Cyptanalysis CDHP , BDHP and Tate pairing under certain conditions
The Tate pairing is less secure than Weil

Rkia Aouinatou (1)
University Mohamed V-Agdal, Rabat, Morocco
Laboratoire de Recherche Informatique
et Telecommunication: *LRIT*
Email: rkiaaouinatou@yahoo.fr

Mostafa Belkasmi (2)
ENSIAS: University Mohammed V- Souissi,
Rabat, Morocco
Email: belkasmi@ensias.ma

ABSTRACT

This work fall within the cadre of Cryptanalysis. Because, under certain condition, we would give a fairly simple method to solve the CDHP (the Problem Computational of Diffie and Hellman) and others problems associated to it. Since, solving this problem, will help us to provide a solution to the BDH (Problem Bilinear of Diffie and Hellman). The CDHP and BDHP are the heart of many cryptosystems in the point of view security, so solving it may be a threat to this cryptosystem's. To elucidate this, we use a concept of geometry algebraic named Tate Pairing.
This work is purely theoretical, we give firstly an overview on the idea and we illustrate it by an examples to see its efficiency.

I. Introduction

In modern cryptography, a lot of protocols and cryptosysem's are based on the Problem of Diffie Hellman. Our aim in this work is to attack many of this problem: CDHP and BDHP, by using what is called Pairing.
Under certain condition, solving the problem Computational of Diffie and Hellman (CDHP) using Tate pairing, may help us to break all cryptosystems based on this problem. And as the BDHP is related to CDHP, then, all the protocols related to it, can be easily attacked. Which imply a real threat to the exchange tripartite of Joux [2] and to the cryptography based on the identity of Boneh and Franklin [1], as well as, others protocols. After this work we will be careful to select the parameters linked to these cryptosystems. And so our contribution is to fix a condition to make into consideration to select such parameters.
Among the reasons that pushed us to address this problem, it is an open question in the article of Bonneh and Franklin [1] which state that there isn't equivalence between the problems CDHP and BDHP. With the fact that, between these two problem we have only the implication CDHP $\longrightarrow$ BDHP. Is it possible to obtain the reverse? The issue is almost solved theoretically but under certain condition. That's we will show in this article.

Organisation

This work is organized as follows: Firstly we give some preliminary mathematics. In the third section we detail our idea in order to solve these problems. We give a conclusion in the end section.

Key Words: CDHP, BDHP, Tate Pairing, Function Rational, Order of Point, Divisor and algorithm of Miller.

II. Preliminaries

A. Elliptic Curves

In general the equation of an elliptic curve E over a finite field k, is of the form:
$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ (*)
The elliptic curve over a field k, is defined as follows:
E(k)={ $(X, Y) \in K^2/(X, Y)$ verifies (*)}
A point P of coordinated (x, y) in an ellitpic curve E is singular, if $\frac{\partial(E)}{\partial(x)}$=0 and $\frac{\partial(E)}{\partial(y)} = 0$. The curve is called singular if it has at least one point singular.
The elliptic curve admits an element neutral noted universally by O, which has the form: (0,1,0) in the projective coordinates.

1) Group law for elliptic curve: An elliptic curve is fitted with an internal law of composition additive:
Let $P = (X_P, Y_P) \in E(k)$ and $Q = (X_Q, Y_Q) \in E(k)$ so :
$P + O = P$, $O + P = P$
$P + (-P) = O$, $-P = (X_P, -Y_P - a_1X_P - a_3)$

Explicit formula

Let $P = (X_P, Y_P)$ and $Q = (X_Q, Y_Q)$. The coordinates of P + Q are defined as:
$X_{P+Q} = \lambda^2 + a_1\lambda - a_2 - X_P - X_Q$,
$Y_{P+Q} = -(\lambda + a_1)X_{P+Q} - \nu - a_3$
With, $\lambda = \frac{Y_Q - Y_P}{X_Q - X_P}$ if $P \neq Q$ and $\lambda = \frac{3X_P^2 + 2a_2X_P + a_4 - a_1Y_P}{2Y_Q + a_1X_P + a_3}$ if not .
In general, for a field k of characteristic different to 2 and 3, the coordinates will be as follows:
If $X_P \neq X_Q$, P+Q is the point of coordinate (X_{P+Q}, Y_{P+Q}) such that: X_{P+Q}=$\lambda^2 - X_P - X_Q$
And, $Y_{P+Q} = \lambda(X_P - X_{P+Q}) - Y_P$ with $\lambda = \frac{Y_Q - Y_P}{X_Q - X_P}$
But if: $X_P = X_Q$ with $Y_P \neq Y_Q$, we will have P+Q=O. And if: $Y_P = Y_Q$, we will have a point double 2P of coordinated (X_{2P}, Y_{2P}), such that $X_{2P} = \lambda^2 - 2X_P$ and $Y_{2P} = \lambda(X_P - X_{P+Q}) - Y_P$, with $\lambda = (3X_P + a)(2Y_P)^{-1}$. Taking into account that the equation of the elliptic curve for a field of characteristic different from 2 and 3 is in the form: $Y^2 = X^3 + aX + b$ after using a suitable change of variable.

2) Scalar Multiplication: To calculate the product scalar kP, several algorithm can be considered (NAF algorithm, Montemogry ...). But we cite for example the following methods [3] which makes the calculations fast enough:
Input: a = m, B = O, C = P;

- if a is even a $\leftarrow \frac{a}{2}$, B=B, C=2C;
- if a is odd,a $\leftarrow$ a-1, B=B+C, C=C;

- if $a \neq 0$, go to step 2.
- **Output** B

3) Order of E (k), with k = F_q: . The order of the field is given by the famous theorem of Hasse:
$q + 1 - 2\sqrt[2]{q} \leq |E(F_q)| \leq q + 1 + 2\sqrt[2]{q}$
In general, we can use the algorithm of Schouf [4] published in 1985 to determine the order of the group.
The order of the point is the smallest integer m such that
mP = O, but if this parameters m doesn't exist the point P admits an infinite order.

4) Point of r-torsion: We say that P is a point of r-torsion (r is a positive integer) if r P = O
Definition 1: Let r be a positive integer, the ensemble
E[r] = { P ∈ E($\overline{F_q}$)/$rP = O$} is called an ensemble of point of r torsion.
$\overline{F_q}$ is an an algebraically closed. The integer r is not necessarily the order of point P it may be its multiple

Definition 2: Let G be an extension of k then we have: E(G)[r]=E[r]⋂G={P∈E(G)/rP=O}
The Degree MOV [5] : Let E be an elliptic curve in F_q and let r be a positive integer. The smallest integer k such that $E[r] = E(F_{q^k})[r]$ is called the MOV degree relatively to r

5) Curves Supersingular : Let E be an elliptic curve defined over $F_(q)$, with q is a power of p.
The curve E is **supersingular**, if it satisfies one of the tree equivalents conditions
1 · $E(F_q) \equiv 1$ mod p, or $E(F_q) = q + 1 - t$, with p|t (t is the trace)
2 . E has a point nontrivial of order p on $\bar{F}_q$, i.e, $E[p] = \infty$.
3 . The endomorphism of the ring E on F_q is non-commutative, or more specifically, it is an order on the quaternion algebra
A no-supersingular curve is called **Ordinary**

Distortions : The distortions have been found by Verheul [6]. Originally, they were used to provide an effective computable isomorphisms between elliptic curve over F^2 of order p^2-p+1. The distortions has the advantage that they send points to independent form. However, finding independent points is an important problem for the pairings.

