MATHEMATICA, Tome 50 (73), N° 2, 2008, pp. 177–186

NON SINGULAR ELLIPTIC CURVES, FROM THEORY TO APPLICATION. ALGORITHM ATTACKS DISCUSSIONS

NICOLAE CONSTANTINESCU

Abstract. Let E be an elliptic curve. Starting from its definition we create a set of restrictions which helps us to realize an implementation in a real system of the theories concerning the infeasibility of the ECDL problem. We also present the implementation methods to compute the necessary parameters in such a system.

MSC 2000. 11G07.

Key words. Elliptic curves, public key cryptography.

1. INTRODUCTION

Defining the elliptic curves means a crucial moment in developing computation methods of certain one-way functions. The practically implementations of the elliptic curves theory were possible only few years ago because they needs a big computing power. Without a computer it is practically impossible to compute elliptic curves parameters for fields which can be taken into consideration in practice. Therefore, being given a function $f : A \to B$ and $x \in A$ we say that f is a one-way function if $f(x) = y$ is easy to compute (by a computer, in polynomial time) and given y it is infeasible to find x, where infeasible refers to computation time which is not acceptable to be taken into consideration. This infeasible time is defined according to the application wherefore the elliptic curve is implemented. In this paper we will discuss the cases of generating efficient curves in order to implement them in practical systems.

2. FINITE FIELDS CALCULATION

In order to implements in computation systems, arithmetics in F_p are used, where p is a prime number, large enough to fulfill certain conditions required by the presented problem. The main problems under consideration refer to calculation in F_p: addition and multiplication. The latter is also the most difficult to solve. In order to create an efficient algorithm in [2, 3, 5] we present methods which start from a special form of p, i.e. $p = b^t - a$, where a has a sufficiently low value. The algorithm is based on multiplication subroutine, followed by reduction subroutine such as

```
Algorithm 1.
1 $q_0 \leftarrow \lfloor x/b^t \rfloor, r_0 \leftarrow x - q_0 b^t, r \leftarrow r_0, i \leftarrow 0$;
2 while $q_i > 0$ do
    • $q_{i+1} \leftarrow \lfloor q_i a/b^t \rfloor$, $r_{i+1} \leftarrow q_i a - q_{i+1} b^t$
```

```
        • $i \leftarrow i+1$, $r \leftarrow r+r_i$;
    3 while $r \geq p$ do $r \leftarrow r-p$.
```

In this way the reduction function uses only shift operations, addition and multiplication by a.
For the calculation of certain parameters found in the systems implemented in practice, RNSA (Residue Number System Arithmetic) is used. This concept is a rather old one and is based on CRT (Chinese Remainder Theorem). Therefore, starting from the integer p, as defined above, we choose p_i prime numbers, so that

$$\prod_{i=1}^{t} p_i > p^2 \tag{1}$$

We will represent an element x *modulo* p as a vector $(x_1, \ldots, x_t)$, where $x \equiv x_i \ (\ mod\ p_i)$. With this representation there can be made fast implementations on computing machines which use 32 or 64 bit-words. One of this ways wherefore such interpretation can be used is in trapdoor functions, applications of this kind being found in the algorithms of Public-Key systems.
Another efficient method of implementing modulo a large prime p arithmetics consist in using Montgomery representation [6] . Let b be the base in which the system works. R and t will be defined so that $R = b^t > p$ will be satisfied. We conclude from this that each element $x \in F_p$ is represented by $xR(mod\ p)$. The reduction operation required by the multiplication process is based on the result provided by Lemma 1

LEMMA 1. *Let be* $0 \leq y \leq pR$, $u = -yp^{-1}(mod\ R)$ *and*

$$x = \frac{(y+up)}{R}.$$

Then x *is an integer such that* $x < 2p$ *and* $x \equiv yR^{-1}(mod\ p)$

Also, the algorithm to compute the Montgomery reduction is:

