The Improved Montgomery Scalar Multiplication Algorithm with DPA Resistance

Yanqi Xu, Lin Chen, Moran Li

Information Science and Technology Institute,

Zhengzhou, 45000, China

e-mail: xyq_1@163.com

Keywords: ECC, DPA, Montgomery scalar multiplication algorithm, security system

Abstract. With Montgomery scalar multiplication algorithm being widely used in elliptic curve cryptography systems, the researches on DPA attacks against Montgomery scalar multiplication algorithm become more extensive, but few researches are about the DPA resistance algorithm. This paper analyzed the DPA resistance capability of the Montgomery scalar multiplication algorithm firstly, and on this basis, proposed an improved algorithm with random Z coordinate to resist the DPA attacks with the characteristics that the parameter Z only participates in the intermediate operations without affecting the final results. This paper described the original algorithm and the improved algorithm using Verilog HDL targeting on the 65 nm standard cell library. Results show that the improved Montgomery Scalar Multiplication algorithm can dramatically improve the anti-DPA attack property with only 0.36% performance and area 9.60% area penalty.

Introduction

Elliptic Curve Cryptography (ECC)[1] is superior to other public key cryptographies such as RSA in high bit strength, excellent calculation speed, and small storage space. Encryption, decryption, signing, verification and other algorithms are all based on the scalar multiplication of points on the elliptic curve[2], so the calculation speed and the ability of attack resistance of the scalar multiplication will determine the calculation capability and safety of the whole curve cryptosystem.

The technology of Side Channel Attacks posed a huge threat to the crypto chip because of its simple attack equipment and measure. Power Analysis Attacks[3] is a common technology of Side Channel Attacks, including Simple Power Analysis (SPA) and Differential Power Analysis (DPA). The design and implementation of scalar multiplication algorithm should also consider to the threat of SPA and the DPA attacks to improve the security of the algorithm.

Reference[4] proved that Montgomery Ladder Scalar Multiplication Algorithm can’t resist the DPA attacks. Reference [5] gave a way to resist the DPA by introducing random redundant operation for decreasing S/N, but this method largely increased the circuit area and power consumption. This paper proposed an improved algorithm of random Z coordinate to resist the DPA attacks combining the random thought with the Montgomery Scalar Multiplication Algorithm, and simulated the DPA resistance capability of the improved algorithm.

The Security Analysis of the Montgomery Scalar Multiplication Algorithm

The Montgomery scalar multiplication algorithm[6] is widely used in engineering field because of its high calculation speed and small storage space. This scalar multiplication algorithm is described based on projection coordinate. The algorithm is showed in Algorithm 1.

Algorithm 1: Montgomery Scalar Multiplication

```
Input: $k = (k_{t-1}, \cdots, k_1, k_0)_2$, $k_{t-1}=1$, $P = (x, y) \in E(\mathbb{F}_{2^m})$.
Output: $kP$.

1. $X_1 \leftarrow x, Z_1 \leftarrow 1, X_2 \leftarrow x^4 + b, Z_2 \leftarrow x^2$ 。{ $(P, 2P)$ }
2. For $i$ from $t-2$ to 0, do
    2.1 If $k_i = 1$， then
        $T \leftarrow Z_1, Z_1 \leftarrow (X_1Z_2 + X_2Z_1)^2, X_1 \leftarrow xZ_1 + X_1X_2TZ_2.$
        $T \leftarrow X_2, X_2 \leftarrow X_2^4 + bZ_2^4, Z_2 \leftarrow T^2Z_2^2.$
    2.2 else
        $T \leftarrow Z_2, Z_2 \leftarrow (X_1Z_2 + X_2Z_1)^2, X_2 \leftarrow xZ_2 + X_1X_2TZ_1.$
        $T \leftarrow X_1, X_1 \leftarrow X_1^4 + bZ_1^4, Z_1 \leftarrow T^2Z_1^2.$
3. $x_3 \leftarrow X_1 / Z_1.$
4. $y_3 = (x + X_1/Z_1)[(X_1 + xZ_1)(X_2 + xZ_2)$
        $+ (x^2 + y)(Z_1Z_2)](xZ_1Z_2)^{-1} + y.$
5. Return $(x_3, y_3)$.
```

The SPA and the time attack require that the key has an extraordinary influence on power consumption. The attacker needs to grasp the exhaustive implementation details and then surmise the relative key information related to operation[7], according to the metric power consumption track and the analysis of one moment's arithmetic operations of encryption devices along the time axis. Through the Montgomery scalar multiplication algorithm's second step we can find, either ki = 1or ki = 0, the algorithm will execute the same calculation so we can't surmise the key by directly analyzing the power consumption track. So this algorithm can resist the SPA and the time attack.