Example of distortion

Field	Curve	Distortion
F_p	$y^2 = x^3 + ax$	$\phi(x, y) = (-x, iy)$
F_p	$y^2 = x^3 + b$	$\phi(x, y)$=(ζ x,y)

Propriety 1 (Verheul)[7] : Let E /F_q be a curve supersingular such that P ∈E(F_q) [n].
If n is relatively prime with the characteristic of F_q. Then there exists a distortion relatively related to p.

Propriety 2 (Verheul)[7] : Let E(F_q) be an ordinary elliptic curve , and let P ∈ E(F_q) [n].
If n is relatively prime to the characteristic of F_q. And E[n] is not in E(F_q), then there is no distortion relatively related to p.

The distortion in supersingular curve is related to the form of the curve. But in general, for supersingular or ordinary curve, we must only know if they have a form equal to that of a Twist Curve. Then we can use diffeomorfism linked to these curves

Some preliminary on Twisted Curves:
1. Twist of degree quadrature: Let $E(F_q) : y^2 = x^3 + ax + b$ be an elliptic curve and v ∈ F_q^* a quadratic non residue in F_q^*. So E'/F: $y^2 = x^3 + v^2ax + v^3b$ is named a quadratic twist of E.
E' is isomorphic to E in an extension of degree 2 on F_q

2. Twist of Large Degree: For any curve E(F_q) it is possible to have different twist from the quadratic one.
In this case we have: E':$y^2 = x^3 + a'x + b'$ with $a' = v^{\frac{4}{d}}a$ and $b' = v^{\frac{6}{d}}b$, v is the root of degree exactly d (not less) on F
All these twists are isomorphic to E (F_{q^d})
The twists possible (either quadratic or with higher degree) are grouped in the following table.
But we can say that for both cases: q = 1(mod d) is a necessary condition for these twists
We includes in the following table the isomorphisms
φ_d: E' ↦ E, with d is the degree of the twists

TABLE I
KIND OF TWIST

d	P∈E	P∈E'	E	E'	φ_d
2	(x,y)	$(vx, v^{\frac{3}{2}}y)$	$y^2 = x^3 + ax + b$	$y^2 = x^3 + v^2ax + v^3b$	$(v^{-1}x, v^{-\frac{3}{2}}y)$
3	(x,y)	$(v^{\frac{1}{3}}x, v^{\frac{1}{2}}y)$	$y^2 = x^3 + b$	$y^2 = x^3 + vb$	$(v^{-\frac{1}{3}}x, v^{-\frac{1}{2}}y)$
4	(x,y)	$(v^{\frac{1}{2}}x, v^{\frac{3}{4}}y)$	$y^2 = x^3 + ax$	$y^2 = x^3 + vax$	$(v^{-\frac{1}{2}}x, v^{-\frac{3}{4}}y)$
6	(x,y)	$(v^{\frac{1}{3}}x, v^{\frac{1}{2}}y)$	$y^2 = x^3 + b$	$y^2 = x^3 + vb$	$(v^{-\frac{1}{3}}x, v^{-\frac{1}{2}}y)$

In a field of characteristic different from 2 and 3, we can transform all the curves in twists, we just find a suitable v

B. Rational function

Lets E(k) be an elliptic curve of equation f(X,Y) = 0. The function g is zero of E(k), if g is a multiple of f, and we can define an equivalence relation on the ring k[E] as: k[X,Y]/(f). The field k(E) is the field of rational functions on E.
The function is rational over k(X,Y), if it set at least one point of E(k) in the form rational. For example, E(F_{q^k}) can be written as $\frac{g(X,Y)}{h(X,Y)}$ with $g(X, Y)$ and $h(X, Y)$ are two function on $E[F_{q^k}]$. And we can write g(X,Y)=$g_x(X)$+Y$g_y(Y)$ with g_x,$g_y \in F_{q^k}[X]$, as $Y^2 = X^3 + aX + b$ (equation of field of characteristic different to 2 and 3)
For a rational function $\frac{g(X,Y)}{h(X,Y)}$ the zeros of $g(X, Y)$ are called the zeros of the rational function, and the zeros of $h(X, Y)$ are its poles. The rational functions defined on an elliptic curve E, admit the number of zero equals to the number of pole (for more details see [8])

C. Divisors

A divisor is a universal concept that relate the zeros and poles with there order of multiplicities. For example, we can write a divisor D as follows:
D=$a_1[P_1]+a_2[P_2]+a_3[P_3]+a_4[P_4]+a_5[P_5]$, with a_1, a_2, a_3, a_4, a_5 ∈ Z are zeros or poles of points P_1, P_2, P_3, P_4, P_5, for an elliptic curve E.
For example $D = [2P] - 3[Q] - 2[P]$. But in this divisor [2P] and 2[P] are different. We called the first a zero of order 1 and the second a zero of order -2
A divisor is so a set generated by symbols [P]. We noted all divisors

by Div(E)
The degree of D is an integer that has the following value: deg($\sum_i a_i[P_i]$)=$\sum a_i$, and its sum is: sum($\sum_i a_i[P_i]$)=$\sum a_i P_i$.
We note all the set of divisors of degree 0 by Div^0
We say that a divisor D=$\sum_i a_i P_i$ is principal, if it is a divisor of degree 0 and if $sum(\sum_i a_i[P_i]) = O$
The set of divisors principal is noted Prin(E).
Two divisors D and D' are equivalent if their difference is an element of Prin(E).
The divisor of the rational function f is defined as follows:
$div(f) = \sum_{p \in E(k)} ord_p(f)[P]$ with $ord_P(f)$, is the order of f at point P (zeros or poles). And we know that any rational functions has degree 0 by [8]
For the divisor D=$\sum_i a_i P_i$ and the function rationale f we have: f(D)=$\prod f(P_i)^{a_i}$, we only requires that we should have the support of D and div(f) to be disjoint
Example of divisors for a known rational function
To find a divisor for an equation of the rational function $ax+by+c$ (equation of a line which pass through the points P_1, P_2 of an elliptic curve E, with $P_1 \neq \pm P_2$). This line intersects the curve in a third point P_3. So the function f(x,y)=$ax + by + c$ has tree zeros at the points P_1, P_2, P_3 and a pole of order 3 in point O. Because, f has tree zeros and since it is a rational function (degree 0), it has necessarily a pole of order 3 in (O), then, div(f)=$P_1 + P_2 + P_3 - 3O$ i.e $(ax + by + c) = P_1 + P_2 + P_3 - 3O$
For the equation of the vertical line ($x - x_Q = 0$) that passe through Q and -Q. By the same reasoning as above we have: $div(x - x_Q) = [Q] + [-Q] - 2O$

