A Dynamic Study with Side Channel against an Identification Based Encryption

Rkia Aouinatou[1], Mostafa Belkasmi[2], Mohamed Askali[3]

[1]University Mohamed V, Faculty of Science-Agdal, Rabat, Morocco
Laboratoire de Recherche Informatique et Télécommunication: LRIT
[2,3]ENSIAS: University Mohammed V, Rabat, Morocco
rkiaaouinatou@yahoo.fr, belkasmi@ensias.ma, m.askali@yahoo.fr

***Abstract*:** Recently, the side channel keeps the attention of researchers in theory of pairing, since, several studies have been done in this subject and all they have the aim in order to attack the cryptosystems of Identification Based Encryption (IBE) which are integrated into Smart Cards (more than 80% of those cryptosystems are based on a pairing). The great success and the remarkable development of the cryptography IBE in the recent years and the direct connection of this success to the ability of resistance against any kind of attack, especially the DPA (Differential Power Analysis) and DFA (Differential Fault Analysis) attacks, leave us to browse saying all the studies of the DPA and DFA attacks applied to a pairing and we have observed that they have no great effect to attack the cryptosystems of IBE. That is what we will see in this paper. In this work we will illuminate the effect of the DPA attack on a cryptosystems of IBE and we would see on what level we can arrive. Thus in the case where this attack can influence on those cryptosystems, we can present an appropriate counter-measures to resist such attack. In the other part, we will also propose a convenient counter-measure to defend against the DFA attack when the embedding degree is even.

***Keywords*:** Pairing, Miller, Smart Cards, Side Channels, DPA Attack, DFA Attack, IBE, IBC, Counter-measure.

1. Introduction

The Identification Based Encryption: IBE is an idea proposed by Adi Shamir in 1984 [1] as a concept and we had to wait until 2001 at which Boneh-Franklin [2] and Cocks [3] have materialized and applied with success the concept of Shamir. With the birth of those two new arts, several companies have begun work with IBE instead of PKI: Public Key Infrastructure; we may cite the two famous companies: Voltage security and NoreTech. This usage has given birth for the first time in the World in 2 November 2004 the integration of IBE cryptosystems in a Smart Card by Gemplus International. Which opens the door to all kinds of attacks of side channel applied to the cryptosystem's of IBE programming in a Smart Card, especially the DPA (Differential Power Analysis) attack, the DFA: Differential Fault Analysis is also a powerful attack. The scheme of Cocks is ineffective since it transforms bit by bit and it is shown that for an equivalent security of 128-bits we need a time 13 times larger than the standard X.509 of PKI, as long as the scheme of Boneh and Franklin is known as being the most famous and the most used, since, this scheme recovers more than 900 of the sites of Google. All the other cryptosystems of IBE which are based on the Random Oracle [2] [4] or not i.e on the Standard Model [5] [6] [7] have the same schedule as [2]. The scheme of Boneh and Franklin is based on what is called pairing; therefore attacking this latter using a DPA can attack the scheme in global. According to our knowledge, there is no study in the literature of the DPA attack that has applied clearly and directly against the IBE cryptosystems, all the studies have limited their search on the attack of pairing. Our goal in this work is to project the DPA attack to the IBC cryptography that is built into the Smart card.

In order to succeed the DPA attack against the pairing, two cases can be offered, secret is in the first argument of the pairing or in its second argument. Following the traditional methods [8] [9], when we make the secret in the first argument, this makes a natural counter-measure against the DPA attack. N. El Mrabet et al in [10] make to default this idea, more, the authors in [10] proposed a method to succeed the DPA attack and this when it is the position of the secret, in the first argument or in the second argument. Unfortunately, the study [10] is not effective; we will talk about its limit in section 3.3.

Our first contribution in this paper is to give a new approach to succeed a DPA attack against the pairing; our method can be applied when it is the position of the secret, first argument or second argument. To see the efficiency of our method we will compare it with that of N. El Mrabet et al which is purely practical (more it make to default the recognized [8] [9]), and this following the number of traces. In addition to this, we will traduce our proposition in IBC: Identification Based Cryptography (IBE is a kind of IBC). This is for the first time is introduced, as all the study of the DPA attack restricts their search on the pairing.

In order to defend the DPA attack against the pairing, there are three counter-measures: the counter-measure of J.S. Coron [11]; that' of D. Page and F. Vercauteren [8] and the one of C. Whelan and M. Scott [9]. As a second contribution of this paper we first study the rigidity of those counter-measures, more we will give new ones to defend the DPA attack.

In other part, the DFA attack is another kind of side channel it relates the ability to investigate cipher and extract key by generating faults in a scheme. The faults are often caused by changing the voltages tampering, applying radiation and so forth.

The traditional study of the DFA attack applied to a pairing are introduced by D. Page and F. Vercauten who proposed a fault attack against the algorithm of Duursma and Lee, N. El Mrabet [12] improve their method in order to satisfy the algorithm of Miller and so the pairing, but his study operate only when the embedding degree k is equal to 4. In their turn D. Yunqi et al [13] generalize [12] to the case when the embedding degree k is even. Our third contribution behind this work is to give a convenient counter-measure against the attack of D. Yunqi et al.

The organization of the lecture is as follows : First we give in section 2 some basics concepts of everything we can need in our study; the traditional study and the principal of the DPA attack will be given in section 3; in section 4 we expose our proposition for a DPA attack, in 4.1 we will give an appropriate method to succeed the DPA attack against the pairing, in 4.2 we will include the projection of the DPA attack in the cryptosystem of IBE, and even on those of IBC; in 4.3 we will give a convenient counter-measures in order to resist against the DPA attack applied to a pairing; section 5 expose a convenient approach to block the DFA attack when the embedding degree is even, as a final step we will terminate with a conclusion.

2. Some Basics

2.1 Introduction to Identification Based Encryption

An Identification Based Encryption (IBE) is a public key system where the public key can be an arbitrary string such as an email address. The corresponding private key can only be generated by a central authority, called Private Key Generator (PKG). The PKG uses a master key to issue private keys following identities request.

Unlike a conventional public key infrastructure (PKI), IBE eliminates the need for a public key distribution infrastructure. There is essentially no need for certificates and store individual public keys. The IBE guarantee an off line encryption, more, the public key are small by comparison with PKI. Thus, IBE systems are considerably easier and so less costly to implement.

Since the proposition of the scheme of Boneh and Franklin [2] to the challenge of Shamir, various Identity Based Encryption based on the pairing, have been proposed. In 2003, Sakai and Kasahara (prove of security in [4]) proposed an IBE scheme in the model random oracle; in 2004 Boneh and Boyen [5] proposed yet in the model selective ID two scheme BB1 and BB2, the BB1 can also operate with random oracle; in 2005 and 2006 respectively Waters [6] and then Gentry [7] proposed a schemes in the model standard. Those entire schemes are based on the pairing.

2.2 General vision in the pairing

The pairing are proposed by the mathematician Weil and Tate in front of XX-th century, since 1993, they are used in cryptography with a negative role according to two attack [14][15], they are converted to have a constructive role in 2000 with the tripartite protocol proposed by Joux [16] and the proposal of Boneh and Franklin [2] in 2001. The pairing is a bilinear map, which take two points on an elliptic curve and provides an element of the multiplicative group of n-th roots of unit. It has three fundamental proprieties: Bilinear, Alternative and Non-degenerate.

Among the pairing we cite: Weil, Tate, Eta, Ate, Twisted Ate, (the two last are a variant of Tate), but in cryptographic implementations we often encounter widely the two first.

2.2.1 Explicit formula of pairing

Let's: r be an integer prime with the characteristic of F_q, K=F_{q^k} a field that contains all roots of unity of order r, $P \in E(K)[r]$,$Q \in E(K)$ two points; D_P and D_Q two divisors of degree 0 with disjoint support and finally f_{D_P} , f_{D_Q} two functions with: div(f_{D_P}) = rD_P, div(f_{D_Q})= rD_Q

Tate Pairing:

The Tate pairing is an application:

$$t_r : E(K)[r] \times E(K)/rE(K) \longrightarrow K^*/(K^*)^r \quad (1)$$

Such that:

$$t_r(P,Q) = f_{D_P}\,(D_Q) \text{ modulo } (K^*)^r \quad (2)$$

But to have an exact formula we will have:

$$t_r(P,Q)) = \left(f_{D_P}\left(D_Q\right)\right)^{(q^k-1)/r} \quad (3)$$

Weil Pairing:

The Weil pairing is defined as follows:

$$e_r : E[r] \times E[r] \longrightarrow \quad \mu_r \quad (4)$$

(μ_r is all the rth roots of unity)

Where:

$$e_r(P,Q) = \frac{f_{D_Q}\,(D_P)}{f_{D_P}\,(D_Q)} \quad (5)$$

Algorithm of Miller:

The calculation of the pairing is not effective until the invention of the algorithm of Miller in 1986 [17] (the algorithm was developed in 2004 [18]).

