About the security of pairing based cryptography

Nadia EL MRABET

Université de Caen - GREYC
nadia.el_mrabet@info.unicaen.fr

Abstract. Since 2001, the interest of cryptographers in pairing based cryptography is very high. Pairings allow construction of original protocols and simplification of existing protocols. Several system of coordinates or elliptic curves are used in pairing based cryptography, it seems fair to wonder which system of coordinates and elliptic curves assure the best security.
keyword: pairing based cryptography, side channel attacks, security.

1 Introduction

Pairings are mathematical tools which were introduced in cryptography during the 90'. At the beginning, it was used to build attacks on cryptosystems, transferring the discrete logarithm problem on elliptic curves, to a discrete logarithm problem on finite fields. The first was the MOV [10] attack in 1993.

Since 2001, pairings are used in a constructive way, simplifying existing protocols [8], [3] or creating new ones [2]. One of the most interesting could be the identity based cryptography. In an identity based protocol the public key of a user is his identity and a trusted authority construct the private key related to his identity. When using pairings in identity based cryptography, the problem of side channel attacks must be taken into account. Indeed, there is a secret to protect: the private key of users.

In [12, 14, 6, 5], the authors study security of pairing based cryptography overs Weirstrass elliptic curves. It has been proved that without protection, the pairing based cryptography in Weierstrass coordinates is vulnerable to Differential Power Attack (DPA), Correlation and fault attacks, all of this attacks are side channel attacks.

Recently, the Edwards elliptic curves were used to compute pairings [1]. Edwards curves became interesting for elliptic curve cryptography when it was proved by Bernstein and Lange in that they provide addition and doubling formulas faster than all addition formulas known at that time. The advantage of Edwards coordinates is that the addition law can be complete (i.e. the formulas for adding or doubling two points are the same) and thus the exponentiation in Edwards coordinates is naturally protected against side channel attacks. Unfortunately, pairing in Edwards coordinates are also vulnerable to side channel attacks.

Considering, different system of coordinates, for different elliptic curves there is different countermeasure possibles. We are going to investigate which one is more secure and less expensive to implement. Indeed, a secure algorithm is not interesting if its implementation is too expensive in time and place.

The outline of the article is the following, first we recall what is the pairing based cryptography in Section 2. Then in Section 3 we describe the differentiel power analysis attack in pairing

based cryptography and the possible countermeasure, and in Section 4 toward fault attacks. We conclude in Section 6.

2 pairing based cryptography

2.1 A short introduction to pairings

In this section we give a brief overview of the definitions of pairings on elliptic curves and of Miller's algorithm [11] used in pairing computation. Let q be a prime power not divisible by 2, E an elliptic curve over $\mathbb{F}_q$ and r a prime factor of $\#(E(\mathbb{F}_q))$. Suppose r^2 does not divide $\#(E(\mathbb{F}_q))$ and let k be the *embedding degree* with respect to r, i.e. the smallest integer such that r divides $q^k - 1$. We denote $\mathcal{O}$ the point at infinity of the elliptic curve.

Definition 1. *A pairing is a bilinear and non degenerate function:*

$$\begin{aligned} e : \mathbb{G}_1 \times \mathbb{G}_2 &\to \mathbb{G}_3 \\ (P, Q) &\to e(P, Q) \end{aligned}$$

where $\mathbb{G}_1$ and $\mathbb{G}_2$ are subgroups of order r on the elliptic curve and $\mathbb{G}_3$ is generally μ_r, the subgroup of the r-th roots of unity in $\mathbb{F}_{q^k}$. In general we take $\mathbb{G}_1 = E(\mathbb{F}_q)[r]$ and $\mathbb{G}_2 \subset E(\mathbb{F}_{q^k})[r]$, where we denote by $E(K)[r]$ the subgroup of K-rational points of order r of the elliptic curve E. We also denote $E[r]$ the subgroup of points of order r defined over the algebraic closure of $\mathbb{F}_q$. Let $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$. The goal of Miller's algorithm is to construct a rational function $f_{s,P}$ associated to the point P and to some integer s and to evaluate this function at the point Q (in fact at a divisor associated to this point). The function $f_{s,P}$ is such that the divisor associated to it is:

$$\mathrm{div}(f_{s,P}) = s(P) - (sP) - (s-1)(\mathcal{O}).$$

Suppose that we want to compute the sum of iP and jP. Take h_1 the equation of the line going through iP and jP and h_2 the equation of the vertical line through $(i+j)P$. Miller's idea is to make use of the following relation

$$f_{i+j,P} = f_{i,P} f_{j,P} \frac{h_1}{h_2}, \tag{1}$$

in order to compute $f_{s,P}$ iteratively. Moreover, Miller's algorithm uses the double-and-add method to compute $f_{s,P}$ in $\log_2(s)$ operations [11].