D. Pairing

A pairing is a bilinear map that takes two points on an elliptic curve and output an element of the group multiplicative of n-th roots of unity. The pairing satisfies the following properties: bilinear, alternative and non-degenerate.
Considering E(k)[r] (points of r-torsion on elliptic curve E)
Bilinear:: $\forall$ P_1,P_2,Q_1, $Q_2 \in E[r]$, $c_r(P_1 + P_2, Q_1) = c_r(P_1, Q_1) \cdot c_r(P_2, Q_1)$ and $c_r(P_1, Q_1 + Q_2) = c_r(P_1, Q_1) \cdot c_r(P_1, Q_2)$
Identity: $\forall P \in E[r]$ $c_r(P, P) = 1$
Alternate: $c_r(P, Q) = c_r(Q, P)^{-1}$
Non-degenerate: If $\forall P \in E[r]$ $c_r(P, Q) = 1$ then $Q = O$ and if $\forall Q \in E[r]$ $c_r(P, Q) = 1$ then $P = O$
It is clear from these properties that we have $c_r \in \mu_r$ (set of the r^{th} roots of unity), since $c_r(P, Q)^r = c_r(rP, Q) = c_r(O, Q) = 1$
Among the pairing we cited: Weil, Tate, Ate, η. But in the implementations cryptographic we often use Weil and Tate.
The Tate pairing is two times faster than Weil [9]. Although, this latter is more desirable for the security and as in cryptography we are more interested to the security. Then, it is better to use Weil pairing. In this study we will see and we will be convinced that the Tate pairing is less secure than Weil.

1) Explicit formula for the pairing: Before giving the explicit formulas for each pairing, we demonstrate firstly the following equivalence:
$[P] - [O]$ and $[P + R] - [R]$ are equivalent [7] for any point R on an elliptic curve.
However according to what we see above we have: div(U)=[P]+[R]+[-(P+R)]-3[O] and
div(V)=[-(P+R)]+[P+R]-2[O], with U is the line that passes through the points P, R, -(P+R). And V is the line that passes through the points P+R and -(P+R).
And then: $[P] - [O] = [P + R] - [R] + div(\frac{U}{V})$ □
Thus, we can write the divisor D_P by one of the expression $[P]-[O]$ or $[P + R] - [R]$

2) Tate Pairing: Let r be an integer which is prime with the characteristic of F_q.
Let k=F_{q^k} be a field that contains all roots of unity of order r, and P $\in E(k)[r]$, Q $\in$ E(k).
Let: D_P and D_Q be two divisors of degree 0 with disjoint support, f_{D_P} a function such that: $div(f_{D_P}) = rD_P$
The Tate pairing is the application :
t_r:E(k)[r]×E(k)/rE(k) $\rightarrow k^*/(k^*)^r$
(P,Q)$\rightarrow t_r(P, Q)=f_{D_P}(D_Q)$ modulo $(k^*)^r$
If we take $D_P = [P] - [O]$, $D_Q = [Q + T] - [T]$ (T is of our choice). So, D_P and D_Q have disjoint supports, then:
$t_r(P, Q)=\frac{f_P(Q+T)}{f_P(T)}$. But for this pairing to have an exact value, it must be defined as follows: $t_r(P, Q) = (f_{D_P}(D_Q))^{(q^k-1)/r}$

3) Weil Pairing: Let: P, Q $\in E[r]$ and D_P, D_Q two divisors of degree 0 with different support. So we can take D_P to be equivalent to $[P] - [O]$ and D_Q equivalent
to [Q + S]-[S], with S is chosen such that P, O, Q+S, S are points different to each others.
As P and Q $\in$ E[r], then rD_P and rD_Q are two principals divisors. So, there are two principal function f_P and f_Q such that: $divf_P = rD_P$ and $divf_Q = rD_Q$
The Weil pairing is defended as follows:
e_r:$E[r] \times E[r] \rightarrow \mu_r$ (μ_r is the set of the r^{th} root of the unity)
such that: $e_r(P, Q) = \frac{f_{D_Q}(D_P)}{f_{D_P}(D_Q)}$
Calculate the pairing is ineffective until the invention of the algorithm of Miller in 1986, but until present we haven't a practical method to implement easily the pairing.

4) Algorithm of Miller: This algorithm compute $f_{D_P}(Q)$ using the following method:
For a divisor $D_P = [P + R] - [R]$ and an integer positive i, we define the following divisor:
$D_i = i[P + R] - i[R] - [iP] + [O]$ which is principal, so there is a rational function f_i such that $div(f_i) = D_i$.
For i=r we have $D_r = r[P + R] - r[R] - [rP] + [O] = rD_P$. Because, rP=O so $f_r = f_{D_P}$ the problem is summarized so in the calculation of $f_r(Q)$
To elucidate this: given $f_{r_1}(Q)$ and $f_{r_2}(Q)$ for an integer positive r_1 and r_2, and the points r_1P, r_2P, $(r_1 + r_2)P$. We want to calculate $f_{r_1+r_2}$
By definition we have: $D_{r_1} = r_1[P + R] - r_1[R] - [r_1P] + [O]$ and $D_{r_2} = r_2[P + R] - r_2[R] - [r_2P] + [O]$,
$D_{r_1+r_2} = (r_1 + r_2)[P + R] - (r_1 + r_2)[R] - [(r_1 + r_2)P] + [O]$
Defining the following equations: $aX + bY + c = 0$ as a line passed through two points r_1P and r_2P (if $r_1 = r_2$ we obtain an equation of the tangent). And posing $L_{r_1P,r_2P}(X, Y) = aX + bY + c$.
Let $X + d = 0$ be the vertical line that passes through the point $(r_1 + r_2)P$ and defining the function $V_{(r_1+r_2)}(X, Y) = X + d$.
Using what we have mentioned previously we have:
$div(L_{r_1P,r_2P}) = [r_1P] + [r_2P] + [-(r_1 + r_2)P] - 3O$
$div(V_{(r_1+r_2)}) = [(r_1 + r_2)P] + [-(r_1 + r_2)P] - 2O$
So, $D_{r_1+r_2} = D_{r_1} + D_{r_2} + div(L_{r_1P,r_2P}) - div(V_{(r_1+r_2)})$.
Which imply $f_{(r_1+r_2)}(Q) = f_{(r_1)}(D_Q) \cdot f_{(r_2)}(D_Q) \cdot \frac{L_{r_1P,r_2P}Q}{V_{(r_1+r_2)}Q}$
As we have $divf_{r_1+r_2}(Q) = divf_{r_1}(Q) + div\ f_{r_2}(Q) + div\ \frac{L_{r_1P,r_2P}}{V_{(r_1+r_2)}}$
Remembered that our aim is to calculate $f_r = f_P$ using the following algorithm that takes as output
$\sigma(f_{(r_1)}(Q), f_{(r_1)}(Q), r_1P, r_2P, (r_1 + r_2)P) = f_{(r_1+r_2)}(Q)$