ALGORITHM 2.

```
    1 $u \leftarrow -yp^{-1}(mod\ R)$
    2 $x \leftarrow (y+up)/R$
    3 if $x \geq p$ then $x \leftarrow x-p$
    4 return $x$.
```

In case of $y = (y_{2t-1}, \ldots, y_1, y_0)_{mod\ b} = y_{2t-1}b^{2t-1} + \ldots + y_1 b + y_0$ we can compute $yR^{-1}(mod\ p)$ in the following way:

ALGORITHM 3.

```
    1 for $i = 0$ to $t-1$
        • $u \leftarrow y_i p'\ (mod\ b)$
        • $y \leftarrow y + upb^i$
    2 $z \leftarrow y/R$
```

```
if $z \geq p$ then $z \leftarrow z - p$
return $z$.
```

These computations are made in case of $p' = -p^{-1}(mod\ b)$. In order to find this one it is necessary to compute $x^{-1}(mod\ 2^w)$.

Algorithm 4.

```
$y \leftarrow 1$
for $i = 2$ to $w$
    • if $2^{i-1} < xy(mod\ 2^i)$ then $y \leftarrow y + 2^{i-1}$
return y.
```

Another important aspect which must be taken into consideration is to solve quadratic equation in modulo p finite fields. These are necessary for computing a $y - coordinate$ of a point on the elliptic curve. It is found by starting from the $x - coordinate$. The equation type to be solved is: $x^2 \equiv a(mod\ p)$. In order to test that such an equation has a solution we will compute Legendre symbol $\left(\frac{a}{p}\right)$, whose value will be 1 in case a is a square modulo p or the value will be 0 in case $a \equiv 0(mod\ p)$. If we are in none of the above cases the Legendre symbol will be -1. The algorithm is presented below

Algorithm 5.

```
1 if $a \equiv 0\ (mod\ p)$ the return 0
2 $x \leftarrow a$, $y \leftarrow p$, $L \leftarrow 1$
3 $x \leftarrow x\ (mod\ y)$
4 if $x > y/2$ then
    • $x \leftarrow y - x$
    • if $y \equiv 3(mod\ 4)$ the $L \leftarrow -L$
5 while $x \equiv 0\ (mod\ 4)$ do $x \leftarrow x/4$
6 if $x \equiv 0\ (mod\ 2)$ then
    • $x \leftarrow x/2$
    • if $y \equiv \pm 3\ (mod\ 8)$ then $L \leftarrow\ -L$
7 $x = 1$ then return $L$
8 $x \equiv 3\ (mod\ 4)$ and $y \equiv 3\ (mod\ 4)$ then $L \leftarrow\ -L$
9 $temp \leftarrow x$
10 $x \leftarrow y$
11 $y \leftarrow temp$
12 go to 3.
```

In the computing machines, the representation are made in base 2, so that, in order to optimize the algorithms all necessary arithmetics must be translated in the finite fields F_{2^n}. Therefore, let be a quadratic equation

$$x^2 + \beta = 0 \tag{2}$$

in F_{2^n}, where its double square will be $x_0 = \beta^{2^{n-1}}$. A nontrivial quadratic equation $x^2 + x + \beta = 0$ will have, in F_{2^n}, a solution of the type $x_0 = \tau(\beta)$, where

$$\tau(\beta) = \sum_{j=0}^{(n-1)/2} \beta^{2^{2j}}. \tag{3}$$

Let be the matrix $T = (T_{ij})$.

$$\alpha^{1+2i} = \sum_{j=0}^{n-1} T_{ij}\alpha^{2^j},\ 0 \leq i \leq n-1, \tag{4}$$

where $(\alpha, \alpha^2, \alpha^{2^2},\ ..., \alpha^{2^{n-1}})$ is a normal base in F_{2^n} over F_2 and $\alpha \in F_2$. $Tr_{q|2}(\alpha_i\alpha_j) = 1$ iff $i = j$, $Tr_{q|2}(z)$ is the trace of $z \in F_q$ over F_2, with $q = 2^n$.