The reduced Tate pairing

In order to illustrate the notion of pairings, we give here the definition of the reduced Tate pairing. The reduced Tate pairing, denoted $\widehat{e}_{Tate}$, is defined by:

$$\begin{aligned} &\mathbb{G}_1 \times \mathbb{G}_2 \mapsto \mathbb{G}_3 \\ &(P, Q) \mapsto \widehat{e}_{Tate}(P, Q) = f_{r,P}(Q)^{\frac{p^k - 1}{r}}. \end{aligned}$$

2.2 pairing based cryptography

The most useful property in pairing based cryptography is bilinearity:

$$\forall (n,m) \in \mathbb{Z}^2,\ e([n]P,[m]Q) = e(P,Q)^{nm}.$$

Pairings permit several protocol simplifications and original scheme creation, for example identity based cryptography protocols. A recent book [9] is dedicated to idendity based cryptography.

The general scheme of an identity based encryption is described in [2].

2.3 side channel attacks in pairing based cryptography

The important point in identity based cryptography is that to decipher a message using an Identity Based Protocol, a computation of a pairing involving the private key and the message is done. Side channel attacks can be therefore applied to find this secret. The particularity of identity based cryptography is that an attacker can know the algorithm used, the number of iterations and the exponent. The secret is only one of the arguments of the pairing.

3 Differential Analysis Family Attack

The aim of this family of attacks is to use the interaction during the execution of an algorithm of the secret and known elements. In the family of differential analysis attack, we include for example the differential power and electromagnetic attacks [4], or the correlation attack [13]. In order to simplify the explanation, we describe the Differential Power Analysis (DPA) Attack.

3.1 Description of Differential Power Analysis Attack

We now introduce some theoretical issues that allow the reader to understand the principle underlying the DPA attack. We consider the output of a gate whose state depends on both the plain text under ciphering (primary inputs) and the secret key. It is called the target node. We consider now a sequence of input patterns $P_0, P_1, \ldots, P_n$ that generate the transitions $T_1(P_0 \rightarrow P_1), T_2(P_1 \rightarrow P_2), \ldots, T_n(P_{n-1} \rightarrow P_n)$ on the circuit primary inputs. A logic simulation of the circuit while monitoring the target node allows classifying these input transitions in two sets, according to a guess on the key:

- P_A, composed by the transitions that make the target node to commute from 0 to 1 and therefore that make the target gate to consume current;
- P_B, composed by the transitions that do not lead the target gate to participate to the power consumed by the circuit (i.e., transitions from 0 to 0, 1 to 1, and 1 to 0 on the target node).

Once we split in two the curves, we compute the average consumption curve in each set P_A and P_B and compute the difference. If any pic of consumption is find then the hypothesis was correct, if not, then it was false.

4 Fault attack Family

4.1 Description of the fault attack

The goal of a fault injection attack is to provoke mistakes during the calculation of an algorithm, for example by modifying the internal memory, in order to reveal sensitive data. This attack needs a very precise positioning and an expensive apparatus to be performed. Nevertheless, current technologies could allow for this attack [7].

We follow the scheme of attack described and completed in [5]. We assume that the pairing is used during an Identity Based Protocol, the secret point is introduced in a smart card or an electronic device and is a parameter of the pairing. In order to find the secret, we modify the number of iterations in the Miller's algorithm by the following way.

First of all, we have to find the flip-flops belonging to the counter of the number of iterations (i.e. $\log_2(s)$) in the Miller's algorithm. This step can be done by using reverse engineering procedures. In classical architecture, the counter is divided into small pieces of 8 bits. To find it, we make one normal execution of the algorithm, without any fault. Then we choose one piece of the counter, and provoke disturbances in order to modify it and consequently the number of iterations of the Miller's algorithm. For example the disturbance can be induced by a laser. Nowadays lasers are thin enough to make this attack realistic [7]. Counting the clock cycles, we are able to know how many iterations the Miller loop has done. Each time, we record the value of the Miller loop and the number of iterations we made. The aim is to obtain a couple $(\tau, \tau+1)$ of two consecutive values, corresponding to τ and $\tau+1$ iterations during the Miller's algorithm.

We denote the two results by $F_{\tau,P}(Q)$ and $F_{\tau+1,P}(Q)$. To conclude the attack, we consider the ratio $\frac{F_{\tau+1,P}(Q)}{F_{\tau,P}(Q)^2}$. By identification in the basis of $\mathbb{F}_{q^k}$, we are lead to a system which can reveal the secret point, which is described in Section **??**.