Algorithm of Miller

Let k be an integer, the algorithm works in an iterative manner. It takes in its output the rational function (recursive) f_k which is generated from the following divisor:
$f_k = \frac{(P+R)^k}{R^k(kP)}$ [10] (since $D_k = k[P + R] - k[R] - [kP] + [O]$). For k=r, $f_r = f_P$. Theses iterations can be calculated from the relation given above i.e
$f_{(r_1+r_2)P} = (f_{(r_1)P} \cdot f_{(r_2)P} \cdot \frac{L_{(r_1P,r_2P)}}{V_{(r_1+r_2)P}})$, from which we deduce:

$f_{2k} = (f_k)^2 \cdot \frac{T_{kP}}{V_{2kP}}$ with T and V are respectively the tangent and the vertical to the point kP.
Before expressing the algorithm of Miller, we express the integer r which is the order of the points, in the basic binary so: $r = \sum_{i=0}^{i=m}(r_i 2^i)$, with the fact that $(f_0) = 1$ and $(f_1) = (\frac{V_{P+R}}{L_{P,R}})$
It is clear that $(f_0) = 1$ and for (f_1) we have: $div(aX + bY + c) = [P] + [Q] + [R] - 3O$ (aX+bY+c is the line passing by P,Q,R), and $div(X - X_Q) = [Q] + [-Q] - 2O$. Then: $\frac{div(aX+bY+c)}{div(X-X_R)} = [P] + [R] - [-Q] - [O]$ but $P + R = -Q$, so $[P + R] - [P] - [R] + [O] = (\frac{V_{P+R}}{L_{P,R}})$ = (f_1). Which proves very well the relationship and the recurrence for i = 1.

Miller(P, Q, r)

Input: r = (r_n...r_0)(binary representation),
P $\in E[r](\subset$ E(F_q)) and Q $\in G_1(\subset E(F_{q^k}))$
Output: $f_{r,P}(Q) \in G_3$ ($\subset F^*_{q^k}$)
T $\leftarrow$ P
$f_1 \leftarrow 1$
for i = n - 1 to 0 do
1: T $\leftarrow$ [2]T
$f_1 \leftarrow {f_1}^2 \times \frac{l_1(Q)}{v_1(Q)}$
l_1 is the tangent to the curve in T.
V_1 is the vertical to the curve in [2]T.
2: if r_i=1 then
$f_1 \leftarrow f_1 \times \frac{l_2(Q)}{v_2(Q)}$
l_2 is the line passing through the point TP
V_2 is the vertical to the point P + T.
Output: Return f_1

E. Problem Bilinear of Diffie Hellman

Before presenting the equivalence between the problem CDHP and the problem BHD, we remember the following problems:
Problem of Discreet Logarithm: DLP
Given P and aP, can we find a?

Problem calculator of Difiie Hellman: CDHP
It is the problem that interests us in this study: Given P, aP, bP, can we find or rather calculate abP?

Problem Decisional of Difiie Hellman: DDHP
Given P, aP, bP, cP, can we say that abP = cP?. But this problem can be solved in polynomial time after using the pairing, for example if we prove that e(P,cP) = e(aP,bP) so abP = cP.

Problem Bilinear of Diffie Helleman: BDHP
Given P, aP, bP, cP can we calculate $e(P,P)^{abc}$?

F. Overview on some technique proposed to cryptanalysis such problem

According to [11], Verheul, Galbraith , Hess and Vercauteren, Satoh, have make their search in this area. We can summarize their result in the following theorem
Theorem [11]: Let e : $G_1 \times G_2 \longrightarrow G_T$ be a non-degenerate pairing between groups of prime order r. Then the following statements are equivalent.
(a) One can solve LPI and RPI in polynomial time.
(b) One can solve LPI in polynomial time and any homomorphism $G_1 \longrightarrow G_2$ can be computed in polynomial time.
(c) One can solve RPI in polynomial time and any homomorphism $G_2 \longrightarrow G_1$ can be computed in polynomial time.
So according to [11] if we have these equivalence we can solve the CDHP. With the fact that
Definition 3 of **RPI** (Right Pairing Inversion problem): Given P $\in G_1$ and $\zeta \in G_T$, find Q $\in G_2$ satisfying e(P,Q) = ζ.
Definition 4 of **LPI** (Left Pairing Inversion problem): Given Q $\in G_2$ and $\zeta \in G_T$, find P $\in G_1$ satisfying e(P,Q) = ζ.
Definition 5 of **GPI** (General Pairing Inversion problem): Given $\zeta \in G_T$, find (P,Q) $\in G_1 \times G_2$ such that e(P,Q) = ζ.
But if we examine very well such idea we can see that its hard (we refer the interest to [14], to more examen the difficulty of such methods).

III. Our Idea

Before exploding our idea we need to show firstly the linearity of some diffeomorphism.

A. Linearity

1) First case: Linearity of some distortions : Firstly ϕ is linear if $\phi(aP)$ = a$\phi(P)$ for all a > 0.
The distortion $\phi(x,y) = (-x, iy)$ and $\phi(x,y) = (\zeta x, y)$ are linear, since:
Using the recursion we can show this propriety. For example for $\phi(x,y) = (-x, iy)$, we have:
Firstly, the linearity is true for a = 1. We would to show it for all a > 0
Suppose that it is true for a-1 i.e : $\phi((a-1)P) = (a-1)\phi(P)$ and we would to show that $\phi(aP) = a\phi(P)$
But to demonstrate this we must prove that:
$\phi(P + (a-1)P) = \phi(P) + \phi((a-1)P)$
We have: $P + (a-1)P = (x_P, y_P) + (x_{(a-1)P}, y_{(a-1)P}) = aP$
With ($\lambda_{aP} = \frac{y_{(a-1)P} - y_P}{x_{(a-1)P} - x_P}$, $x_{aP} = (\lambda_{aP})^2 - x_P - x_{(a-1)P}$, $y_{aP} = \lambda_{aP}(x_P - x_{aP}) - y_P$)
On the other hand we have $\phi(P) + \phi((a-1)P) = (-x_P, iy_P) + (-x_{(a-1)P}, iy_{(a-1)P})$
With $\lambda_{\phi(P)+\phi((a-1)P)} = \frac{iy_{(a-1)P} - iy_P}{-x_{(a-1)P} + x_P} = -i\lambda_{aP}$, so $x_{\phi(P)+\phi((a-1)P)} = (-i\lambda_{aP})^2 + x_P + x_{(a-1)P}$ = -x_{aP} and $y_{\phi(P)+\phi((a-1)P)} = -i\lambda_{aP}(-x_P + x_{aP}) - iy_P$ =iy_{aP}
So: $\phi(P) + \phi((a-1)P)$ = (-x_{aP},iy_{aP})
And since $\phi(P + (a-1)P) = \phi(aP) = (-x_{aP}, iy_{aP})$
We have very well $\phi(P + (a-1)P) = \phi(P) + \phi((a-1)P)$
And as we have assumed by induction that $\phi((a-1)P) = (a-1)\phi(P)$
So: $\phi(aP) = \phi(P + (a-1)P) = \phi(P) + \phi((a-1)P) = \phi(P) + (a-1)\phi(P) = a\phi(P)$. This clearly shows the linearity of this distortion
By the same method as above, we shows the linearity of the other distortion $\phi(x,y) = (\zeta x, y)$
Observation:
1. There are distortions which are not linear, for example the distortion $\varphi(x,y)$=(w $\frac{x^p}{r^{(\frac{2P-1}{3})}}, \frac{y^p}{r^{p-1}}$) which is suitable to the curve $y^2 = x^3 + ax$ defined on the fields F_{p^2}, $r^2 = a$, r$\in F_{p^2}$, $w^3 = r$, $w \in F_{p^6}$, is not linear
2. The distortions declared above are not the only ones that are linear, it may exist others.