The formula of pairing includes the rational function f_r and to calculate it, Miller use the following iterative method:

We define the following divisors D_i (for an extra definition we send the interested to [19]):

$$D_i = i[P + R] + i[R] + [iP\ ] + [O] \quad (6)$$

By the same we can write:

$$D_{r1+r2} = (r_1 + r_2)\,[P + R] + (r_1 + r_2)[R] + [(r_1 + r_2)P] + [O] \quad (7)$$

Then:

$$D_{r1+r2} = D_{r1} + D_{r2} + \text{div}\,(L_{r1P,\,r2P})/\text{div}(V(r_1+r_2)) \quad (8)$$

We can so extract the following iteration:

$$f_{(r_1+r_2)}(Q) = f_{(r_1)}\left(D_Q\right) \times f_{(r_2)}\left(D_Q\right) \times \frac{L_{r_1P,r_2PQ}}{V_{(r_1+r_2)PQ}} \quad (9)$$

The algorithm of Miller is just based on (9)

Algorithm of Miller (P, Q, r)

```
Input: r=($r_n$...$r_0$)(binary representation),
        $P \in G_1(\in E(F_q))$ and
        $Q \in G_1(\ E\in (F_{q^k}\ ))$
Output: $f_{r,P}\ (Q) \in G_3\ (\in F_{q^k})$ :
$T \longleftarrow P$
$f_1 \longleftarrow 1$
$f_2 \longleftarrow 1$
For i = n - 1 to 0 do
    $T \longleftarrow [2]T$
    $f_1 \longleftarrow f_1^{\,2} \times l_1(Q)$
     $l_1$ is a tangent line to the curve in T.
    $f_1 \longleftarrow f_1 \times v1(Q)$
    $v_1$ is the vertical to the curve in [2]T.
     If  $r_i$=1  then
```

```
        $f_2 \longleftarrow f_2^2 \times l_2(Q)$
        $l_2$ is the line which pass from (PT).
        $f_2 \longleftarrow f_2^2 \times v_2(Q)$
        $v_2$ is a vertical line which pass from the point
        P + T.
    End If
End For
Return $f_1/ f_2$
```

2.3 Basic scheme of Boneh and Franklin

IBE was proposed by Adi Shamir in 1984 [1] as a solution to the problem of the revocation of the public key and the requirement of the certificate in PKI. In IBE (Identification-Based Encryption) the public key can be represented as an arbitrary string such as an email address. Its corresponding private key is generated by a Private Key Generator (PKG) who authenticates users according to their corresponding identities.

This idea was proposed by A. Shamir only as concept. And we will wait until 2001 at which D. Boneh and M. Fanklin [2] propose an elegant scheme in the model Random Oracle using the pairing. In the following we remember the basic scheme of Boneh and Franklin, we send the interested to the original paper [2] for a more details.

To encrypt a message $M \in \{0,1\}^n$, choose a number $r \in Z_q$ and the public parameters:

$< q, G_1, G_2, e, n, P, P_{pub} = sP, Q_{ID}, H_2 >$ (see [2] for a more details).

The message is encrypted as follows:

$C = < rP, M + H_2(g^r) >=< U, V >$

With $g = e(Q_{ID}, P_{pub}) \in G_2{}^*$

To decrypt this message using the private key

$d_{ID} = sQ_{ID} \in G_1$,

Calculate: $V+H_2(e(d_{ID}, U)) = M$

Note that:

$$e(d_{ID}, U) = e(sQ_{ID}, rP) = e(Q_{ID}, P)^{sr} = e(Q_{ID}, P_{pub})^r = g_{ID}{}^r \quad (10)$$

2.4 Smart Card

We can reference the idea of a Smart Card to the year 1947 at which an Engineer British noticed that under the effect of a large current, a Bakelite substrate volatilizes irreversibly by creating an effect on its memory, hence the idea of a portable memory. The concept of the Smart Card was invented in the year 1974 by Roland Moreno. But the Smart Card doesn't exist publicly until 1983, since then it begin to be developed by decreasing the number of its remaining unit and increasing the number of its bits (32 bits in 2005). To have a common physical characteristics of Smart Cards, several ISO (International Organization for Standardization) have been proposed and they are carrying from 1987. Two types of Smart Cards: Memory cards and Microprocessor cards, also known as asynchronous cards. In the cryptography we are interested only in this latter because it is often used for computer security and cryptography, as it focuses a coprocessor which contains many of the operations cryptographic: multiplication, etc. DES encryption...

Unfortunately, Smart Cards can simply brittle against worm attack like the one given in [20], against side channel like differential power analysis, timing attacks, fault analysis, etc.

3. Background Information on the DPA Attack

3.1 Introduction

Differential Power Analysis (DPA) is a powerful technique which allows recovering secret data that is manipulated in the interior of a Smart Card or any circuit (hard disk of PC) by monitoring power signals.

The DPA is based on statistical methods (the average distance, the Pearson coefficient, maximum likelihood, etc). In general, DPA make a statistical study from multiple curves.

There are several types of DPA, the most powerful is HODPA (High Order DPA), as it uses a statistical methods on the correlation of several input parameters and measurement results.

The DPA attack was planned in 1975 by Roland Moreno. A theory research study is given by P. C. Kocher, J. Jaffe, and B. Jun in 1999 [21].

Most electronic circuits today (especially those of a chip) are based on CMOS technology. In this technology the state change causes a door charge or a discharge electrical of the transistors that are considered as capacity C. And so for a change of state of one bit from 0 to 1, a charge is stored in the capacity and this amount to the fact that the capacity is connected to VDD. For the converse (1-0) the capacity discharges, the state transitions of bit 0 to 0 or 1 to 1 does not contribute to the variable global of the electrical circuit.

3.2 Theoretical principle of the DPA Attack

In this study the DPA attack that interests us is that applied to a pairing (in all this study we note the pairing by e), hence, for the attack to have a sense, we consider that both the input of the pairing e are: P public parameter and R the secret that we seeks. To perform the attack we associate a hypothesis about the value of a bit of R, and we give several different entries of our choice to the known parameter P. Repeatedly running the algorithm to compute the pairing ie Miller with these entries chosen and we memorize the traces of current $T_{11}, T_{12}, .., T_{1m}$, ($500 \le m \le 1000$ as it was specified in [22]). DPA make assumptions about the secret (hypothesis bit by bit), it determines the correct hypothesis of the secret and to determine this latter, we make the following analysis:

For a clear analysis of the data, we assemble the current traces T_{1j} into two sets depending on the value of bit b running in Miller (the calculation of the pairing e is based on the algorithm of Miller) named the bit target. We then form two sets T_0 and T_1:

$T_{1j} \in T_0|$ Miller (P_j, R) [b] = 0, we change P_j according to our choice

$T_{1j} \in T_1|$ Miller (P_j, R) [b] = 1 (11)

For each hypothesis, M_{0i} and M_{1i} are respectively the average of the sets T_0 and T_1.

$$M_{0i} = \frac{\sum_{j=1}^{m}\left(1 - \mathrm{Miller}\left(P_j, R\right)[b]\right).T_{0i}}{n - \sum_{j=1}^{m}\left(1 - \mathrm{Miller}\left(P_j, R\right)[b]\right)} \quad (12)$$

$$M_{1i} = \frac{\sum_{j=1}^{m}\left(\mathrm{Miller}\left(P_j, R\right)[b]\right).T_{1i}}{\sum_{j=1}^{m}\left(1 - \mathrm{Miller}\left(P_j, R\right)[b]\right)} \quad (13)$$

We then calculate the difference between these two averages:

$$M_{DPA} = M_1 - M_0 \quad (14)$$

If the hypothesis is not correct, the bit b is equal to the actual bit with probability $\frac{1}{2}$ for each P_j. So the trace of current caused by transitions of different types ([0-1] and [1-0]) can be found in a same set (T_0 or T_1). Therefore, it is likely that the two averages M_0 and M_1 are equal and that the curve of DPA is flat and close to zero.

