field multiplication using a version of Montgomery modular multiplication (MMM) [12] which includes a conditional subtraction and a cryptographic device in which every such subtraction can be observed on some side channel or combination of side channels. It is shown that this association leaks sufficiently for it to be computationally possible to deduce private keys for standard elliptic curves even if they are used just once.

The rest of this paper is organized as follows. Section II introduces the background theory regarding the ECC's point multiplication algorithm, Montgomery Modular Multiplication algorithm and SPA attack. Section III presents a novel SPA attack on ECC with countermeasures. Attack results are given in Section IV. Finally, we conclude in Section V.

II. BACKGROUND

The following section will briefly cover the background theory, required for understanding this work. First, we give an overview of ECC algorithm and Montgomery multiplication followed by a brief introduction to side channel analysis.

A. Elliptic curve scalar multiplication

An elliptic curve is a set of points P which are solutions of a bivariate cubic equation over a finite field, such as the prime finite field and the binary finite field [13].

In ECC, the secret key d is mainly involved in the scalar multiplication operations, while scalar multiplication is realized by repeated addition of the same point. If d is a positive integer and P a point on an elliptic curve, the point multiplication dP is the result of adding d copies of P [14, 15]:

$$dP = \underbrace{P + P + \ldots + P}_{d}$$

There is a common implementation of ECC's scalar multiplication, such as the Binary Method shown in Algorithm 1:

Algorithm 1 (Binary algorithm)
Input: d, P
Output: dP
1. $T_0 = P$
2. for $i = n - 2$ to 0
    $T_0 = 2T_0$
    if $d_i = 1$ then $T_0 = T_0 + P$
3. output T_0

The above point multiplication implementations contain point addition and point doubling. The key d determines the procedure of doubling and addition operation. It consists of a point doubling operation if the key bit is 0, and a point doubling followed by a point addition operation if the key bit is 1.

B. Montgomery modular multiplication

Suppose the elliptic curve is defined over the Galois field $GF(P)$ and elements of this prime field are represented as long integers modulo P written to base r with digits in lowercase. Suppose $R(\geq P)$ is the upper bound we wish to have on the inputs and outputs for MMM. Then we assume the version of MMM given in Algorithm 2 [12].

Algorithm 2 (MMM algorithm)
Input:A and B such that $A, B < R \leq r^n$ and P prime to r
Output: C such that $C = ABr^{-n} mod\ P$ and $C < R$
1. $C \leftarrow 0$
2. for $i = 0$ to *n-1*
    $q_i \leftarrow -(c_0 + a_i b_0) p_0^{-1} mod\ r$
    $C \leftarrow (C + a_i B + q_i P)\ div\ r$
3. if $C \geq R$ then $C \leftarrow C - P$
4. output C

Note that there is a conditional subtraction at the end of MMM algorithm. We can obtain the probability of conditional subtraction in modular squaring and multiplying in [18].

In the case of squaring X, the probability is $p_s = prob(X^2 r^{-n} + Z > P)$ where Z is uniform on [0, P]. Hence:

$$p_s = \int_0^P P^{-1} f(x) x^2 r^{-n} dx = \frac{1}{3} P r^{-n}$$

In the case of multiplying two independent, random residues X and Y, the probability of the conditional subtraction is $p_M = prob(XYr^{-n} + Z > P)$ for equi-distributed Z, namely:

$$p_M = \int_0^P \int_0^P P^{-1} f(x) f(y) xy r^{-n} dx dy = \frac{1}{4} P r^{-n}$$

In general, $P \approx r^{-n}$, so $p_s \approx 1/3$ and $p_M \approx 1/4$.

C. Power analysis

Power analysis attacks use the fact that the instantaneous power consumption of a hardware device is related to the instantaneous computed instructions and the manipulated data. There are two types of power analysis, the simple power analysis (SPA) and the differential power analysis (DPA), which are described in [2, 16]. DPA computes hypotheses of the power consumption for each input and key candidate and compares them to the recorded power consumption of the device. Such a hypothesis can be computed by calculating the Hamming weight (HW) of a processed value.

In this paper, we only take care of the SPA on point multiplication. SPA makes use of such an instruction performed during a scalar multiplication algorithm that depends on the data being processed. Apparently, Algorithm 1 has a branch instruction conditioned by a secret exponent d, and thus it reveals the secret d if power consumptions of point addition and point doubling are distinguishable.