2) Second case: Linearity of φ_d: For all the isomorphisms declared above [Table 1] we have checked their linearity. We can choose one among them to know how it works, for example φ_2
We still ruse the demonstration of recursion. But we give only its big lines and afterwards, it is simple to extract it
The parameters λ_t, $x_{(P+Q)_t}$, x_{P_t}, x_{Q_t} are reserved to the points of the twists
We must show that $\varphi_2(P + Q) = \varphi_2(P)$+ $\varphi_2(Q)$
As we have: $\lambda_t = \frac{v^{-(\frac{3}{4})}}{v^{-(\frac{1}{2})}}\lambda$=$v^{-(\frac{1}{4})}\lambda$

So, $x_{(P+Q)_t} = (v^{-(\frac{1}{4})}\lambda)^2 - v^{-(\frac{1}{2})}x_P - v^{-(\frac{1}{2})}x_Q = v^{-(\frac{1}{2})}x_{P+Q}$
And $y_{(P+Q)_t} = v^{-(\frac{1}{4})}\lambda(v^{-(\frac{1}{2})}x_P - v^{-(\frac{1}{2})}x_{P+Q}) - v^{-(\frac{3}{4})}y_P = v^{-(\frac{3}{4})}y_{P+Q}$
The relationship is therefore very simple to extract.

B. Compute of CDHP

Our idea to solve CDHP is to use the pairing, since the first use of the pairing is in cryptanalysis. However in 1993 Menezes-Okamoto-Vanstone used the Weil pairing to reduce the discrete logarithm problem in finite field to elliptic curve. One year after Frey Ruck proposed a similar attack using Tate. Also in this work we use this later to solve the CDHP.
The security of several cryptosystem is based on Computational Diffie Helman Problem for very large integer (greater than 256 bit for an elliptic curve). Can we solve this problem? the answer may be yes. The idea is very simple using Tate pairing (or rather the rational function associated to this pairing). Given P, aP and bP, trying to calculate abP. We choose the Tate pairing and we proceed as follows:
Firstly, we compute the order of the point P, aP, bP.
Then we have $t_{r_{aP}}(aP, bP)$=$(f_{D_{aP}}(D_{bP}))^{(q^k-1)/r_{ab}}$. But this expression may be trivial, according to the following properties:
Propriety 3 (Galbraith) [7]
Let $P \in E(F_q)[r]$, with r is relatively prime to q so:
$t_r(P, P) \neq 1$ if $k = 1$
And $t_r(P, P)$ = 1, for k > 1.

So: $t_{r_{aP}}(aP, bP) = t_r(P, P)^{ab} = 1$, for any integers a and b. Then this calculation is trivial.
But to remedy this problem we have the following property:

Propriety 4 (Veurheul)[7]
Let r be a prime, $P \in E(F_q)[r]$ and $Q \in E(F_{q^k})$ linearly independent to P, k > 0. So $t_r(P, P)$ is non-degenerate ie $\neq$ to 1

To elucidated this result to our case, we choose so one of the linear diffeomorfismes reported earlier (most convenient to the elliptic curve chosen) and we will have:
$t_{r_{aP}}(aP, \phi(bP)) = t_{r_P}(P, a\phi(bP)) = t_{r_P}(P, \phi(abP))$ (by the bilinear of the pairing and the linear of the diffeomormism). This equality can not be trivial, since aP, $\phi(bP)$, and also P, $\phi(abP)$ are linearly independent.
So $t_{r'}(aP, \phi(bP)) = t_r(P, \phi(abP))$ is not trivial (r' and r are respectively the order of aP and P).
Which implies that
$(f_{D_{aP}}(D_{\phi(bP)}))^{\frac{q^k-1}{r'}} = (f_{D_P}(D_{\phi(abP)}))^{\frac{q^k-1}{r}}$
Then:

$$(f_{D_{aP}}(D_{\phi(bP)}))^{\frac{r}{r'}} = f_{D_P}(D_{\phi(abP)}) \quad (1)$$

Exploitation of the idea

As we have $f_r = \frac{(P)(P)}{(2P)}\frac{(P)(2P)}{(3P)}.....\frac{(P)((r-1)P)}{(rP)} = f_{D_P} = f_P$
We must simplify only this expression. In the numerator figure the lines that link to two points different, such that $L_{(P),(2P)} = (P)(2P)$ which is a line that links the two points P and 2P. And we have in the denominator the vertical line that passes through one point (tangent). For example $V_{2P} = (2P)$ is a vertical line that passes through 2P. By Maple or by another software (logiciel), we calculate P, 2P ,....., rP. And after it is easy to find the corresponding equation of lines for each numerator, and that of denominator. By a suitable programming (or by hand ... if r is small), we simplify the expression of f_P taking into account that $Y^2 = X^3 + eX + f$ for example (equation of a chosen elliptic curve). We simplify each degree of Y that exceeds 2, in the end we get a formula of the form:

$$f_P = \frac{f_{P_{nu_X}} + Y f_{P_{nu_Y}}}{f_{P_{de_X}} + Y f_{P_{de_Y}}} \quad (2)$$

With $f_{P_{nu_X}}$ and $f_{P_{nu_Y}}$ are in k[X] (k is the chosen field) and of degree less than or equal to r.
Returning to (1) we associate to $\phi(abP)$ the coordinate of $(X_{\phi\phi(abP)}, Y_{\phi(abP)})$. After the algorithm of Miller, we calculate $f_{D_{aP}}(D_{bP})$ after having replaced D_{bP} by its expression, for example $D_{bP} = [bP + R] - [R]$ with R is of our choice.
It is easy to apply the algorithm of Miller to $f_{D_{aP}}(D_{bP})$, as aP, bP are given. After then, we calculate: $f_{D_{aP}}(D_{bP})^{\frac{r}{r'}}$.
But $D_{abP} = [abP] - [O]$ replacing this expression in (1) we find that:
$f_{D_P}(\phi(abP)) = (f_{D_{aP}}(D_{bP})^{\frac{r}{r'}})(f_{D_P}(O))$
Also according to the algorithm of Miller, we calculate $f_{D_P}(O)$. We then find that