The DPA can utilize the data dependence by large amount of energy track to analyze the device's power consumption of the fixed time. Then the attacker obtains the invariants of the calculation process(such as key's information)[7]. So as to analysis conveniently, we use this form which is equal to the second step of Algorithm 1 as follows:

If $k_i = 1$, then $P_1 \leftarrow P_1 + P_2, P_2 \leftarrow 2P_2$.

If $k_i = 0$, then $P_2 \leftarrow P_1 + P_2, P_1 \leftarrow 2P_1$.

Because kt-1 = 1, P1 = P, P2 = 2P, the next, when kt-2 = 0, P1 = 2P, P2 = 3P; when kt-2 = 1, P1 = 3P, P2 = 4P. Thus we can see that the different value of kt-2 can generate different middle consequence, and different middle consequence will generate different power consumption which can be utilized by DPA. Document [4] simulated the DPA attacks against Montgomery scalar multiplication algorithm in the environment of EDA and proved that this algorithm can't resist the DPA attacks.

The Improved Algorithm of Montgomery Scalar Multiplication With DPA Resistance

Montgomery scalar multiplication algorithm can be realized by projection coordinates--turn inversion to multiplication to improve the efficiency of the algorithm. The result of operation is unrelated to the value of Z. Combining with this character, this article added a random number generator in the algorithm's hardware implementation, and the generator can generate a random Z before every dot product, thus the intermediate result introduces a random ingredient because of Z. Power consumption is related to data and in this algorithm even we perform twice identical input operations the power consumption won't be the same, so it can resist the DPA attacks. The improved algorithm of random Z coordinate is as follows:

```
Algorithm 2:The Improved Montgomery Scalar Multiplication
Input: $k=(k_{t-1},\cdots,k_1,k_0)_2$, $k_{t-1}$=1, $P=(x,y)\in E(\mathbb{F}_{2^m})$ . $k$<n
Output: $kP$ .
1.    $X_1 \leftarrow xZ_1, Z_1 \leftarrow random, X_2 \leftarrow X_1^{\,4}+bZ_1^{\,4}, Z_2 \leftarrow X_1^{\,2}Z_1^{\,2}.$
2.    For $i$ from $t-2$ to 0, do
    2.1    If $k_i=1$， then
        $T \leftarrow Z_1, Z_1 \leftarrow (X_1Z_2+X_2Z_1)^2, X_1 \leftarrow xZ_1+X_1X_2TZ_2.$
        $T \leftarrow X_2, X_2 \leftarrow X_2^{\,4}+bZ_2^{\,4}, Z_2 \leftarrow T^2Z_2^{\,2}.$
    2.2 else
        $T \leftarrow Z_2, Z_2 \leftarrow (X_1Z_2+X_2Z_1)^2, X_2 \leftarrow xZ_2+X_1X_2TZ_1.$
        $T \leftarrow X_1, X_1 \leftarrow X_1^{\,4}+bZ_1^{\,4}, Z_1 \leftarrow T^2Z_1^{\,2}.$
3.    $x_3 \leftarrow X_1/Z_1.$
4.    $y_3=(x+X_1/Z_1)[(X_1+xZ_1)(X_2+xZ_2)$
          $+(x^2+y)(Z_1Z_2)](xZ_1Z_2)^{-1}+y.$
5.    Return $(x_3,y_3)$ .
```

We used hardware to realize Algorithm 2 in the domain of GF(2192), and adapt the improved algorithm of Montgomery FIOS which is suitable for hardware to realize the core multiplication unit. We adapt single port writing and dual port reading register file to inject parameter and dispatch the data conveniently. In order not to affect the operational efficiency, the random generator and the arithmetic unit perform in parallel and store the random number for the next round operation.

The hardware architecture of random Z coordinate improved algorithm is as follows:

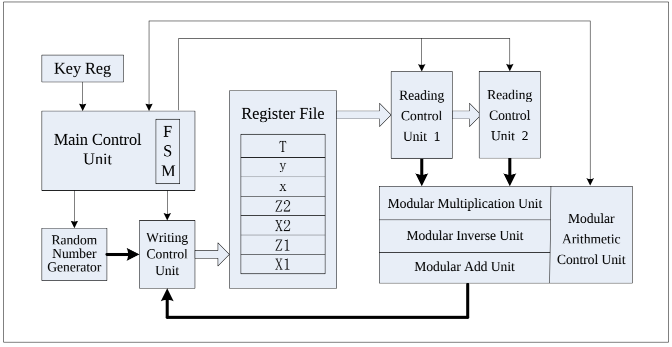


Fig. 1. The hardware of random Z coordinate improved algorithm.

