A Study on Side Channel Cryptanalysis in Elliptic Curve Cryptosystems

Katsuyuki Okeya

Abstract

Mobile devices such as smartcards are penetrating in our daily life in order for us to be comfortable. When cryptographic schemes are implemented on computers such as smartcards, side channel attacks are particular menaces to them. Since electric power is provided from the outside of them, the attacker can observe the power consumption while they perform cryptographic operations. In side channel attacks, the attacker utilizes the power consumption for revealing the secret, since the power consumption is usually linked to the operations associated with the secret key.

The aim of this thesis is to construct efficient countermeasures against side channel attacks. For this purpose, we first attempt to attack the known countermeasures, and study the essence of side channel attacks. Then, we utilizes the essence for constructing efficient countermeasures which are suitable for the mobile devices.

There are two approaches to resist against side channel attacks; physical and algorithmic approaches. While the physical approach increases the cost of IC chip, the algorithmic approach does not reduce the performances. Since the mobile devices such as smartcards are inexpensive, the cost is critical. Thus, to construct algorithmic countermeasures is important.

Prior to communication among the mobile devices, they authenticate reciprocally. In order to authenticate, public key cryptosystems are required. Besides, the mobile devices has scarce computational environments only, so that we have to make an effort to optimize the memory and efficiency of the cryptosystem. Elliptic curve cryptosystem (ECC) is a public key cryptosystem and suitable for the purpose because of its short key size. The known approaches to ECC proved the mathematical security of ECC, and attempted to perform more efficiently. However, the appearance of side channel attacks has forced us to enhance such computation algorithms to be secure against side channel attacks. As a result, many countermeasures against side channel attacks have been proposed. However, some of them have not been proved their immunity against side channel attacks.

First, we propose two novel attacks against known countermeasures. One is a side channel attack against Oswald's countermeasure, and the other is a second-order differential power analysis against Möller's countermeasure. Oswald proposed a randomized addition-subtraction chains countermeasure, which utilizes a signed digit representation of an integer together with randomization

concept of procedures. In order to show the vulnerability of this type of countermeasures, we construct an attack against Oswald's countermeasure. We assume that the attacker can distinguish elliptic addition and elliptic doubling using a single observation of power consumption. Then the attacker can construct a sequence that consists of elliptic addition and elliptic doubling. We show that the attacker can recover the secret using plural such sequences. Thus Oswald's countermeasure or some such countermeasures are vulnerable to the proposed attack.

Second, we show the vulnerability of countermeasures with pre-computation table. Möller proposed a countermeasure using the window method, which utilizes a pre-computation table for accelerating the computation. The countermeasure performs the fixed procedure independent from the secret, and does not use dummy operations. In order to accelerate the countermeasure, a pre-computed table is utilized. We point out that a second-order differential power analysis can distinguish whether two accesses to the pre-computed table use the same entry or not. Since the table access is linked to the secret, the attacker can reveal the secret. Thus Möller's countermeasure is vulnerable to the proposed attack. Note that we need to take measure against the proposed attack if a pre-computed table is utilized for speeding up.

Finally, we propose two novel countermeasures against side channel attacks. One is a countermeasure using the Montgomery form of elliptic curves, and the other is a countermeasure using the width-w non-adjacent form. Montgomery proposed the Montgomery form of elliptic curves in order to accelerate the elliptic scalar multiplication. We propose an appropriation of the scalar multiplication method on the Montgomery form for preventing against side channel attacks. Because the method performs one elliptic addition and one elliptic doubling per a single bit of the secret, which thwarts side channel attacks. A drawback of the use of Montgomery-form elliptic curves is that the y-coordinate of the scalar multiplied point is not obtained. In order to overcome this problem, we propose a y-coordinate recovery method. Another problem is that if we utilize randomized projective coordinates for enhancing the immunity of the countermeasure, randomized projective coordinates increases the computational cost of the countermeasure. In order to overcome this problem, we propose a method in which the same elliptic point is used in two ways; randomized and un-randomized representations. The method provides the countermeasure with high security and high speed. On the other hand, from the mathematical point of view, some special elliptic curves do not provide the expected security. For this reason, we discuss the specialty of the Montgomery-form elliptic curves, and conclude that they are not so special that they cannot keep the expected security. In fact, we show that the Montgomery form is as secure as the Weierstrass form, which is a usual form of elliptic curves. Therefore, the countermeasure using the Montgomery-form elliptic curve is suitable for the mobile devices.

The width-w non-adjacent form is an accelerated scalar multiplication method. It utilizes a pre-computed table with 2^{w-2} entries, which is quite small compared with other scalar multiplication methods with pre-computed table. We convert the width-w non-adjacent form to a countermeasure against side

channel attacks. Indeed we generate a scalar sequence with the fixed pattern, e.g. $|0..0x|0..0x|...|0..0x|$, where x is positive odd integers with $x < 2^w$. Thus the size of the table is 2^{w-1}, which is optimal in the countermeasures with pre-computed tables. In order to resist against the second-order differential power analysis, the countermeasure should be used together with the randomization renewal method. Since the proposed countermeasure provides small memory and good efficiency, it is suitable for the mobile devices.