3. OPTIMIZATION IN ELLIPTIC CURVES ARITHMETICS

As the elliptic curves theory was founded a long time ago there is a large variety of interpretations and also ways to solve them. Let be an integral of type

$$\int \frac{\mathrm{d}x}{\sqrt{4x^3 - h_2x - h_3}}. \tag{5}$$

The inverse function of such an integral is called elliptic function. Let be two constants α_1 and α_2, a function and a double periodic function over R then Weierstrass function will be of the type

$$(\gamma')^2 = 4\gamma^3 - \alpha_1\gamma - \alpha_2. \tag{6}$$

This pair (γ, γ') will define a point on the curve

$$y^2 = 4x^3 - \alpha_1x - \alpha_2 \tag{7}$$

making an elliptic curve.

Definition 1. Let be $p > 3$ a prime integer. The elliptic curve $y^2 = x^3 + \alpha_1x + \alpha_2$, defined over Z_p is the set of solutions $(x, y) \in Z_p \times Z_p$ to the congruence

$$y^2 \equiv x^3 + \alpha_1x + \alpha_2 \pmod{p}, \tag{8}$$

where $\alpha_1, \alpha_2 \in Z_p$ are constants such that $4\alpha_1^3 + 27\alpha_2^2 \not\equiv 0 \pmod{p}$ together with a special point $\mathfrak{O}$ called the point at infinity.

As already described in section 2 the main problems are to define the addition of two points in such a field and to make multiplications by a given integer to a point on the elliptic curve. Let be A_1 and A_2 two points from the elliptic curve. The adding problem of these points can be split in two categories:

- $x_1 = x_2$ and $y_1 = y_2$
- other cases.

Lemma 2. *Let E denote an elliptic curve given by*

$$E : Y_2 + \alpha_1 XY + \alpha_3 Y = X^3 + \alpha_2 X^2 + \alpha_4 X + \alpha_6 \tag{9}$$

and let be $A_1 = (x_1, y_1)$ and $A_2 = (x_2, y_2)$ two points on the curve. Then

$$-A_1 = (x_1, -y_1 - \alpha_1 x_1 - \alpha_3). \tag{10}$$

Set

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ \gamma = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \tag{11}$$

where x_1, x_2 satisfy the condition $x_1 \neq x_2$ and, from this point we will have

$$\lambda = \frac{3x_1^2 + 2\alpha_2 x_1 + \alpha_4 - \alpha_1 y_1}{2y_1 + \alpha_1 x_1 + \alpha_3},\ \gamma = \frac{-x_1^3 + \alpha_4 x_1 + 2\alpha_6 - \alpha_3 y_1}{2y_1 + \alpha_1 x_1 + \alpha_3}. \tag{12}$$

In case of equality between x_1 and x_2 and $A_2 \neq -A_1$ the sum of these two points will be the point A_3 with the following coordinates:

$$x_3 = \lambda^2 + \alpha_1\lambda - \alpha_2 - x_1 - x_2,\ y_3 = -(\lambda + \alpha_1)x_3 - \gamma - \alpha_3. \tag{13}$$

Thus we will have

(1) $x_2 = x_1$ and $y_2 = y_1$. Then $A_1 + A_2 = \mathfrak{O}$
(2) Otherwise $A_1 + A_2 = B$, $B(x_3, y_3)$, where

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1 \tag{14}$$

and

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & A_1 \neq A_2; \\ (3x_1^2 + a)(2y_1)^{-1}, & A_1 = A_2. \end{cases} \tag{15}$$

In practice there are used the elliptic curves defined over a finite field F_q, which means that the study will be made on an abelian group. Let be s the number of points on an elliptic curve E, defined over F_q. Then $s = \#E(F_q) = q+1-t$, where $\#E(F_q)$ is named trace of Frobenius at q. Thus we can define Frobenius endomorphism as being

$$\varphi = \begin{cases} E(\overline{F}_q) \to E(\overline{F}_q) \\ (x, y) \to (x^q, y^q) \\ \mathfrak{O} \to \mathfrak{O}. \end{cases} \tag{16}$$

An approximation of the number of points on an elliptic curve is given by Hass's Theorem, in this way t must fulfill the condition

$$|t| \leq 2\sqrt{q}. \tag{17}$$

In order to compute the addition of two points on elliptic curve in finite fields one of the solutions will be Weil pairing implementation. Let be a finite field K and an elliptic curve defined over this field $E(K)$ with $E(m)$ its group of m-torsion points if $char(K) = p$ and $gcd(m, p) = 1$ then there are m^2 such points.