On the other hand, if the hypothesis is correct, the bit b is equal to the actual bit with a probability of 1. Therefore the traces of current caused by transitions of the same type ([0-1] or [1-0]) will meet in a same set (T_0 or T_1) and therefore a strong peak amplitude will be displayed.

3.3 Traditional study of the attack DPA applied to the pairing

The early studies of DPA attack applied to a pairing are started from 2006. The first study is that of D. Page and F. Vercauteren [8], they exploited a study applied to the Duursma-Lee algorithm, but it is not effective as it is restricted only on the algorithm of Duursma-Lee and on the supersingular curve, it does not touch and develops the DPA globally. C. Whelan and M. Scott [9] brought a study more global, it can be applied either on Tate, Ate, Eta. Since, they focused their study in the arithmetic operations which are developed within the algorithm of Miller: Multiplication (the Shift and XOR method), Root square reduction. The same idea was used by Tae Hyun Kim et al [23] in which they concentrate only on Eta pairing.

All these studies are theoretical. A more practical study was proposed by Nadia El Mrabet et al in 2009 [10] and we had not met any similarly practical study applied to a pairing. More it put in default the two studies [8] [9].

According to N. El Mrabet et al instead of use the Miller to attack pairing, it suffices only to use the equation of the line l_1 developed for example in coordinate Jacobean. The attack can be applied to other coordinates: Affine, Projective, more to Edward, but it is preferable to use the Jacobean, according to [24] in which the authors prove that those coordinate are more suitable to accelerate the calculate of pairing (the calculate of f_2 in algorithm of Miller can omit-see algorithm of Miller in section 2.2).

To validate the DPA attack practically against the algorithm of Miller, the authors in [10] has implemented a circuit in which they evaluate the equation of the line l_1

$$(l_1(x_Q, y_Q) = Z_3Z^2y_Q\text{-}2Y^2\text{–} (3X^2 - aZ^4)\ (Z^2x_Q - X)) \quad (15)$$

in Miller algorithm. The authors divide the circuit in three steps. So, to succeed the DPA attack [10] it suffice to attack firstly Z from step (2) $R_1=Z^2 \times x_Q$ and then determine X from step (3) ($R_1=Z^2 \times x_Q$ - X). Once the two coordinate X and Z are determined it shall be easy to attack the remaining coordinate Y from the equation of the elliptic curve.

This study is not practical for the following reasons:

Firstly, the circuit is simulating to architecture of 8 bits and for a level of security of 160 bits, the authors propose to just divide the architecture in 8 bits, but, this is not true. Because we are not in the case of DES, since the DES is divided to S_{BOX} (S_{BOX1} + …+ S_{BOX8}) connected by XOR, we can attack each S_{BOX} in last step (in the 16-th round) which is encrypted on 6 bits and do the research exhaust on the remaining 8 bits (56-48 = 8). As to l_1 it is not possible to divide it in pieces of 8 bits, because, it developed the compute of the total bits (160-bits).

But this problem can be solved by simulating a circuit for a wanted security.

Another weak weakness in [10], is that we cannot base the success of the DPA attack on a circuit that serves this success; we would so make to attack the software without rebuild a helpful hardware! A circuit similar to that proposed in [10] can speed up the calculation in the Smart Card, but because of the threat of the DPA attack we cannot integrate it in smart wearing secrets. We must so find ways to attack the cards that have a hardware standard, do not forgetting that ID card (specialize for cryptography) can have a particular construction.

In the following proposition we will take into account all those weaknesses.

4. Dynamic and Convenient Study For an attack DPA

4.1 Proposition of a convenient DPA Attack against the pairing

As we have pointed out, the study [10] makes in default both [8] and [9]. In [9] make the secret in the first parameter of the pairing is a cons-measure, like [10], we will make to default this idea.

To succeed the DPA attack against the pairing which is based on the algorithm of Miller, we will treat the two cases: secret is in the first argument (1st case) and in the second argument (2ed case).

<u>1st case:</u> The compute of the algorithm of Miller's is based on the order r of the first argument, we propose to attack this order and after calculate the inverse r' of this r. Attacking this order allows us to attack the point in search in the IBE cryptosystems (that's we will see later). The method to attack the order r is as follow:

To attack r (see the algorithm of Miller in section 2.2), we can use the SPA (Simple Power Attack), but since it is easy to find a cons measure against the SPA (SPA is almost ineffective today), we propose so to use the DPA.

In Miller's algorithm there are two different steps, a step which calculates the doubling and another calculate adding, following the binary representation of r. If r_i = 0 (r_i is the binary representation of r in step i) Miller calculate the doubling and if r_i = 1, the addition operation is liveliness to be calculate in the algorithm of Miller. So if we could distingue the kind of a step (adding or doubling) which is run, we could then determine the type of the bit r (0 or 1) in the step in question. To do this, we propose to block the algorithm of Miller for example in the step doubling

We suppose for example that r_i = 1 where r_i is the binary representation of r (see algorithm 2.2)

1. If f(Q) - (Q) = 0 put T_i in T_0
   Where f is the function computed by our self by the algorithm of Miller in the step doubling, without using Miller algorithm which we search to attack its secret. We note that Q is known.
   Until g is the function we can initially turn by the algorithm of Miller (which contain the secret) in the step doubling.
2. If f(Q) - g(Q) = 1 put Ti in T_1

Calculate T =$\overline{T}_0$- $\overline{T}_1$, where $\overline{T}_0$ and $\overline{T}_1$ are the average of the packet T_0 and T_1 respectively.

If the curve T represent one or lot of pick of consumption so $r_i = 1$, if not $r_i = 0$

In order to block the algorithm of Miller in the step doubling or adding suffices to know or at least to simulate the number of the clock cycles of doubling and that's of adding. In another way, we can simulate two points in an experiment card: 1st argument and 2ed argument. After, we can ask Miller to show to us for example DOU and ADD when it finishes from doubling and adding respectively. Even if, the point of the first argument may be different from the point R in search, but we can at least simulate the time for adding and doubling.

Using this method it will be easy for us to determine the kind of each step, step by step using a DPA attack, starting with step 1, 2, 3 and so forth.

2ed case: We describe the attack considering that in this case, we can have several methods to exploit it. For example, to attack the second parameter, we can consider the following: In the algorithm of Miller we need the computation of the line l_1 and that's of v_1 which are respectively the tangent and the vertical (line 10 and 12 in Miller's algorithm-see section 2.2). Those two lines have in their expressions a second parameter correlate with that's of the first argument in a form simple; we can therefore use simpler expressions among them (especially the vertical) to conduct a DPA attack.

To see the effectiveness of our method over that of [10] we keep the same parameters as it, the first parameter will therefore be in Jacobean coordinates, as this is very useful for the acceleration of the pairing [24], until the second is only in the Affine coordinate. The equation of the line l_1 will have so the form:

$$l_1(x_R, y_R) = Z_3Z^2y_R - 2Y^2 - (3X^2 - aZ^4)(Z^2x_R - X) \quad (16)$$

The coordinates (X, Y, Z) are for the point of the first parameter (point P public) that we change according to our choice, so, playing on this choice we can obtaining a good results. Since, $Z_3 = 2YZ$ we execute always our algorithm of Miller for $Y_P = 0$. This allows us to eliminate the part that contains y_R in l_1 which will have the form:

$$l_1(x_R,y_R) = (aZ^4 - 3X^2)(Z^2x_R - X) \quad (17)$$

We note that if we take always $Y_P = 0$, we can get more points, so a good chance to succeed the DPA attack. Since, we can fix Z_P and searching for X_P suitable in the equation of the elliptic curve E: $Y^2 = X^3 + aXZ^4 + bZ^6$ (which is in the projective coordinates, it can be calculated from the points $((\frac{X_P}{Z_P{}^2}, \frac{Y_P}{Z_P{}^3})$ in the Affine coordinates). Like that, for each Z_P chosen, we can obtain at most three X_P convenient from the equation $X^3 + aXZ^4 + bZ^6 = 0$.