$$f_{D_P}(\phi(abP)) = cte_1 \quad (3)$$

We replace $\phi(abP)$ by its coordinates in the expression of f_{D_P} which is (2) to find : $Y_{\phi(abP)}$ in function of $X_{\phi(abP)}$ using (3). Then we replace this expression in $Y^2 = X^3 + eX + f$ which gives us an equation of degree less than or equal to r and its solution is the $X_{\phi(abP)}$ that we seek.
Substituting this solution in the equation of elliptic curve, this gives us the expression of $Y_{\phi(abP)}$.
These coordinates are exactly the coordinates of $\phi(abP)$ which we want. Then we can easily calculate abP
But since for r greater than (> 12), we can not get to solve an equation of degree r. We can then use the following method:
We discuss this method according to the case:
1^{st} case: Assuming that r is even ie r=$2r''$ and if we return to $t_{r'}(aP, \phi(bP)) = t_r(P, \phi(abP))$. Exposing by r'', we find: $(t_{r'}(aP, \phi(bP)))^{r''} = (t_r(P, \phi(abP)))^{r''}$, which is still equivalent to
$(t_{r'}(aP, \phi(bP)))^{r''} = (t_r(r''P, \phi(abP)))$. So $(f_{D_{aP}}(D_{bP}))^{r''} = f_{D_{r''P}}(\phi(abP))$
We proceed as above, therefore we find:

$$f_{D_{r''P}}(\phi(abP)) = (f_{D_{aP}}(D_{bP}))^{r''}(f_{D_P}(O)) = cte_2 \quad (4)$$

But as $f_{D_{r''P}}$= $\frac{(r''P)(r''P)}{(2r''P)}$ (because 2r"P=O), so

$$f_{D_{r''P}} = f_{r''P} = y - m_{r''P}x - \beta_{r''P} \quad (5)$$

Since $V_{2r''P} = 1$ (2r"P=O).
With the fact that $\beta_{r''P} = y_{r''P} - m_{r''P} \cdot x_{r''P}$ and $m_{r''P} = \frac{3x^2_{r''P}+1}{2y_{r''P}}$
We replaces in the expression (5) the point $\phi(abP)$ with there coordinate $y_{\phi(abP)}$ and $x_{\phi(abP)}$
In the end we substitute the founded expression in (4) to find for example $y_{\phi(abP)}$ in function of $x_{\phi(abP)}$ (or reverse). After having substitute the founded expression in the expression $Y^2 = X^3 + eX + f$ (equation of the chosen elliptic curve). We find very well the equation (linked to $x_{\phi(abP)}$) of tree degree which is resolved, may be by hand or with a software. After calculating $x_{\phi(abP)}$ we replacing it in the equation of the elliptic curve to extract $y_{\phi(abP)}$.
So the coordinate ($x_{\phi(abP)}$,$y_{\phi(abP)}$) are exactly the coordinate of $\phi(abP)$, after it is easy to extract abP .
2^{nd} case: If r is odd which is a case always meted, so we do as follows:
We discuss also this case according to the case
First case: r is factorial ie it is not prime, so we have: r = $r''r'''$. With one of the factors is very large, assuming that is r'' (so r''' should be small)
Then exponent by r'' we have: $(t_{r'}(aP, \phi(bP)))^{r''}$ =

$(t_r(P,\phi(abP)))^{r''}$ which imply that
$f_{r'''}(D_{\phi(abP)}) = (t_{r'}(aP,\phi(bP)))^{r''}$
So, if we can simplify
$f_{r'''} = \frac{(r''P)(r''P)}{(2r''P)}\frac{(r''P)(2r''P)}{(3r''P)}.....\frac{(r''P)((r''r'''-1)P)}{(r''r'''P)}$, we can arrived at the result, but this is linked to r'''
If not, we can do otherwise (pursued for example the following method)
Second case: r is not factorial ie r is prime, it is the most worse case and the most hard to break.
We search for a point Q in E(k) this point is not in E [r], with condition that P-Q and Q have an order even. If we have this we can resolve the problem, since:
Supposing for example that the order of P-Q is 2k and that of Q is $2k'$. In addition assuming for example that $k > k'$ so k=$k'k''$.
Returning now to the equation: $t_{r'}(aP,\phi(bP))$ = $t_r(P,\phi(abP))$
So $t_{r'}(aP,\phi(bP))$ = $t_r(P-Q+Q,\phi(abP))$ = $t_{2k}(P-Q,\phi(abP))$ $t_{2k'}(Q,\phi(abP))$
Exposing by k imply that: $(t_{r'}(aP,\phi(bP)))^k$=$(t_{2k}(P-Q,\phi(abP)))^k(t_{2k'}(Q,\phi(abP)))^k$
The term $(t_{2K}(P-Q,\phi(abP)))^k = t_{2k}(k(P-Q),\phi(abP))$ = $f_{k(P-Q)}(D_{\phi(abP)})$ is simplificative (it is an equation of two variable with degree 1). And for the second term i.e $(t_{2k'}(Q,\phi(abP)))^k$ we have: If k'' is divisible by 2 then we have: $(t_{2k'}(Q,\phi(abP)))^k = 1$, if not, it depends on k'' we can find the desired expression (more simplificative), but if not we should change the Q.
The third term $(t_{r'}(aP,\phi(bP)))^k$ = cte, since we know aP and bP. So persuading as above we can extract the coordinate $(x_{\phi(abP)}, y_{\phi(abP)})$

Existence of P-Q and Q with the desired order: Let E be an elliptic curve defined over F_q, then E(F_q) is a commutated group of rank equal to 1 or 2. So [12] E(F_q) $\simeq Z_{n_1} \oplus Z_{n_2}$ with $n_1 \setminus n_2$ and $n_1 \setminus$ q-1.
The following algorithm [12] is summarize to calculate n_1 and n_2.
Algorithm (Miller):
1. Calculate N = card(E(K)) (using Schoof's algorithm or one of its variants).
2. Take U, V at random from E.
3. Calculate s = ord(U); t = ord(V) (to do this we must know the factorization of N).
4. Calculate m = ppcm(s,t) and $\zeta = e_m(U,V)$ a root of unity.
5. Calculate d = ord(ζ), verified if md = N.
6. If it is true then n_1= d, n_2 = m. Otherwise return to 2.

So we chose P-Q and Q the points of order n_1 and n_2.
There is a strong probability that we can found n_1 and n_2 even. Since, we may find n_1 even (q-1 is even), as we search only in the corresponding U and V which can give this condition and if we find this, automatically the n_2 will be also even.