The probability for obtaining two consecutive numbers is sufficiently large to make the attack possible. In fact, for an 8-bits architecture only 15 tests are needed to obtain a probability larger than one half, $P(15, 2^8) = 0.56$, and only 28 for a probability larger than 0.9.

5 Countermeasure to these attacks

To protect an identity based protocol against side channel attacks, several countermeasure where introduced.

5.1 The third Coron's countermeasure

This countermeasure is efficient only for projective and Jacobien coordinates. It consists in using homogeneity of the coordinates. For exemple, in projective coordinates, a point $P = (X_P, Y_P, Z_P)$ is also the point $(\lambda X_P, \lambda Y_P, \lambda Z_P)$ for λ a non zero integer.

5.2 The bilinearity countermeasure

There are several countermeasure using the bilinearity of pairings. We give here some of them:

- take random $\lambda \neq 0$ and compute $e(\lambda P, \frac{1}{\lambda}Q)$,
- take λ and γ such that $\lambda \times \gamma = 1 \bmod(r)$ and compute $e(\lambda P, \gamma Q)$,
- take a random point R and compute $\frac{e(P+R,Q)}{e(R,Q)}$.

6 Conclusion

We present side channel attacks in pairing based cryptography and the countermeasures to prevent them. The less expensive countermeasure is the third Coron's countermeasure. This countermeasure is very easy to introduce in a pairing algorithm and cost only three multiplications in $\mathbb{F}_p$, the drawback is this countermeasure is efficient only for projective and Jacobien coordinates. The other techniques are efficient for every system of coordinates but they are much more expensive. The countermeasure using integers needs a point multiplication over $E(\mathbb{F}_p)$ and $E(\mathbb{F}_{p^k})$. The countermeasure using a random point involves two pairing computations. Consequently, it seems more interesting to implement pairing in projective or jacobien coordinates and then use the third Coron's countermeasure.

References

1. C. Arne, T. Lange, M. Naehrig, and C. Ritzenhaler. Faster Pairing Computation of the Tate pairing. Cryptology ePrint Archive, Report 2009/155, `http://eprint.iacr.org/2009/155`, 2009.
2. D. Boneh and M.K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 213–229, London, UK, 2001. Springer-Verlag.
3. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In Colin Boyd, editor, *Advances in ASIACRYPT 2001*, volume 2248 of *mylncs*, pages 514–532. Springer Verlag, 2001.
4. E. De Mulder, S. B. Örs, B. Preneel, and I. Verbauwhede. Differential power and electromagnetic attacks on a fpga implementation of elliptic curve cryptosystems. *Comput. Electr. Eng.*, 33(5-6):367–382, 2007.
5. N. El Mrabet. What about vulnerability to a fault attack of the Miller's algorithm during an identity based protocol? In *Advances in Information Security and Assurance*, volume 5576, pages 122–134, London, UK, 2009. Springer-Verlag.
6. N. El Mrabet, G. Di Natale, and M.L. Flottes. A practical differential power analysis attack against the miller algorithm. In *PRIME 2009 - 5th Conference on Ph.D. Research in Microelectronics and Electronics, Circuits and Systems Magazine*, IEEE Xplore, 2009.
7. D.H Habing. The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits. In *IEEE Transactions On Nuclear Science*, volume 39, 1992.
8. A. Joux. A one round protocol for tripartite Diffie-Hellman. In *ANTS-IV: Proceedings of the 4th International Symposium on Algorithmic Number Theory*, pages 385–394, London, UK, 2000. Springer-Verlag.
9. M. Joye and G. Neven. *Identity-Based Cryptography.* vol. 2 of Cryptology and Information Security Series, IOS Press, 2009.
10. A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 80–89, New York, NY, USA, 1991. ACM.
11. V. S. Miller. The Weil pairing, and its efficient calculation. In *Jounal of Cryptology*, volume 17, pages 235–261, Secaucus, NJ, USA, 2004. Springer-Verlag New York, Inc.
12. D. Page and F. Vercauteren. Fault and side channel attacks on pairing based cryptography. In *IEEE Transactions on Computers*, 2006.
13. C. Whelan and M. Scott. Side channel analysis of practical pairing implementation: Which path is more secure? In *VietCrypt 2006*, Lecture Notes in Computer Science, 2006.
14. C. Whelan and M. Scott. The importance of the final exponentiation in pairings when considering fault attacks. In *Pairing-Based Cryptography Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 225–246, 2007.