The point doubling and addition can be implemented as the traditional procedure in [14]. When a=p-3 and Z=1, point doubling needs 8 multiplications, but point addition needs 11 multiplications. And the operation procedure of point doubling is fully different from that of point addition. Therefore their power consumptions are highly distinguishable and vulnerable to SPA.

D. Countermeasures

In order to be resistant against SPA, any branch instruction of exponentiation algorithm should be eliminated. There are mainly two types of countermeasures at algorithm level: the fixed procedure method and the indistinguishable method. The fixed procedure method deletes any branch instruction conditioned by a secret exponent like double-and-add-always method, Montgomery-ladder method, and window-based method [17]. The indistinguishable method conceals all branch instructions of exponentiation algorithm by using indistinguishable addition and doubling operations, in which dummy operations are inserted.

The most widely used method to resist SPA attack are double-and-add-always method and Montgomery-ladder method. Double-and-add-always method is described in Algorithm 3. In this method, the operations of point doubling and addition are always executed whatever the key bit is through insertion of false point additions. By measuring the power consumption during the ECC operation, the attackers can't retrieve the secret key.

Algorithm 3 (Double-and-add-always algorithm)
Input: d, P
Output: dP
1. $T_0 = P$
2. for $i = n - 2$ to 0
    $T_0 = 2T_0$
    if $d_i = 1$ then $T_0 = T_0 + P$
    else $T_1 = T_0 + P$
3. output T_0

III. A NOVEL SIMPLE POWER ANALYSIS

In this section, we present a powerful simple power analysis attack on point multiplication with double-and-add-always method. Note that this attack can also be used to defeat the Montgomery-ladder method.

A. Description of the Attack

For simplicity, we assume the main side channel leakage is from an implementation of field multiplication using

Montgomery Modular Multiplication (MMM) in which there is an observable, final, conditional subtraction. However, it must be emphasized that this choice is only for convenience in evaluating the probabilities. A similar attack could be mounted against any modular multiplier exhibiting data-dependent side-channel leakage.

According to algorithm 2, there is a conditional subtraction decided by the two multipliers of the modular multiplication. This means that the conditional subtraction of a modular multiplication in the point multiplication is decided by the input point and the bits of private key used before computing this modular multiplication, when the point multiplication algorithm is fixed.

The attack of this paper is based on above principle. By knowing the input point of the point multiplication and guessing the partial private key, the attacker can deduce the conditional subtractions of the medial Montgomery modular multiplications. If the deduction correspond to actual situation by analyzing the power consumption of point multiplication, the guessing key is right, otherwise is wrong. Now we give a concrete process of this attack when the target is point multiplication using the standard double-and-add-always algorithm.

Assuming that the attacker knows the $i-1$ most significant bits, he can guess $d_i = 0$ and compute the output of i round that equals the input of $i+1$ round. In general, the coordinate system is Jacobian and coefficient of the elliptic curve equation is $a = -3$, so there are 19 modular multiplications in every round. By knowing the input of $i+1$ round, the positions of conditional subtractions of these 19 modular multiplications can be confirmed. Contrast to the power consumption of $i+1$ round, if the positions of conditional subtractions are identical, the guess $d_i = 0$ is right, otherwise $d_i = 1$. We can repeat this attack until the last round in which the key bit can be retrieved only by exhausting method.

The preconditions for success of this attack is that the positions of conditional subtractions of these 19 modular multiplications is different more or less when $d_i = 0$ or $d_i = 1$. According Section II the probability that two squares' (two multiplies' respectively) the conditional subtraction are the same is ${p_s}^2 + (1-p_s)^2 = 5/9$ (${p_M}^2 + (1-p_M)^2 = 5/8$ respectively). Then we can deduce that the probability that all the conditional subtraction positions of 19 modular multiplications are the same is $(5/9)^7 \times (5/8)^{12} \approx 2^{-14}$, because there are 7 squares and 12 multiplies. This probability can be ignored and almost only one input point and corresponding power trace need to recover the whole key.

If the Montgomery-ladder method also uses the Montgomery modular multiplications, it can be broken in the same way.

Note that this attack can also be applied to ECDSA. Despite only the ephemeral key can be retrieved from the scalar multiplication by above attack method, we can recover the sign key easily.

B. *Countermeasures*

Because only one power trace of scalar multiplication is need in above attack method and the target is only the exponent key, the common countermeasures like exponent blinding is not useful.