Lemma 3. *Let E be an elliptic curve over F_q and m is a prime which divides $\#E(F_q)$ but which does not divide $q-1$ and $m \neq char(F_q)$. Then $E(F_{q^k})$ contains the m^2 points of order m iff m divides $q^k - 1$*

According to [1] we will define Weil pairing as being $E(m) \times E(m) \to \gamma_m$ where γ_m is the group of mth roots of unity in $\overline{K}$. Thus, let be $B_1, B_2 \in E[m]$ and we choose a function g in E whose divisor satisfies

$$\text{div}(g) = \sum_{D \in E[m]} (B_1' + D) - (D) \tag{18}$$

with $B' \in E(\overline{K})$ such that $[m]B' = B$. In this case, we define e_m as:

$$e_m = \begin{cases} E[m] \times E[m] \to \gamma_m \\ (B_1, B_2) \to \frac{g(X+B_1)}{g(X)}. \end{cases} \tag{19}$$

In the case of the implementation in computing systems of a subfield curve, of the type F_{q^n}, n must be greater than 1 and the coefficients from F_q. We will define [8, 9] as a new addition method (and subsequently multiplication method by an integer) of two points on the elliptic curve using Frobenius Expansion. In equation (16) φ must satisfies equation

$$\varphi^2 - [t]\varphi + [q] = [0]. \tag{20}$$

In this way we will define an addition and multiplication method which will speed up the finding of the result. For the particular case where there is a subfield F_{q^n} provided that the multiplication factor, let it be K, to satisfy the property $|K| \leq \lfloor q/2 \rfloor$.

4. APPLICATION IN COMPUTING INFEASIBILITY OF ECDL

Since the development of the computing systems and the use of trapdoor functions, the implementations based on elliptic curves have been considered useful. Therefore, these have become the subject of research in order to obtain certain characteristic which will make their practical implementation efficient. The first condition described in the previous section was to use certain representations in finite fields in order to obtain solvable values of the points (their coordinates). The implementation in real systems is especially conditioned by the computation time necessary to find a multiplication coefficient. Thus, we define an elliptic curve E over a field F_q, n being the order of group $E(F_q)$ and P, Q elements in $E(F_q)$. The $ECDL$ problem is to find an integer so that $Q = [m]P$. In the previous section was presented a method of reducing the computation complexity using Weil pairing method. Based on Weil pairing on $E[n]$, there is a polynomial time reduction of the $ECDL$ on $E(F_q)$ to the DLP in F_{q^l}. The number q must be the smallest integer which fulfills the condition $q^l \equiv m(mod\ n)$ with $gcd(n, q) = 1$. In case q is prime, according to [7] there is a method to generate a subfield in which m will be computed, the study subfield being generated by p. Also, in [4] Pohlig and Hellman reduce the problem to a subgroup of prime power order in G. Let G be a group with an order divisible by a prime number p and $B = [K]A$. If the order of G is n, then the problem can be reduced to a subgroup of order p by solving $B' = [n']B = [K_0]([n']A) = [K_0]A'$ where

$$n' = \frac{n}{p^{c-1}}$$

and p^c is the largest power of p dividing n. In this way A' is a number of order p. Solving this problem we will find the value of K_0, by $K \bmod p$. Then, the obtained values by K mod $p^2, p^3, ..., p^c$ are computed. We assume that $K \equiv K_i \pmod{p^i}$ is known and $K = K_i + \lambda p^i$ for a fixed $\lambda \in Z$. Then $D = (B - [K_i]A) = [\lambda]([p^i]A) = [\lambda]H$ where D and H are known and H has the order