So, for each Z_P suggested we may get $1 \leq$ number $(X_P) \leq 3$. Applying the DPA attack as previously (section 3.2) to Miller's algorithm by combining the points (X, 0, Z) as points of the first argument that we changes each time, we are interested only in l_1 which have the form (17). This allows us to extract bit by bit x_R, after it is simple to extract y_R from the equation $y^2 = x^3 + ax + b$.

Following the coordinate used in the first argument and those of the second argument (Affine, Projective, Jacobean or Edward) we can exploit other methods.

4.2 Translation of our DPA attack to the IBE and IBC

Firstly, we will treat the case where the secret is in the first argument (case related to the order). Our proposal in this sense does not affect directly the secret, but we will see that it is enough useful to attack the cryptosystems of IBE and IBC (Identification Based Cryptography). We will limit our study to the cryptosystem of Boneh and Franklin (section 2.3), the study is also valid for [4] [5] [6] [7] and others, we just play on their syntax. Before exploiting this, we can say that operating the IBE cryptosystem in the Smart Card has no sense, as its password can be fairly cryptanalysis in the authentication phase (attack presented in [25]) that's why Smart Card request (require) a secure channel between sender and receiver, this is impractical.

For ongoing communication between the sender and receiver concerning a subject, the sender can reuse the scheme of Boneh and Franklin to encrypt the messages to the receiver, always with the same parameters $< q, G_2, G_2, e, n, P, P_{pub} = sP, Q_{ID}, H_2 >$, the only thing that he can changes is r which he change it for each message (in fact C =ciphertext= $< rP, M+H_2(g^r) > = <U,V >$). Therefore to not recalculate it each time, the sender just programs the function:

$$r \longrightarrow g^r = e(Q_{ID}, P_{pub})^r$$

He stores it in somewhere, and the best place to keep it away the eyes of the opponents in order to reuse the calculations by changing only r, is in the Smart Card. Since it is imperative to access to this, which is impossible.

The only things left to an opponent are to use a covert side channel attacks and more particularly a DPA attack. To program (the sender) g^r, three opportunities are offered to us: Use r in the first argument ($g^r = e(rQ_{ID},P_{pub})$), in the second argument $g^r = e(Q_{ID},rP_{pub})$ or in the exponent $g^r = e(Q_{ID},P_{pub})^r$.

This is for a communication, sender to receiver. For the opposite (i.e receiver to sender), because of r which is changing each time, it is possible that the receiver need the calculation of $e(d_{ID},U) = e(sQ_{ID}, rP)$ and then to reuse it, he store it in a smart card.

We will light up all the three case of ciphers and that's of decryption.

Begin with the first case of encryption.

In this case, the secret is placed in the first argument and therefore according to our method (paragraph 4.1) it suffices only to attack the order r' of rQ_{ID}. Attacking r' and familiarizing with the order of rQ_{ID} of the point Q_{ID}, allows us to attack r, as $r=rQ_{ID}- r'$.

In made rQ_{ID} is not known but since Q_{ID} is public, we can for example calculate it using the following algorithm:

Algorithm to calculate kP

```
Input: a = m, B = O, C = $Q_{ID}$;
If a is even a $\longleftarrow \frac{a}{2}$, B=B, C=2C;
  If a is odd,
    a $\longleftarrow$ a-1, B=B+C,C=C;
      If a $\neq$ 0, go to step 2.

      End if
    End if
End if
Output B
```

Remarks:

1. To calculate rQ_{ID} we can initialize with m=q, as $Q_{ID} \in G_1$, this latter is cyclic with order q. With bQ_{ID} (b < q is of our choice, we can choose it great) we can accelerate the previous algorithm. We demand to the algorithm to profit t in the output when bQ_{ID}=O. So $rQ_{ID} = tb^{-1}$.
2. We cannot attack r from rQ_{ID}, rP or any another expression, as it is a discrete logarithm problem.
3. The authority can give to the user rQ_{ID} as the sender Alice need it to calculate for example, $e(rQ_{ID}, P_{pub})$ (to calculate the order of rQ_{ID}, Alice need to know Q_{ID}).

Once r is attacked it will be simple to calculate:
$e(Q_{ID}, P_{pub})^r = g^r$.
Turning now to the second case of the encryption i.e
$e(Q_{ID}, rP_{pub})$. Our method of the second case allows us to attack directly rP_{pub}, so easily calculating $e(Q_{ID},rP_{pub}) = g^r$. It still to us now the 3th of the encryption i.e the case bound to the exponent ($g^r = e(Q_{ID}, P_{pub})^r$).
To calculate the exponentiation several methods can be used, we cite for example that's of string by Chain or by Window, both these methods are sensitive to the consumption attacks. For example, with the first i.e by Chain a DPA attack is effective to find the secret (the study of Jean-Sebastien Coron [11]) as that of Window; we just apply a SPA attack (Pierre-Alain Fouque et al [26]). We cannot explain those methods, more, we cannot bring any proposal and as there are several methods to exploit exponentiation, we can limit only to give the appropriate counter-measures.
Going now to the decryption, in $e(sQ_{ID},rP)$ the secret door in the first argument it is d_{ID}, since, the second point rP is public. Then the attack of $e(sQ_{ID}, rP)$ can be made with the same ways as 1st case of the encryption i.e attacking the order r' of sQ_{ID} and using r_{QID} we can determine $s=r_{QID}$-r', but this is very dangerous, as s is the master key.
Attacking g^r may present a threat to the communication Alice-Bob as it allows to calculate $H_2(g^r)$, because H_2 is public. This allows the opponent Eve to attack one of the messages in the communication Alice-Bob, after she can calculates $M + H_2(g^r) + H_2(g^r)= M$. So, she can follow the communication Alice-Bob. Our adversary Eve in this case has a near relation to Alice or to Bob, she may be a colleague or a client of work.

In reality, Smart Cards are used to hidden a signature or a protocol of Key agreement protocol, since likely, an authority can sign the private key of a sender to a receiver in a Smart Card. We have examine all the signatures: Sakai-Ohgishi- Kasahara's ID-based signature (IBS) [27], Hess's IBS [28], Cha-Cheon's IBS [29] Paterson's IBS [30] and we note that it doesn't give good result. The great goal that we imagine to attack a signature is to attack the secret key S_{ID} and because of the pattern formulas of [27] [28] [29] [30] and the fact that the signatures can be reused once time; we note that this is hard.
By contrast, the DPA can influence on the Key agreement, because for example if we take the scheme of Chen Kudla's Key Agreement [31], it is possible that an entity A stores a key $K_{AB} = e(S_A,T_B +aQ_B)$ in a Smart Card. But, attacking at the same time S_A and $T_B + aQ_B$ is hard, since when we change one of the inputs to carry out an attack DPA we lost the secret. Then, either we attack S_A which is the key secret, using the same method of 1st case of encryption, or, attacking $T_B + aQ_B$ using the 2ed case of encryption and after calculating $T_B +aQ_B -T_B$ (since $T_B = bQ_B$ is public). But attacking $K_{BA} = e(Q_A,Q_B)^{s(a+b)}$ is hard, except that if we have the opportunity to get two cards, one that contains
$K_{AB} = e(S_A$, TB + $aQ_B)$
and the other contains $K_{BA} = e(T_A+bQ_A, S_B)$.
This may be through a cooperation between two opponents, one (Eve) have the opportunity to get a card that contains K_{AB} while the other (Cesar) can get the card that contains K_{BA}. So Eve can access to s after she attack $S_A = sQ_A$ using the method of the 1st case of encryption, by the same method Cesar can calculate a+b after he has access to the order of $T_A + bQ_A$ = (a+b)QA.
So, the key: $K = kdf(K_{AB}) = kdf(K_{BA}) = kdf(e(Q_A, Q_B)^{s(a+b)})$ can be extract easily, kdf is the key derivations of the function (kdf may be a hash function H_2: $G_2 \longleftarrow \{0,1\}^*$).
The same method can be applied to other protocols.
As we have present the effect of a DPA attack on IBE cryptosystem's (and IBC), we move now to know in what level we can arrive by comparing our method with [10] which is purely practical. We compare our method: make the secret in the first argument and in the second argument with the study [10] which addresses only the first argument. Our comparison take into account only the numbers of traces of each method, we perform the comparison forgetting that we must reusing the analysis by increasing the number of traces obtained when a peak not desirable is display (insufficient air). According to [22], the studies will almost succeed when the secret correlate with a point public number between 500 and 1000 for a multiplication and a number of 65 280 = $2^9 5^2$ for the subtraction.
For our experiment (table I) we accept 800 = $2^5 5^2$ choice for the two studies [10] and our, also we accept that the two points P (public) and R (secret) have the same order of 160-bits in the security.