It is clear that constant time modular multiplication is essential for security and the attacker need to know the input point in this attack, so the countermeasures such as base point blinding, random projective coordinate [11] and eliminating the conditional subtraction are all good choices.

IV. EXPERIMENT RESULT

To examine the effect of the proposed SPA attack in section III, the experiments are conducted on a hardware implementation of ECC. The experimental setup consists of a PC, a power tracer, a smart card and a LeCroy oscilloscope. The smart card has a PAE coprocessor and algorithm library. The coprocessor is used to compute modular multiplication and addition. The algorithm library is used to provide a high level interface to ECC cryptography implemented on the coprocessor and includes countermeasures against SPA and DPA attacks.

In practice, the crucial demand of this attack method is that the judges of conditional subtraction in power trace are accurate. There are many methods to discriminate modular multiplications with or without conditional subtraction such as measuring the timing of multiplications, pattern matching. The latter is chosen because it is more stable. Specific steps are as follows:

First, acquiring a power trace of point multiplication and finding a modular multiplication with conditional subtraction in it as a pattern. Then the correlation coefficient between this pattern and the every successive region of the power trace point by point is computed and all regions whose correlation coefficients are higher than an appropriate threshold such as 0.9 are averaged into a new pattern. The new pattern selected in this experiment is as shown in Fig.1.

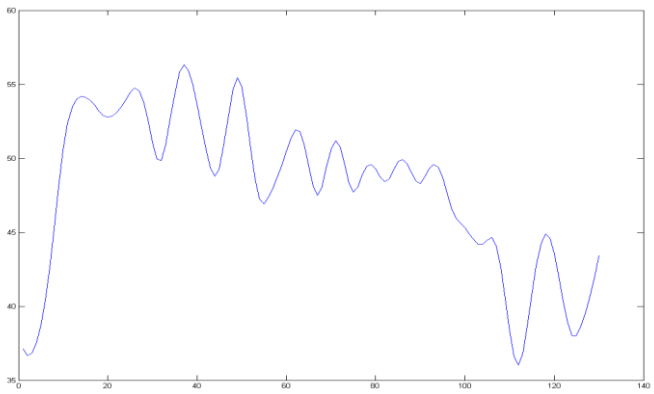

Fig. 1. The new pattern of MMM with conditional subtraction

Secondly, the correlation coefficient between new pattern and the every successive region of the power trace point by point is recomputed and the partial result is as shown in Fig.2.

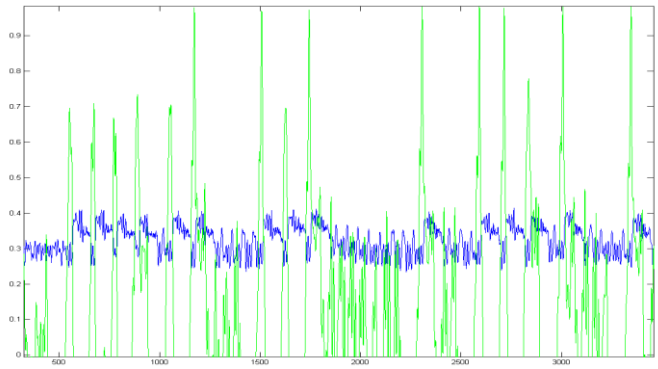

Fig. 2. The correlation coefficient between new pattern and the every successive region of the power trace point by point

From Fig.2 it can be seen that the correlation coefficients can be divided into two groups. The first group is higher than 0.9 and the second is between 0.6 and 0.9. It means that the first group is matched with the pattern well and they are all modular multiplications with conditional subtraction. Obviously, the modular multiplications in second group have no conditional subtraction.

After that the above judge and attack methods are made into program and applied on a standard scalar multiplication using double-and-add-always algorithm. The experimental results show that it is easy to recover the whole secret key less than several seconds.

V. CONCLUSION

A novel simple power analysis attack on elliptic curve scalar multiplication such as double-and-add-always algorithm is presented in this paper. The method basically uses the information about the conditional subtraction of Montgomery modular multiplications, and retrieves the secret key by measuring the power consumption of point multiplication. The method can be considered as an enhancement because it works even in cases where the standard simple power attack fails because of the countermeasures such as the double-and-add-always algorithm.