$$h = \frac{n}{p^i}.$$

The value of $\lambda \bmod p$ can be determinated from $K \bmod p$. Let be

$$h' = \frac{h}{p^{c-i-1}}$$

then we will obtain $\lambda \bmod p$ by solving the problem $D' = [h']D = [\lambda_0]([h']H) = [\lambda_0]H'$ where H' is a point of order p. Next, we will compute the points from a subgroup of order p. When $n \bmod p^c$ is computed for all p, prime divisors of n, we will obtain the final solution K using *Chinese Remainder Theorem.* The complexity of this attack is of order $\sqrt{2}n$. It will become infeasible when the order of the curve is large enough. In [1]it is described the elliptic curve with the following form:

(1) $G = (E, +)$, E is an elliptic curve modulo an integer prime number p, $\alpha \in E$ is a point with order a prime number

$$q = \frac{\#E}{h},$$

where $h = 1,\ 2\, or\, 4$

(2) $G = (E, +)$, E is an elliptic curve over a finite field F_{2^n}, $\alpha \in E$ is a point with order a prime number

$$q = \frac{\#E}{h},$$

where $h = 2\, or\, 4$

We noted $\#E$ as the number of points from elliptic curve E, with $p+1-2\sqrt{2}p \leq \#E \leq p + 1 + \sqrt{2}p$. We are able to attack the key based on elliptic curve using the Pollard Rho method in a subgroup of order q. In order to ensure the security of the cryptographic system based on elliptic curve, in [10] it is recommended to use $p \approx 2^{160}$ in case (1) and n=160 in case (2).

In order to define the subfield curves it is defined:

Definition 2. Let be E an elliptic curve over a finite field F_q where $N_n = \#E(F_{q^n}),\ n > 1$. For undetermined T we define Zeta function as being the series:

$$Z(E;T) = \exp\left(\sum_{n\geq 1}\frac{N_n}{n}T^n\right). \tag{21}$$

Theorem 1. *Let be E an elliptic curve over F_q and c_1 its trace of Frobenius at q, with $N_1 = q + 1 - c_1$. Then*

$$Z(E;T) = \frac{P(T)}{(1-T)(1-qT)}. \tag{22}$$

$P(T)$ it is defined in the following way:

$$P(T) = 1 - c_1T + qT^2 = (1-\alpha T)(1-\overline{\alpha}T), \tag{23}$$

where the magnitude of α is $\sqrt{q}$ and $P(T)$ is non-positive.

Wherefore, giving F_q, E and c_1 as in *Theorem* 1 it is possible to compute

$$\#E(F_q) = q^n + 1 - c_n,\ for\ any\ n \geq 1 \tag{24}$$

where

$$c_n = c_1c_{n-1} - qc_{n-2}. \tag{25}$$

The starting coefficient, c_0, is 0. Following the conditions imposed by the above descriptions there can be constructed elliptic curves with a good practical application using the following generating algorithm:

Algorithm 6.

```
1 Construct a random $E$, with its coefficients in $F_q$
2 Compute $\#E(F_q)$
3 Check the conditions above imposed for an elliptic curve (in order to
  be infeasible against attack). If failed then go to 1
4 attempt to factor $\#E(F_q)$ in feasible time. If failed then go to 1
5 if $\#E(F_q) = ab$ with $a < \overline{a}$ and $b$ is prime then $E$ is an "acceptable-
  elliptic-curve". Return $E$. If failed then go to 1.
```

Using such curves we can construct algorithms for information transfer in computer networks. Thus the information confidentiality is ensured in the case of potential listening of the communication channel. First of all, we take into consideration the assurance of the attack infeasibility, defining a function of information validity. The necessary condition will be that the necessary time to solve *ECDL* problem has to be longer than the time defined by the function of the validity information. It is observed a continuous development of the methods of reducing the *ECDL* problem for certain particular cases of problems whose solving needs polynomial time computation, thus new curve, according to the above definition.