Table I. Comparison between [10] and Our Study

Study [10]	**nbtraces to attack Z_R**	**nb_{traces} to attack X_R**	**nb_{traces} to attack l_1=sum**
One bit	$2^5 5^2$ traces	2^8×5×51 traces	$2^5 5(5+2^3×51)$ traces
160 bits	2^{165}×52 traces	2^8×5×51 traces	2^{165}×2065 traces

Our	**nb_{traces} to attack 1st argument (order r)**	**nb_{traces} to attack 2ed argument (x_R)**
One bit	$2^5 5^2$ traces	2^8×5×51 traces
160 bits	$2^{165}×5^2$ traces	2^{168}×5×51 traces

nb_{traces} is the number of traces.
It is visible that:

$$2^{165}5^2 = 2^{165} \times 25 << 2^{165} \times 2065$$

and that

$$2^{168} \times 5 \times 51 = 2^{165} \times 2040 << 2^{165} \times 2065.$$

4.3 Convenient Cons-measure

A cons-measure permits to resist against any attack of side channel, in particular an attack DPA.
The counters measures are divided in two types: hardware and software, but in the sequel we are interested only in software.
Several cons-measures have been proposed against a DPA attack applied to a pairing, we include:
($\forall\lambda \in Fp^*$, $(X, Y, Z) = (\lambda^2 X, \lambda^3 Y, \lambda Z)$ proposed by Coron [11]; $e([s]P,[r]Q) = e(P,Q)^{sr}$ such that sr = 1 mod(l), with l is the order in the algorithm of Miller, this cons-measure is introduce by Page and Vercauteren [8];
$e(P,Q) = e(P,Q + R)e(P,R)^{-1}$ proposed by Scott [9].
We are going to make in default some of those cons-measures, begin with the first. This cons-measure was based on the homogeneity so $(\lambda^2 X, \lambda^3 Y, \lambda Z)$ can play the same role as (X, Y, Z), but this cons-measure is fragile. Since, if we attack $(\lambda^2 X, \lambda^3 Y, \lambda Z)$ we can attack (X, Y, Z) basing on the fact that:

$$\frac{\lambda Z}{\lambda^2 X} \times \lambda Z = cte_0 \longrightarrow X = cte_1 Z^2 \quad (18)$$

Also:

$$\frac{\lambda^2 X}{\lambda^3 Y} \times \lambda Z = cte_2 \longrightarrow Y = cte_3 XZ \longrightarrow$$
$$Y = cte_1 cte_3 Z^3 \quad (19)$$

We replace in the equation

$Y^2 = X^3 + aXZ^4 + bZ^6$, X and Y with their expressions in (18) and (19), which allow us to extract Z and then extract X and Y using always (18) and (19).
By contrast, the cons-measure $e([s]P,[r]Q) = e(P;Q)^{sr} = e(P,Q)$ can render the service, since, we provide r, s such that sr = 1 mod l to mask P and Q. This cons-measure is hard, because make the secret in P or Q and mask this secret by r or s paralyzes the attack. Because, even if we try to attack the secret in which make in its expression one of the parameters s or r it still to us the second parameter in the other argument. It is not possible to attack simultaneously a secret multiply by one of the parameters, and attack at the same time the second parameter in another argument. Since, to attack the secret in one argument we must change the other argument and once we made that change we lose the second parameter.
We note that the proposal [9] to choose a random r and s such that rs = 1 mod l can render the service is not true, because, we shouldn't get the same r and s which are stored in the card.
For the third measure we doubt in its efficacy, since in
$e(P,Q) = e(P,Q +R)e(P,R)^{-1}$ the secret is in its second argument masked by R (the secret must be Q, because if it is P the cons-measure has no role) and we retrench the mask by the expression $e(P,R)^{-1}$. This expression has an inverse, and since the inverse consumes much electrically, we can so separate e(P,Q+R) from e(P,R), then we can attack firstly Q+R, after attack R, so calculate Q+R-R = Q.
Now, as we have presented the effectiveness for each cons-measure, we'll discuss the effect of these counter-measures in our methods.
We start by the exponentiation, any previously proposed cons-measure in the literature does not resist to this operation. The two pairing Tate and Weil, admit in their output a reduction modulo l, because the output of Weil μ_l (the set of all l-th root of unit) and that of Tate is $\frac{K^*}{K^{*l}}$. So for the tow pairing $e(P,Q)^l = e(P,Q)$, using this we can build a cons-measure. Choose λ as an arbitrary number, so $e(P,Q)^r = e(P,Q)^{r+\lambda l}$, we cannot extract r as we don't know λ and in the preferable l (it is due to have an unknown l).
Another cons-measure that we can brings against an exponentiation is to choose λ and λ such that λ λ' = 1, then calculate $e(\lambda P,Q)^{\lambda' r} = e(P,Q)$. So, we cannot extract r as we don't known λ' and more λ.
As concern our method, make the secret in the first argument, or in the second argument, the cons-measure $e([s]P,[r]Q) = e(P,Q)^{sr}$ such that rs = 1 mod l can render the service. In addition to the case make the secret in the first argument, we propose the cons-measure e(σP,Q) to paralyze the DPA attack. The σ is an invertible parameter that we add for example in the public parameters following the form:
$< q, G_1, G_2, e, n, P, P_{pub} = sP, Q_{ID}, \sigma Q_{ID}, H_2 >$, the parameter σ is invertible with an inverse σ′, it suffices only to calculate $e(\sigma P, Q)^{\sigma'}$ for decryption.
Our method of the first argument consists to find the order of the secret to use it following the method that we have mentioned in paragraph 4.1 (i.e that's of 1st case of encryption). For example in the scheme of Boneh and Franklin, our secret is r in the expression $e(rQ_{ID}, P_{pub})$ that we can attack it by the method of 1st case of encryption. But if we change this expression by $e(r\sigma Q_{ID}, P_{pub})$, the only things that we can attack is rσ, we cannot attack anywhere r as we don't know σ.
As concerned make the secret in the second argument, because of the fact that the cons-measure $e(P,Q + R)e(P,R)^{-1}$ is very expensive for a Smart Card, more we doubt on its efficiency, we propose so to use the cons-measure e(P,Q+aP) as e(P,Q+aP)=e(P,Q). Because, e(P,aP)=1, P is public and a is a secret parameter chosen by the user.

5. Dynamic and Convenient Study to block an DFA attack for any even Embedding Degree

5.1 Traditional proposals

In [8], D. Page and F. Vercauteren have proposed a fault attack against the algorithm of Duursma and Lee. Their attack consists to disrupt the number of iterations of this algorithm in coordinate Affine. In [12] N. El Mrabet developed their idea in order to satisfies the algorithm of Miller, her proposal requires to have two consecutive results in the step doubling or adding, which are $f_{\tau,P}(Q)$ and $f_{\tau+1,P}(Q)$, and then calculate the ratio

$$R = \frac{f_{\tau+1,P}(Q)}{f_{\tau,P}(Q)^2} \quad (20)$$

The attack relies on solving a system obtained by identification elements in the basis of F_{p^k}. Using Jacobian coordinates and k = 4, the author found a simple system if $r_{\tau+1} = 0$ and a little difficult if $r_{\tau+1} = 1$.
As weakness, the [8] is only valid to the algorithm Duursma and Lee in which figure the product:

$$\prod_{i=1}^{m}[(-y_P{}^{3^i}.y_Q{}^{\frac{1}{3^{i-1}}}.\sigma(x_P{}^{3^i} + x_Q{}^{\frac{1}{3^{i-1}}} + b)^2).(x_P{}^{3^i} +$$
$$xQ13i-1+b)2\rho-\rho2] \quad (21)$$

So when we get two results after an injection of fault $R_{m'+r}$ and $R_{m'+r+1}$, their relationship can be simplified to:

$$(-y_P{}^{3^i}.y_Q{}^{\frac{1}{3^{i-1}}}.\sigma(x_P{}^{3^i} + x_Q{}^{\frac{1}{3^{i-1}}} + b)^2).(x_P{}^{3^i} + x_Q{}^{\frac{1}{3^{i-1}}} + b)^2\rho - \rho^2 \quad (22)$$

It is obvious that solving this equation is not easy as we need to calculate an i^th^ root, in addition to this weakness, for pairing in which remain an exponentiation (Tate, Ate, Eta, Twisted Ate ...). To succeed the attack it requires reversing $q^k - 1$, so know the root in question where k is a selected embedding degree. The problem was treated for k = 3, k = 6 in [32] and [9] respectively, but for general degrees, this pose a great problem, so exponentiation is counted in [9] as convenient cons-measure against DFA attack applied to a pairing.