The experimental results overturn several potential misconceptions. First, the regular point multiplications such as Montgomery ladder and double-and-add-always algorithm are not panaceas against simple power analysis. It protects only one aspect of the implementation. Secondly, the standard exponent blinding technique can provide no protection at all against some attacks. And thirdly, modular multiplication can leak sufficient data for a successful attack even when a key is used just once, such as in the Digital Signature Algorithm (DSA).

To summarize the results, the method is new and more powerful than the standard simple power analysis attack and poses a serious threat against certain algorithms. More countermeasures should be chosen to prevent this attack. The work done in this paper is just a try to breaking the ECC's private key using a simple power analysis, more novel method and further researches are expected in the future.

Acknowledgment

This work is supported by "China's 12th Five-Year Plan" Microelectronics Advance Research Projects Fund (No. 51308010609) and Shanghai Science and Technology Talents Funds (No. 14R21421100).

References

[1] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, editor, Advances in Cryptology – CRYPTO'96, pages 104 – 113. Springer-Verlag, 1996.

[2] P. Kocher, J. Jaffe, and B. Jun. "Differential power analysis," Proceedings of CRYPTO'99, Springer-Verlag, Berlin, pp. 388–397, 1999.

[3] J.-S. Coron. Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, CHES 99, LNCS 1717, Springer-Verlag, 1999, pp. 292 – 302.

[4] J. Lopez and R. Dahab. Fast multiplication on elliptic curves over GF(2m) without precomputation. In C, .K. Ko, c and C. Paar, editors, CHES 99, volume 1717 of Lecture Notes in Computer Science, pages 316 – 327. Springer-Verlag, 1999.

[5] K. Okeya and K. Sakurai. Power analysis breaks elliptic curve cryptosystems even secure against the timing attack. In B. Roy and E. Okamoto, editors, Progress in Cryptology – INDOCRYPT2000, volume 1977 of LNCS, pages 178 – 190. Springer-Verlag, 2000.

[6] M. Joye and J.-J. Quisquater. Hessian elliptic curves and sidechannel attacks. In C, .K. Ko, c, D. Naccache, and C. Paar, editors, CHES 2001, volume 2162 of LNCS, pages 412 – 420. Springer-Verlag, 2001.

[7] P.-Y. Liardet and N. P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In C, .K. Ko, c, D. Naccache, and C. Paar, editors, CHES 2001, volume 2162 of Lecture Notes in Computer Science, pages 401 – 411. Springer-Verlag, 2001.

[8] M. Joye and C. Tymen. Protections against differential analysis for elliptic curve cryptography: an algebraic approach. In C, .K. Ko, c, D. Naccache, and C. Paar, editors, CHES 2001, volume 2162 of LNCS, pages 386 – 400. Springer-Verlag, 2001.

[9] B. Moller. Securing elliptic curve point multiplication against sidechannel attacks. In G.I. Davida and Y. Frankel, editors, Information Security, volume 2200 of LNCS, pages 324 – 334. Springer-Verlag, 2001.

[10] P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods for Factorizations," Mathematics of Computation, vol. 48, pp. 243-264, 1987.

[11] J. S. Coron. Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, CHES 99, LNCS1717, (1999), 292-302

[12] P. L. Montgomery, Modular Multiplication without Trial Division, Mathematics of Computation 44, no. 170, 1985, pp. 519 – 521.

[13] A. J. Menezes, "Elliptic Curve Public Key Cryptosystems," Kluwer Academic Publishers, Norwell, 1993.

[14] IEEE Std-1363-2000: Standard Specifications for Public Key Cryptography, January 2000.

[15] X. F. Tang, "The VLSI Implementation of ElliPtie Curve Cryptography IP," Master Thesis, Circuits and Systems of Department of Electric Engineering of Zhejiang University, China, February 2004

[16] C. Kocher, "Timing attacks on Implementations of Diffie-Hellman, RSA, DSS, and other system", CRYPTO' 96, Lecture Notes in Computer Science, 1109(1996), Springer-Verlag, 104 – 113

[17] K. Koyama and Y. Tsuruoka, "Speeding up elliptic cryptosystems by using a signed binary window method", Advances in Cryptology-Proceedings of Crypto'92, Lecture Notes in Computer Science, 740 (1993), Springer-Verlag, 345 – 357.

[18] C. D. Walter. Simple Power Analysis of Unified Code for ECC Double and Add. CHES 2004. M. Joye and J.-J. Quisquater, Springer Berlin / Heidelberg. 3156: 86-115.