This paper compiled the hardware module in the 0.18um technology by DC and compared with Algorithm One. The result is as follows:

Table I .The Area and Efficiency’s Comparison Between Algorithm 1 and Algorithm 2

	Algorithm 1	**Algorithm 2**	**Comparison**
Gates	85253	93437	Increased by 9.60%
Clock Cycle	97510	101020	Increased by 0.36%

Algorithm 2 adds the random number generator, so the area is increased by 9.60%. Because the random number generating and the mathematical unit don’t affect the efficiency, the algorithm only adds twice modulus square operations and three times modulus multiplication, the efficiency of the algorithm is only decreased by 0.36%.

Test the DPA Resistance Capability of the Improved Algorithm

To test the DPA resistance ability of the improved algorithm, this paper attacked the improved algorithm by DPA attacks in the environment of EDA. Processes are as follows:

1. Build power analysis simulation system. First, we described the 192-bit length algorithm with Verilog HDL, and wrote the testbench, then integrated the hardware description file in the environment of DC tool to generate gate-level netlist file, and then changed the gate-level netlist file

and testbench into vcd file through NC simulation. At last, we analyzed the power consumption of the vcd file with PrimePower and recorded the result.

2. Collect the data. Based on the Power Consumption Data Acquisition System in Step 1, we used fixed key to encrypt the 1000 random points $P_0, P_1, \cdots, P_{999}$ separately and recorded the 1000 groups power consumption data $S_0[j], S_1[j], \cdots, S_{999}[j]$ (j is the sample points).

3. Generate discernibility function. Known $k_{191} = 1$, we could speculate $k_{190} = 1$, and other bits are any value that the speculated key is $k_g = (1, 1, \mathrm{x}, \cdots, \mathrm{x}, \mathrm{x})_2$. Then we used Modelsim to calculate the k_g and the 1000 random points P to get a group of discernibility function values $D_0, D_1, \cdots, D_{999}$.

4. Deal with the data. We used D_i to divide the power consumption curve in Step 2 into two groups according to these standards:

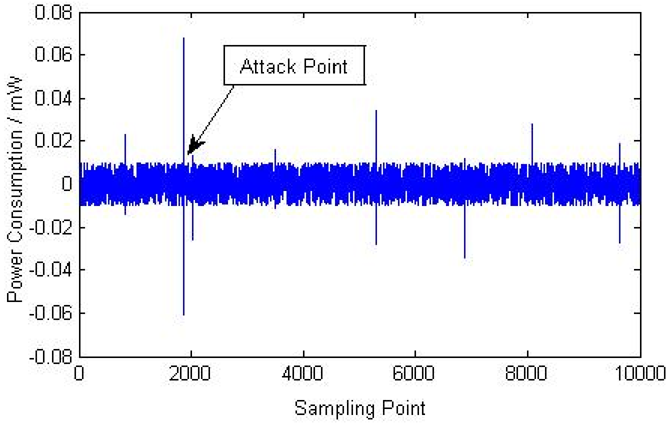
$$S_0 = \{S_i[j] \mid D_i = 0\}$$

$$S_1 = \{S_i[j] \mid D_i = 1\}$$

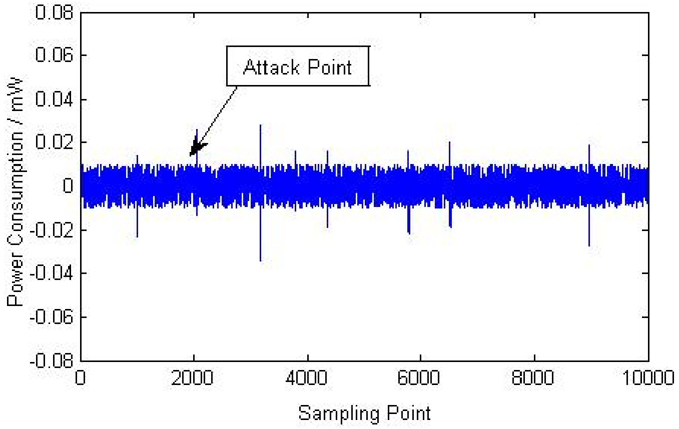
Then we calculated every sample point's average value of two group's power consumption curve and subtract.

$$\begin{aligned}\Delta[j] &= \mathrm{E}(S_1) - \mathrm{E}(S_0)\\ &= \frac{1}{|S_1|}\sum_{S_i \in S_1} S_i[j] - \frac{1}{|S_0|}\sum_{S_i \in S_0} S_i[j]\end{aligned}$$

We can repeat these steps and get the power consumption's difference curves of the original Montgomery scalar multiplication algorithm and the improved algorithm. As shown in Figure 2 and Figure 3.