4.1. Discussion about the necessary time to solve ECDL. This section describes the required times on a one-processor and multiprocessor machine in order to solve ECDL.

Single processor machine

At this point, we have to speak about the intractability of elliptic functions. For this reason, taking as starting point [11] we shall describe the necessary time to solve the elliptic curve discrete logarithm problem. The fastest algorithm known to date is Pollard method which takes about $\sqrt{2}\frac{\pi n}{2}$ steps to make an elliptic curve addition, where n represents the order of any generated point. In a software implementation, if we assume that an adversary can perform $4 * 10^3 MIPS$ in the field $Z_{2^{155}}$ [12] (a high performance machine) and that for every generated point he spends $\approx 2^{20}$ steps then we conclude that he can solve in one year, implementing an optimal algorithm,

$$[\frac{(4 * 10^9}{2^{20}})] * (60 * 60 * 24 * 365) \approx 2^{35}. \tag{26}$$

It is known that any new solution means a new point on the elliptic curve $E(Z_p)$ [13, 14].

Parallel machine case

In [15] it is illustrated the parallel implementation of Pollard method, where 1000 processors are used in an implementation in $Z_{2^{155}}$, and their conclusion is that 1500 years are necessary to find all points.

Acknowledgements. The author has been supported by Grant GAR 315/2007 with the Romanian Academy.

REFERENCES

[1] Blake, I. F., Seroussi, G. and Smart, N. P., *Elliptic Curves in Cryptography*, Cambridge University Press, 2002.

[2] Crandall, R., *Method and apparatus for public key exchange in a cryptographic system*, U. S. Patent Number 5159632.

[3] Lercier, R. and Morain, F., *Counting points in elliptic curves over F_{p^n} using Couveignes algorithm*, Rapport de Recherche LIX/RR/95/09.1995.

[4] Lercier, R., *Computing isogenies in F_{2^n}*, White Paper, 197–212.

[5] van Lint, J. T., *Introduction to Coding Theory*, Springer-Verlag, 1982.

[6] Montgomery, P. L., *Modular multiplication without trial division*, Math. Comp., **44**, 519–521, 1985.

[7] Pohlig, G. L. and Hellman, M. E., *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic signifiance*, IEEE Trans. Info. Theory, **24**, 1978, 106–110.

[8] Smart, N. P., *Elliptic curves over small fields of odd characteristic*, Journal of Cryptography, **12**, 141–151, 1999.

[9] Solinas, J. A., *An improved algorithm for arithmetic on a family of elliptic curves*, Springer-Verlag, 1997.

[10] Stinson, D. R., *Cryptography - Theory and Practice*, CRC Press, 2002.

[11] Certicom White Paper, *The elliptic curve cryptosystem for smart card*, Published: May 1998.

[12] Agnew, G., Mullin, R. and Vanstone, S., *An implementation of elliptic curve cryptosystem over $F_{2^{155}}$*, IEEE Journal on Selected Areas in Communications, **11** (1993), 804–813.

[13] Gao, S., von Zur Gathen, J., Panario, D. and Shoup, V., *Algorithms for Exponentiation in Finite Fields*, Journal of Symbolic Computation 2000, **29**, 879–889.

[14] Lim, C. and Lee, P., *A key recovery attack on discrete log-based schemes using a prime order subgroup*, Advances in Cryptography 1997, **1294** (1997), Springer-Verlag, Lecture Notes in Computer Science, 275–288.

[15] van Oorschot, P. C. and Wiener, M. J., *Parallel Collision Search with Cryptanalytic Applications*, Journal of Cryptology, **12** (1999) , Springer - Verlag, 1–28.

Received August 06, 2007

University of Craiova,
Computer-Science Department
A.I. Cuza street, no. 13, Craiova, Romania
E-mail: nikyc@central.ucv.ro