Numerate Application : To better understand our ideas we propose the following example:
This example has been proposed in the article of Bonneh Franklin
Choosing the curve $y^2 = x^3 + 1$ over the field F_{11} and P=(2,3) a point of this curve
Applying the method declared above, we must firstly find the order of P
As 2P=P+P=(2,3)+(2,3)
We have $m_{P,P} = \frac{3x^2}{2y} = \frac{3\times4}{6} = \frac{12}{6} = 2$
Then $x_{2P} = 2^2 - 4 = 0$
And $y_{2P} = 2(2) - 3 = 1$ so $\boxed{\text{2P = (0,1)}}$
3P=2P+P=(0,1)+(2,3)
$m_{2P,P} = \frac{3-1}{2-0}$=1
$x_{3P} = 1^2 - 0 - 2 = -1 = 10$
And $y_{3P} = 1(2-10) - 3 = -11 = 0$ so $\boxed{\text{3P = (10,0)}}$
4P=2P+2P=(0,1)+(0,1)
$m_{2P,2P}$ = 0
Then $x_{4P} = 0$
And $y_{2P} = 10$ so $\boxed{\text{4P = (0,10)}}$
5P=4P+P=(0,10)+(2,3)
$m_{4P,P} = \frac{10-3}{0-2}$=$\frac{7}{9} = \frac{7\times5}{9\times5} = 2$
$x_{5P} = 2^2 - 0 - 2 = 2$
And $y_{5P} = 2(0) - 3 = 8$ so $\boxed{\text{5P = (2,8)}}$
For 6P = 5P+P we have $x_{5P} = x_P = 2$
And $y_{5P} \neq y_P$ therefore necessarily $\boxed{\text{6P = O)}}$ then P have ordr 6
We have, 6 doesn't divide 11, but 6 $\setminus 11^2 - 1$. So we can grouping the calculate in the field F_{11^2}
Our goal in this exercise is to find a point 20P from the points 4P and 5P
Using the diffeomorphism $\phi(x,y) = (\zeta x, y)$ which is suitable to the curve used, so we have:
$t_3(4P,\phi(5P)) = t_6(P,4\phi(5P)) = t_6(P,\phi(20P))$ (according to the propriety: bilinear of the pairing and the linear of distortion)
As P has an order even 6=2.3 so exposing by 3 we find:
$t_3(4P,\phi(5P))^3 = t_6(P,\phi(20P))^3$
Firstly, according to [7] we have $\zeta = \frac{11-1}{2}(1 + 3^{(\frac{11+1}{4})}) = 5(1+5i)=5+3i$
So : $\phi(5P) = (\zeta x_{5P}, y_{5P}) = ((5+3i)2, 8)$ = (10 + 6i,8)
Without passing by the algorithm of Miller we can calculate $t_6(4P,\phi(5P))^3$, because it is equal to $t_6(12P,\phi(5P))$ = $t_6(O,\phi(5P)) = 1$, since f_0 = 1
And then $f_{3P}(D_{\phi(20P)}) = 1$
But 3P has order 2
So $f_{3P} = f_2 = \frac{(3P)(3P)}{6P} = \frac{T_{3P}}{V_{6P}}$
As 6P = O, $V_{6P} = 1$ and $T_{3P} = V_{3P} = x - x_{3P}$ = x-10 = x+1
In addition we have $f_{3P}(D_{\phi(20P)}) = \frac{f_{3P}(\phi(20P)}{f_{3P}(O)}$ = 1
Since $f_{3P}(O)$ = 1 so $f_{3P}(\phi(20P)) = 1$
Then $x_{\phi(20P)} + 1 = 1$ imply $x_{\phi(20P)} = 0$
Which implies that $y_{\phi(20P} = 1$ or $y_{\phi(20P} = -1 = 10$ because $y^2 = x^3 + 1$
Then $\phi(20P) = (0,1)$ or $\phi(20P) = (0,10)$
So $20P = (0,1)$ or $20P = (0,10)$ since $\phi(20P) = (\zeta\ x_{20P}, y_{20P})$ then $20P = (\zeta^2\zeta\ x_{20P}\ ,\ y_{20P})$ = (x_{20P} ,y_{20P}) as $\zeta^3 = 1$
We have then $20P = (0,1)$ or 20P = (0,10) =4P
The case (0.10) is excluded, because we can not find from aP and bP an abP = aP or to bP
So 20P = (0,1) = 2P which is true, since 20P = 18P+ 2P= O+2P = 2P

C. From BDH to CDHP

Always with Tate, we can answer the question posed in the article of Bonneh Franklin [1], which is: can we go from BDH to CDHP? Yes, the answer is summarized as follows:

Given P,aP,bP,cP and $t(aP,bP)^c = cte$ can we find for example abP?
As: $t(aP,bP)^c = t(P,P)^{abc} = t(P,P)^{cab} = t(cP,abP) = cte$
If cP has small order r (cP can be large so the order of cP can be small), we have therefore:
t(cP,abP)=$f_{D_{cP}}(D_{abP}) = cte$
In this case we calculate by Miller only $f_{D_{cP}}(O)$ so:

$$f_{D_{cP}}(abP) = cte f_{D_{cP}}(O) = CTE \tag{6}$$

We must so write $f_{D_{cP}}$ in the following form:
$f_r = \frac{(cP)(cP)}{(2cP)}\frac{(cP)(2cP)}{(3cP)}.....\frac{(cP)((r-1)cP)}{(rcP)} = f_{D_{cP}} = f_{cP}$
By the same procedure as we mentioned above, we simplify the expression $f_{D_{cP}}$ to obtain an expression as follow:
$f_{cP} = \frac{f_{cP_{nu_X}} + Y f_{cP_{nu_Y}}}{f_{cP_{de_X}} + Y f_{cP_{de_Y}}}$
We replace the coordinates of abP=(X_{abP}, Y_{abP}) in this expression After (6) we get the coordinates of $Y_{\phi(abP)}$ according to that of $X_{\phi(abP)}$. In the equation of the curve we replace the Y_{abP} and so

we find an equation of degree at most r (its solution depends on the value r, we can even accepted an equation of degree < 20). Its solution is $X_{\phi(abP)}$ that we search, so it is easy to calculate $Y_{\phi(abP)}$. Then we can extract X_{abP} and Y_{abP}.

But if r is not small, according to the parity of r and pursuing the method stated above, we can extract ($X_{\phi(abP)}$,$Y_{\phi(abP)}$) and then (X_{abP},Y_{abP})
Similarly we calculate acP, bcP □

D. Recap

As we can see, to cryptanalysis CDHP and BDHP we are linked sequently on the following condition:

1) The need of an isomorphism linear (section III.A) convenable to the curve used
2) The parity of the order of the point used in the elliptic curve, since an odd order (precisely a prime order) is very strong to be cryptanalyst (section III.B)
3) The order of the elliptic curve, however the composite order may serve the cryptanalysis (the last Algorithm of Miller)

We will add this condition to the following one mentioned in the literature [13]:

1) # E(F_q) should have a sufficiently large prime factor n to resist the parallelized Pollard ρ-attack;
2) # E(F_q) $\neq$ q to resist Semaev, Smart and Satoh-Araki attacks on anomalous curves;
3) r doesn't divide q^k-1 for $1 <$ k < 30, to resit the MOV attack. This requirement is not inevitable. We can choose a larger q instead of large k to achieve security as well. However, a large q will slow down the speed of group operations.
4) Choosing F_{2^m}, m should be prime to resist some attacks on elliptic curve based on F_{2^m} where m is composite. (subffield basis)

Concrete observation : With the Weil pairing we can not reach to attack neither CDHP nor BDH since:
If $e_r(aP, \phi(bP)) = e_r(P, \phi(abP))$
So $\frac{f_{D_{\phi(bP)}}(D_{aP})}{f_{D_{aP}}(D_{\phi(bP)})} = \frac{f_{D_{\phi(abP)}}(D_P)}{f_{D_P}(D_{\phi(abP)})}$
And then $f_{D_{\phi(bP)}}(D_{aP}) \times f_{D_P}(D_{\phi(abP)}) = f_{D_{\phi(abP)}}(D_P) \times f_{D_{aP}}(D_{\phi(bP)})$
In one equation we have two unknown f_{abP} and D_{abP} which is infeasible to be resolved!!