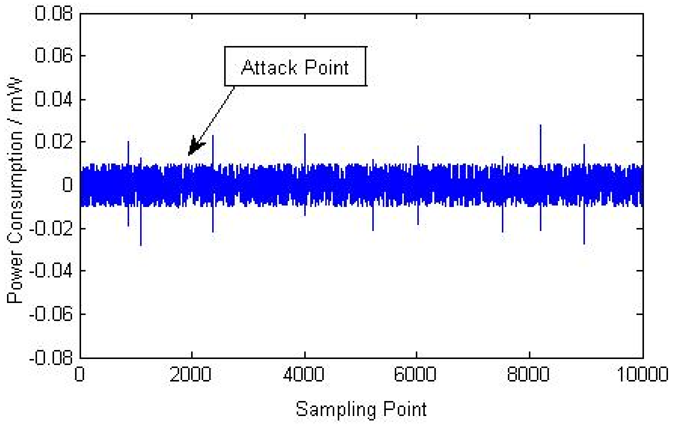


(a) The difference curve of power consumption when guessing the key right.

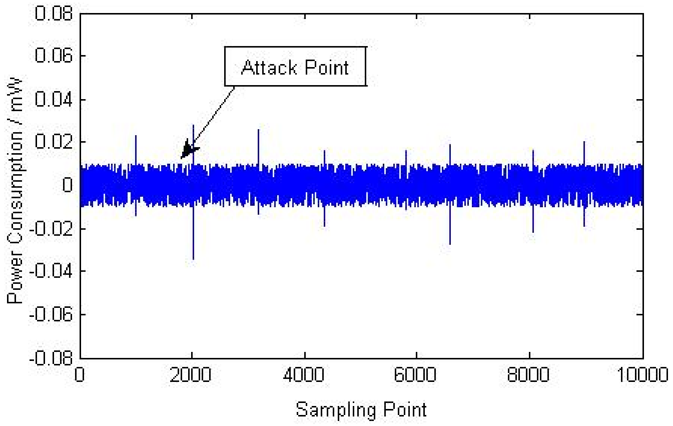


(b) The difference curve of power consumption when guessing the key wrong.

Figure 2 The result of DPA's attack to Montgomery scalar multiplication algorithm



(a) The difference curve of power consumption when guessing the key right.



(b) The difference curve of power consumption when guessing the key wrong.

Figure 3 The DPA attack to the improved algorithm basing on random Z coordinate.

Comparing the figure 2(a) and figure 2(b) we can see that there are apparent peaks when the speculated key is right and there isn't any peak when the speculated key is wrong, so we can conclude that the Montgomery scalar multiplication algorithm can't resist DPA attacks and we can attack the algorithm one bit by one bit for right key according to the above steps.

From the Figure 3 we can see there won't be any peak when the speculated key is right or wrong and we can conclude that the random Z coordinate can change the related features of the key and the power consumption so as to disable statistical means and resist the DPA attacks in the end.

Conclusion

This paper analyzed the safety of the Montgomery scalar multiplication algorithm, proposed an improved algorithm basing on random Z coordinate. Its ability of DPA resistance is verified by EDA simulation tools. Results show that the improved Montgomery Scalar Multiplication algorithm can dramatically improve the anti-DPA attack property. Otherwise, many scalar multiplication algorithms adopt standard projection coordinate, Jacobi projection coordinates and Lopez-Dahab projection coordinates to improve the efficiency. Because all these projection coordinates use the parameter Z only participates in the intermediate operations without affecting the final results, we can transplant the random Z coordinate into other algorithms basing on projection coordinate. Consequently, the improved algorithm has important practical value.

References

[1] Koblitz N. Elliptic curve crytosystems[J]. Mathematics of Computation, vol48, pp. 203-209,1987.

[2] Chung S C, Lee J W, Chang H C, et al. “A high-performance elliptic curve cryptographic processor over GF (p) with SPA resistance”[C]//Circuits and Systems (ISCAS), 2012 IEEE International Symposium on. IEEE,pp.1456-1459,2012.

[3] Kocherp, Jaffe J, Jun B. Differential Power Analysis[C]. Proceedings of Advances in CRYPTO’99, LNCS 1666. Springer-Verlag, Berlin Heidelberg, pp.388-397, 1999.

[4] Deng Qiu Cheng, Bai Xue Fei, Guo Li. Research on Differential Power Analysis Attack on ECC Algorithm[J]. Microelectionics & Computer, vol,28(2),pp 3-5, 2011.

[5] Dan Yong Ping. Chip Implementation and it’s Security Defence for Elliptic Curve Cryptosystems over GF(2m)[D]. Wuhan: Huazhong University of Science and Technology, 2008.

[6] Darrel Hankerson, Alfred Menezes, Scott Vanstone. Guide To Elliptic Curve Cryptography[M]. Zhang Huan Guo, transl. Beijing: Publishing House of Electronics Industry, 2005.

[7] Stefan Mangard, Elisabeth Oswald, Thomas Popp. Power Analysis Attacks. Feng Deng Guo, Zhou Yong Bin, Liu Ji Ye, transl. Beijing:Science Press, 2010.