This problem does not arise for Nadia El Mrabet [12], as there are many methods in literature microelectronics that allow stopping the calculations before exponentiation, read the intermediate result between the execution of the algorithm of Miller and exponentiation, or cancel the exponentiation step.

But, as it is said in [12] this attack presents only the case when the embedding degree was equal to 4. More, the authors found that the attack could not recover the secret in the case where $r_{\tau+1} = 1$. The attack proposed in [13] generalize that's in [12] as it present an attack DFA for any even embedding degree and when $r_{\tau+1}= 1$. In the sequel, we propose an appropriate cons-measure against the two attacks [12] and [13].

5.2 Proposal cons-measure to block the attack [12, 13]

5.2.1 Small change in Miller to block an DFA attack for any embedding degree

To block the attack [12] [13] i.e for any embedding degree, we propose to add a random integer r_2 in the algorithm of Miller (paragraph 2.2) as it is elaborate in the algorithm below:

Modified Algorithm of Miller (P, Q, r)

```
Input: $r=(r_n...r_0)$(binary representation),
        $P \in G_1(\in E(F_q))$ and
        $Q \in G_1( E\in (F_{q^k}))$
Output: $f_{r,P}(Q) \in G_3 (\in F_{q^k})$ :
T ⟵ P
$f_1$ ⟵ 1
$f_2$ ⟵ 1
$r_2 \in F_p$
For i = n - 1 to 0 do
   T ⟵ [2]T
   $f_1$ ⟵ $f_1^2 \times l_1(Q) \times r_2$
   $l_1$ is a tangent line to the curve in T.
   $f_1$ ⟵ $f_1 \times v_1(Q) \times r_2$
   $v_1$ is the vertical to the curve in [2]T.
    If $r_i=1$ then
      $f_2$ ⟵ $f_2^2 \times \times l_2(Q) \times r_2$
      $l_2$ is the line which pass from (PT).
      $f_2$ ⟵ $f_2^2 \times v_2(Q) \times r_2$
      $v_2$ is a vertical line which pass
      from the point P + T.
    End If
End For
Return $\frac{f_1}{f_2} \times r_2^{(numi=0)-(numi=1)-1}$
```

Advertisement 1: The modified algorithm of Miller is correct and it can take the same result as the traditional algorithm can complete after the exponentiation final (Tate pairing and its variants).

Proof 1: $r_2 \in F_p$, after raising to a power $\frac{p^k-1}{r}$, the calculate can be simplifies to the original calculation, as,

$r_2^{\frac{p^k-1}{r}} = 1$. Since, $(\frac{p^k-1}{r}) = (\frac{p^k-1}{\varphi_k(p)}) \times \frac{\varphi_k(p)}{r}$ (result of Koblitz and Menezes [33]) and as

$$p^k - 1 = \prod_{k'/k} \varphi_{k'}(p) \quad (23)$$

So, $\varphi_1(p)= (p-1)/ (\frac{p^k-1}{\varphi_k(p)})$ (24)

This result seems valid to a pairing in which figure exponentiation (Tate and its variants) and that Weil cannot benefit. But, it is possible to raise it to a power and it is proved that this operation is also useful to reduce the complexity of the Weil pairing.

Advertisement 2: The modified algorithm of Miller resists to the fault attacks [12][13].

As [13] generalize [12], it suffices to make the proof for [13].

Proof 2: Begin with the case where $r_{\tau+1} = 0$. After the identification the two equations:

$$R = \frac{f_{\tau+1,P}(Q)}{f_{\tau,P}(Q)^2}$$

And

$$f_{\tau+1,P}(Q) = f_{\tau,P}(Q)^2 \left(2{Z_j}^3 Y_j y\sigma - 2{Y_j}^2 - 3\left({X_j}^2 - {Z_j}^4\right)\left(x{Z_j}^2 - X_j\right)\right) \quad (25)$$

With the fact that:

$R = R_{2n-1}\, \xi_{n-1}\, \sigma + R_{2n-2}\, \xi_{n-2}\, \sigma + \ldots + R_n\, \sigma + R_{n-1}\, \xi_{n-1} + R_1\, \xi + R_0$ (26)

lead to the following system:

$$\begin{cases} 2{Z_j}^3 Y_j y_{n-1} = R_{2n-1} \\ 2{Z_j}^3 Y_j y_{n-2} = R_{2n-2} \\ \cdot \\ \cdot \\ \cdot \\ 2{Z_j}^3 Y_j y_0 = R_n \\ (-3{Z_j}^2({X_j}^2 - {Z_j}^4))x_{n-1} = R_{n-1} \\ \cdot \\ \cdot \\ \cdot \\ (-3{Z_j}^2({X_j}^2 - {Z_j}^4))x_1 = R_1 \\ -3{Z_j}^2({X_j}^2 - {Z_j}^4)x_0 + 3({X_j}^2 - {Z_j}^4))X_j - 2{Y_j}^2 \\ = R_0 \end{cases} \quad (27)$$

After replacing the expressions of x and y respectively by:

$x_0 + x_1\xi + ::: + x_{n-1}\, \xi_{n-1}$ and $y_0 + y_1\xi + ::: + y_{n-1}\, \xi_{n-1}$ (28)

Carry out the relocation proposed in the modified algorithm of Miller to the system (27), this latter will be changing to:

$$\left\{\begin{array}{l} 2r_2{Z_j}^3Y_jy_{n-1} = R_{2n-1} \\ 2r_2{Z_j}^3Y_jy_{n-2} = R_{2n-2} \\ \vdots \\ 2r_2{Z_j}^3Y_jy_0 = R_n \qquad \Rightarrow \\ (-3r_2{Z_j}^2({X_j}^2 - {Z_j}^4))x_{n-1} = R_{n-1} \\ \vdots \\ (-3r_2{Z_j}^2({X_j}^2 - {Z_j}^4))x_1 = R_1 \\ r_2(-3{Z_j}^2({X_j}^2 - {Z_j}^4)x_0 + 3({X_j}^2 - {Z_j}^4))X_j - 2{Y_j}^2) \\ \qquad = R_0 \end{array}\right.$$

(29)

$$\left\{\begin{array}{l} 2r_2{Z_j}^3Y_jy_{n-1} = R_{2n-1} \\ 2r_2{Z_j}^3Y_jy_{n-2} = R_{2n-2} \\ \vdots \\ r_2{Z_j}^3Y_j = \lambda_0 r'_2 \qquad (B.1) \\ (-3r_2{Z_j}^2({X_j}^2 - {Z_j}^4))x_{n-1} = R_{n-1} \\ \vdots \\ {Z_j}^2({X_j}^2 - {Z_j}^4) = \lambda_1 r'_2 \qquad (B.2) \\ (-3{Z_j}^2({X_j}^2 - {Z_j}^4)x_0 + 3({X_j}^2 - {Z_j}^4))X_j - 2{Y_j}^2) \\ \qquad = \lambda_2 r'_2 \qquad (B.3) \end{array}\right.$$

With r'_2 represent the inverse of r_2 in F_p (the two are not known).

By (B.1), we draw $Y_j = \frac{\lambda_0 r'_2}{{Z_j}^3}$ (eq 1).