E. PDL with MOV and FR

From which we stated above, we can attacked the CDHP and the BDH using Tate. We will see that this pairing may well serve us to attack the PDL by comparison with Weil.

1) Attack of Menezes-Okamoto-Vanstone (MOV attack): It is an attack that use Weil pairing. It functioned in the following manner:

A. Algorithm of Reduction MOV: **Input:** P $\in$ E(F_q) of order r, and Q $\in \prec P \succ$
Find k, minimal such that E[r] $\in E(F_{q^k})$
Find R $\in$ E[r] and calculate $\alpha = e_r(P, R)$
Calculate $\beta = e_r(Q, R)$
Calculate the discrete logarithm of β versus α in F_{q^k}
Output: the integer l such that Q=lP

2) Attack of Frey-Ruck: Similarly Frey and Ruck used the following method, to project the discrete logarithm problem of an elliptic curves to the finite field

B. Algorithm of Reduction of FR: **Input:** P $\in$ E(F_q) of order r and Q $\in \prec P \succ$
Find k, minimal such that $\mu(r) \in E(F_{q^k})$
Find R $\in E(F_{q^k})$ such that R is not belonging to $rE(F_{q^k})$ (and then $t_r(P, Q)$ is not trivial)
Calculate $\alpha = t_r(P, R)^{(q^k-1)/r}$ and $\beta = t_r(Q, R)^{(q^k-1)/r}$
Calculate l, the logarithm discrete of β versus α in F_{q^k}
Output: The integer l such that Q=lP

Algorithm A is more desirable than Algorithm B. Because, the calculations by Weil are twice times quick [9] by comparison with Tate pairing. So it is desirable to use algorithm B as it is two time quick than A. More than that, if we take a point P in E [r] and if we seek to a point Q in E [r] we will have:
$e_r(P, Q) = \frac{t_r(P,Q)}{t_r(Q,P)}$. That is to say, in the expression of Weil we use twice times Tate. So, the numerical result in the algorithm of Weil may be great than Tate. Since, it is twice time great than this later and thus, extract l from $e_r(P, Q)^l$ is difficult than extract it from $t_r(P, Q)^l$.
After all this, we shows that calculating PDL by Weil is more difficult by comparison with Tate

IV. Conclusion

The Tate pairing can serve very well the cryptanalysis for two reasons:

1) **The projection of discrete logarithm of the elliptic curve on the finite field is less rigid than Weil**
2) **The resolution of CDHP and BDH which are the heart of the security of the most cryptographic cryptosystem (for example the scheme basic of Bonneh and Franklin), can be trivial to attack using Tate pairing**

But this last condition is linked to:
1) The diffeomofism used (suitable to the curve used: Supersingular or Ordinary), 2) The parity of the order of the point used, 3) The #E (cardinal of the elliptic curve).
To block such attack we can use for example: the curve supersingular which has a distortion not linear. Or, the ordinary curve with embedding degree k, not divisible by neither the degree of the twist (2,3,4,6). We privilege so the prime embedding degree such as 11, 13, 17, 19... But as we need the twist to speed up the calculate of the Pairing, we can so block the attack after using the condition 2. Even if it is naturally and always utilized (according to the Pollard ρ-attack), but in this work we have demonstrate by an others methods that it's necessary to making it. More than that, we see that it is insufficient (condition 3) and we add to it the need of the curve of #E=rh or #E=r, with r and also h will be a great primes integers (with the fact that the complexity of Algorithm(Miller) i.e the second is related to the complexity of factorizing #E).
Thus, we proved that under this condition the Tate pairing is less secure than Weil (with this latter we can not attack neither CDHP nor BDH because we have always two unknown f_{abP} and D_{abP})

Acknowledge : We would like to thank Nadia El Mrabet for her helpful and comments. And the head of our laboratory Mr Aboutajdinne Driss.

References

[1] D. Boneh and M. Franklin. "Identification based Encryption from Weil Pairing", Appears in SIAM J. of Computing, Vol. 32, No. 3, pp.586-615, 2003.
[2] Joux. A one round for traipatite Deffie Hellman", Algorithmic number theory. International symposium No4, Leiden , PAYS-BAS (02/07/2000)

[3] A.Shikfa. ”Bilinear Pairing Over Elliptic Curve”, 2005. Available at: http://www-sop.inria.fr/maestro/MASTER-RSD/html/2004-05/05-master-shikfa.pdf
[4] R. Schoof : Elliptic curves overnite eld and the computation of square roots mod p, Mathematics of Computation, 44(1985), pp. 483- 494.
[5] A. Menezes, T. Okamoto, S. Vanstone. ”Reducing elliptic curve logarithms to logarithms in a fnite feld ” IEEE Tran. on Info. Th., Vol. 39, pp. 1639-1646, 1993.
[6] E. R. Verheul : Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems, Journal of Cryptology 17 (2004), pp. 277 - 296.
[7] Luther Martin. ”Introduction To Identity Based Encryption”. Available at: http://www.artechhouse.com/GetBlob.aspx?strName=Martin-238-CH04.pdf
[8] Andreas Enge. ”Elliptic Curve And Their Application To Cryptograpy: An introduction”. Kluwer Academic Publishers, 1999.
[9] J.C. Bajard and N. El Mrabet. Pairing in cryptography : an arithmetic point of view. In Advanced Signal Processing Algorithms, Architectures, and Implementations XVII, part of the SPIE Optics & Photonics 2007 Symposium (Proceedings of SPIE), volume 6697, pages 66970O.1-66970O.11, August 2007.
[10] Ben Lynn ”On the Implementation Of Pairing Based Cryptosystemes”, 2007(June). Thesis.
[11] John Boxall, Andreas Enge. Some security aspects of pairing-based cryptography. ANR Project PACE. Pairings and Advances in Cryptology for. E-cash. October 3, 2009.
[12] Thai Hoang. ”Application des Couplage En Cryptographie”, 12 July 2005. Available at: http://www.math.ucla.edu/ leth/stuff/couplage.pdf
[13] Zhaohui Cheng. Simple Tutorial on Elliptic Curve Cryptography. December 2004.
[14] S. Galbraith, and F. Hess, and F. Vercauteren. Aspects of Pairing Inversion. Cryptology ePrint Archive, Report 2007/256, 2007.