The (B.2) lead to have ${X_j}^2 - {Z_j}^4 = \frac{\lambda_1 r'_2}{{Z_j}^4}$

After using those tow equation and (B.3), it leads to the equation:

$$X_j = \frac{(\lambda_2 + 3\lambda_1 x_0){Z_j}^6 + 2\lambda_0 r'_2}{3\lambda_1 {Z_j}^4} \qquad \text{(eq 2)}$$

Substituting this equation in (B.2) permit to obtain:

$({\lambda_2}^2 + 9{\lambda_1}^2x_0 - 9{\lambda_1}^2)\,{Z_j}^{12} + (4{\lambda_0}^2\lambda_2 r'_2 + 12{\lambda_0}^2\lambda_1 x_0 r'_2 -$ 9λ13r′2Zj6+4λ04r′2

(eq 3)

The latter equation (eq 3) cannot be resolved as it contains the two unknown Z_j and r'_2.

The same things will be saying for the two equation ((eq 1) and (eq 2)) in which figure r'_2.

As a conclusion, we cannot any where extract the secret.

Concerning the case where $r_{\tau+1} = 1$, the attack is based on the two equations:

$$R = \frac{f_{\tau+1,P}\,(Q)}{f_{\tau,P}\,(Q)^2}$$

$f_{\tau+1,P}\,(Q) = f_{\tau,P}\,(Q)^2\left(2{Z_j}^3Y_jy\sigma - 2{Y_j}^2 - 3({X_j}^2 -\right.$ Zj4xZj2−Xj(ZjXPZ2j2−X2jyσ)-(YPZ2j3−Y2j)x-$(X_PY_{2j} - X_{2j}Y_PZ_{2j}))$ (30)

With the fact that:

$R = R_{2n-1}\,\xi_{n-1}\,\sigma + R_{2n-2}\,\xi_{n-2}\,\sigma + \ldots + R_n\,\sigma + R_{n-1}\,\xi_{n-1} + R_1\,\xi + R_0$ (31)

$x = x_0 + x_1\xi + ::: + x_{n-1}\,\xi_{n-1}$ (32)

$y = y_0 + y_1\xi + ::: + y_{n-1}\,\xi_{n-1}$ (33)

With the five equations (20), (30), (31), (32) and (33) we can extract the system:

$$\left\{\begin{array}{c} f_0(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = a_0 \\ f_1(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = a_1 \\ \ldots \\ f_{2n-2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = a_{2n-2} \\ f_{2n-1}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = a_{2n-1} \\ {Y_P}^2 - {X_P}^3 + 3X_P - b = 0 \\ {Y_j}^2 - {X_j}^3 + 3X_j{Z_j}^4 - b{Z_j}^6 = 0 \\ {Y_{2j}}^2 - {X_{2j}}^3 + 3X_{2j}{Z_{2j}}^4 - b{Z_{2j}}^6 = 0 \\ X_{2j} = -8X_j{Y_j}^2 + 9({X_j}^2 - {Z_j}^4)^2 \\ Y_{2j} = 3({X_j}^2 - {Z_j}^4)(4X_j{Y_j}^2 - X_{2j}) - 8{Y_j}^4 \\ X_{2j} = 2X_jZ_j \end{array}\right.$$

(34)

After applying the mutation proposed in the modified algorithm of Miller, the system (34) can be changed to:

$$\left\{\begin{array}{c} f_{0r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = b_0 \\ f_{1r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = b_1 \\ \ldots \\ f_{(2n-2)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) \\ = b_{2n-2} \\ f_{(2n-1)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) \\ = b_{2n-1} \\ f_{2n} = {Y_P}^2 - {X_P}^3 + 3X_P - b = 0 \\ f_{2n+1} = {Y_j}^2 - {X_j}^3 + 3X_j{Z_j}^4 - b{Z_j}^6 \\ = 0 \\ f_{2n+2} = {Y_{2j}}^2 - {X_{2j}}^3 + 3X_{2j}{Z_{2j}}^4 - b{Z_{2j}}^6 \\ = 0 \\ f_{2n+3} = X_{2j} + 8X_j{Y_j}^2 - 9({X_j}^2 - {Z_j}^4)^2 = 0 \\ f_{2n+4} = Y_{2j} - \ 3({X_j}^2 - {Z_j}^4)(4X_j{Y_j}^2 - X_{2j}) + 8{Y_j}^4 \\ = 0 \\ f_{2n+5} = X_{2j} - 2X_jZ_j = 0 \end{array}\right.$$

(35)

The resolution of this system (multi-variants) is based on the search of the Gröbner basis which can engender it.

This later is based on the method of eliminate term.

Let < be an order monomial defined by the monomer of $F_p[X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}]$.

The search for a Gröbner basis can be done in general using the compute of S-polynomial [34]:

Let f_1 and f_2, we have:

$$S(f_1, f_2) = u_1f_1 - u_2f_2$$

with lcm = LM(f_1) U LM(f_2) and $u_i = \frac{\text{lcm}}{\text{LT}(f_i)}$ for i ∈ {1, 2}. With the fact that:

- LM (f_i) represent the monomer of the head of f_i, it is defined by: LM(f_i) = X^{ρ}, where $\rho = \max\{\alpha \in N_n$ such that: the coefficients of fi ≠ 0 }.
- LC(f_i) is the dominant coefficient of f_i, it is defined by LC(f_i) = $\mathrm{coefficient}(f_i)_{\rho}$.
- LT(f_i) is the head term of f_i, it is defined by: LT(f_i) = LC(f_i) .LM(f_i)

The system (35) cannot be resolved following the sequel reason:

Reason

Firstly, the r_2 figure necessary in the syntax of S-polynomial of $f_{ir_2}$for any i ∈ {0, 1… 2n-1}, and this which is the function to be taken in (35**),** since:

As we have multiplying each function of (35) (that's of {0, …, 2n-1}) by r_2, with, $r_2 \in F_p$. So, the r_2 exist in all the coefficients dominant of f_{ir_2} and this for any i ∈ {0, 1, ..., 2n-1}.

As a consequence:
We have, ∀ (i,j) ∈{0, 1,…, 2n-1}^{2}:

$$S\left(f_{ir_2}, f_{jr_2}\right) = \frac{\mathrm{lcm}}{r_2 LC_{reste}(f_{ir_2})} f_{ir_2} - \frac{\mathrm{lcm}}{r_2 LC_{reste}(f_{jr_2})} f_{jr_2} \quad (36)$$

$$= r'_2\left(\frac{\mathrm{lcm}}{LC_{reste}(f_{ir_2})} f_{ir_2} - \frac{\mathrm{lcm}}{LC_{reste}(f_{jr_2})}\right) f_{jr_2} \quad (37)$$

And,

∀ (i,j) ∈ {0, 1,..., 2n-1} × {2n, ..., 2n+5}:

$$S(f_{ir_2}, f_j) = \frac{\mathrm{lcm}}{r_2 LC_{reste}(f_{ir_2})} f_{ir_2} - \frac{\mathrm{lcm}}{LC(f_j)} f_j \quad (38)$$

$$= r'_2\left(\frac{\mathrm{lcm}}{LC_{reste}(f_{ir_2})} f_{ir_2} - r_2 \frac{\mathrm{lcm}}{LC(f_j)} f_j\right) \quad (39)$$

To find a convenient Gröbner basis to the system (35), it suffices to use the algorithm of Buchberger [34]:

Algorithm of Buchberger

```
Input:
 I = < $f_{0_{r_2}}$ ,…, $f_{2n-1_{r_2}}$, f2n, …, f2n+5 >
 ∈ Fp[$X_P$ , $Y_P$ , $X_j$ , $Y_j$ , $Z_j$ , $X_{2j}$ , $Y_{2j}$ , $Z_{2j}$ ]
Output: G basis Gröbner of I.
   G  ⟵  $f_{0_{r_2}}$ ,…, $f_{2n-1_{r_2}}$, f2n, …, f2n+5
   CA ⟵  {S($f_i$,$f_j$), 0 ≤ I, j ≤ 2n+5}
   While CA ≠ 0 do
     Choose s ∈ CA and extract the CA
     r ⟵  s div G
      If r ≠ 0 so
       CA ⟵ CA U {S(g,r), g ∈ G}
       G  ⟵ G U {r}
      End if
   End while
Return G
```

The compute of the step 5 can be done by:

r ⟵ r + LT(S(f_i, f_j)) (division of two polynomial with variant variables).

Basing on two equations (37) and (39), the Gröbner basis of the system (35) is so:

$$\begin{cases} g_{0r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ g_{1r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ \cdot \\ \cdot \\ \cdot \\ g_{(2n-2)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ g_{(2n-1)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ g_{(2n)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ g_{(2n+1)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ g_{(2n+2)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ g_{(2n+3)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ g_{(2n+4)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \\ g_{(2n+5)r_2}(X_P, Y_P, X_j, Y_j, Z_j, X_{2j}, Y_{2j}, Z_{2j}) = 0 \end{cases} \quad (40)$$

The second step of the resolution of the system (40) consist to eliminate its parameters until find a polynomial with one variable; but in this case, the found polynomial is with two variable, and this because of the existence of r_2 (or the reverse of r_2 which is r'$_2$). As a consequence, the system (35) cannot be resolved.

6. Conclusion

We have presented in those papers firstly a DPA attack against a pairing, or rather against Miller's algorithm; our attack is effective whatever it is the position of the secret. We have translated DPA attack to the cryptography based in identity which is the first in the literature. The cryptosystems and the protocol's of Key Agreement are sensitive to this attack by contrast the syntax of the scheme of signature make to their natural cons-measure against the attack. Our study is purely theoretical, even if we do not shown its success practically, but to get a material results we have based on the study of which is purely practical and we arrived at the conclusion that attacking a protocol of IBE for a level of security 160- bits, using our method we need at least $2^{165}5^2$ traces, which is expensive, but we cannot say that it is impossible especially for an active opponent. The attack is a real threat to the IBE, especially when we have effective precautions close to a protocol of IBE and we just want to assure our care, therefore a DPA attack can make the service. Since, we can only test certain bits, but we have presented the appropriate counter measures to resist it. Among the obstacle that can be presented to succeed a DPA attack it is to specify the position and the style of the coordinate used (is it in the first argument, in the second argument? Or does it have a Projective coordinates, Affine, Jacobean and so forth). Also we have the problem of time, since for a calculation of 1024-bits of RSA we need only 300ms, which is very small if one wants to consider only the time of the operations that construct this protocol!.

Secondly, we have exposed a method to defend the DFA attack which is an even embedding degree.

Acknowledge

We would like to thank gratefully the head of our Laboratory LRIT, Aboutajdine Driss and the anonymous reviewers.

References

[1] Shamir, “Identity based cryptosystems and signature shemes” Proceedings of CRYPTO, USA, pp. 47-53, 1984.

[2] D. Boneh, M. Franklin, “Identity based encryption from the Weil pairing” 21st Annual International Cryptology Conference, Santa Barbara, California, USA, pp. 231-229, 2001.

[3] C. Cocks, “An identity based encryption scheme based on quadratic residues” 8th IMA International Conference Cirencester, UK, pp. 360-363, 2001.

[4] L. Chen and Z. Cheng. Security proof of Sakai-Kasahar's identity-based encryption scheme. In Proceedings of Cryptography and Coding, Cirencester, UK., pp. 442-459, 2005.

[5] D. Boneh, X. Boyen, “Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles” Proceedings of EUROCRYPT, Interlaken, Switzerland, pp. 223-238, 2004.

[6] B. Waters. “Efficient identity-based encryption without random oracles”. 24th Annual International Conference on the Theory and Applications of Cryptographic, Denmark, pp. 114-127, 2005.

[7] C. Gentry, “Practical identity-based encryption without random oracles” 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, pp. 445-464, 2006.

[8] D. Page, F. Vercauteren, “Fault and side channel attacks on pairing based cryptography”. In IEEE Transactions on Computers, Vol. 55, No. 9, pp. 1-6, 2006.

[9] C. Whelan and M. Scott, “Side channel analysis of practical pairing implementation: Which path is more secure” First International Conference on Cryptology in Vietnam, Hanoi, Vietnam, pp 99-114, 2006.

[10] N. El Mrabet, G. Di Natale, M.L. Flottes, “A practical diferential 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, French, 2009.

[11] J.S Coron, “Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems” First International Workshop, CHES’99 Worcester, MA, USA, pp. 292-302, 1999.

[12] N. El Mrabet, “What about Vulnerability to a Fault Attack of the Miller’s Algorithm During an Identity Based Protocol” Third International Conference and Workshops, Seoul, Korea, pp. 122-134, 2009.

[13] D. Yunqi, W. Jiang, W. Yun, Ma. Chuangui “Fault Attack against Miller’s Algorithm for Even Embedding Degree” International Journal of Network Security, Vol.16, No.3, pp. 185-193, 2014.

[14] A. Menezes, T. Okamoto, S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field” IEEE Trans. Inf. Theory, Vol. 39, No. 5, pp. 1639-1646, 1993.

[15] G. Frey, H. Rück, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves” Math. Comput. Vol. 62, No. 206, pp. 865-874, 1994.

[16] A. Joux, “A one round protocol for tripartite Diffie Hellman” Journal of Cryptology, Vol. 17, No. 4, pp. 263-276, 2004.

[17] V. Miller, “Use of elliptic curves in cryptography” Proceedings of CRYPTO, New York, USA, pp. 417-426, 1986.

[18] V.S. Miller, V. S, “The Weil pairing, and its efficient calculation” Jounal of Cryptology, Vol. 17, No.4, pp. 235-261, 2004.

[19] J. H. Silverman, “The arithmetic of elliptic curves’’ Book, 2nd Edition, Series. Graduate Texts in Mathematics, Vol. 106, 2009.

[20] O. Toutonji, S. Moo Yoo, “An Approach against a Computer Worm Attack’’ International Journal of Communication Network and information security (ijcnis), Vol. 1, No.2, pp. 47-53, 2009.

[21] C. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis” Proceedings of the 19th Annual International Cryptology Conference on Advance in Cryptology, London, pp. 388-397, 1999.

[22] N. El Mrabet, “Arithmétique des couplages, performance et résistance aux attaques par canaux cachés” Montelier. Thesis, Université Montpellie II - Sciences et Techniques du Languedoc, French, 2009.

[23] T. H. Kim, T. Takagi, D.G. Han, H. W. Kim, J. Lim, “Side Channel Attacks and Countermeasures on Pairing Based Cryptosystems over Binar Fields” 5th International Conference, CANS Suzhou, China, pp. 168-181, 2006.

[24] P.S.L.M. Barreto, B. Lynn, M. Scott, “On the selection of pairing friendly groups” 10th Annual International Workshop, SAC 2003, Ottawa, Canada, pp. 17-25, 2004.

[25] A. K. Pathan. “A Review and Cryptanalysis of Similar Timestamp-Based Password Authentication Schemes Using Smart Cards’’ International Journal of Communication Network and information security (ijcnis), Vol. 2, No.1, pp.15-20, 2010.

[26] P.A. Fouque, S. Kunz-Jacques, G. Martinet, M. Fréderic and V. Fréderic, “Power Attack on Small RSA Public Exponent” 8th International Workshop, Yokohama, Japan, pp. 339-353, 2006.

[27] R. Sakai, K. Ohgishi, M.Kasahara, “Cryptosysytems based on pairing”, In proceeding of the 2000 Symposium on Cryptograph and Information Security-SCIS, Okinawa, Japan, 2000.

[28] F. Hess, “Efficient Identity Based Signature Schemes Based on Pairings” 9th Annual International Workshop, SAC, Newfoundland, Canada, pp. 310-324, 2003.

[29] J. Cha, J.H. Cheon, ”An Identity-Based Signature from Gap Diffie-Hellman Groups” 6th International Workshop on Practice and Theory in Public Key Cryptography Miami, FL, USA, pp.18-30, 2003.

[30] K. G. Paterson, “ID-based signatures from pairings on elliptic curves”, Electronics Letters, Vol. 38, No. 18, pp. 1025 – 1026, 2002.

[31] L. Chen, C. Kudla, “Identity based authenticated key agreement from pairings” Proceeding, Computer Security Foundations Workshop, pp. 219-233, 2003.

[32] M. Joye, G. Neven, “Identity-Based Cryptography” Book, Vol 2, Cryptology and Information Security

Series. IOS Press, Amsterdam, The Netherlands. Chapter of Book . 2008.

[33] N. Koblitz, A. Menezes, “Pairing-based cryptography at high security levels’’ 10th IMA International Conference, Cirencester, UK, pp. 13-36, 2005.

[34] B. Buchberger. “Gröbner bases: An algorithmic method in polynomial ideal theory’’ Book, Multidim System Theory-Progress, Directions and Open Problems in Multidimensional Systems, Vol. 16, pp. 184- 232, 1985.