ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII "AL.I. CUZA" DIN IAŞI (S.N.)
MATEMATICĂ, Tomul LV, 2009, f.1

SECRET SHARING AND SHARED DIGITAL SIGNATURE USING ELLIPTIC CURVES

BY

RĂZVAN LIŢCANU* **and SILVIA PALAŞCĂ**

Abstract. This note is a short presentation of the elliptic curves cryptography. We illustrate this important aspect of the modern cryptography by a shared digital signature protocol, that adapts the classical elliptic curve digital signature scheme to a collective user and extends a distributed key generation protocol proposed by Tang [13].

Mathematics Subject Classification 2000: 14G50, 11T71, 11G07, 94A60.

Key words: public key cryptography, elliptic curves, Edwards curves, digital signature.

1. Introduction. Since the publication of the breakthrough article of Diffie and Hellman [2] in 1976, the public-key cryptography has gained the leading part in the theory and practice of the information security. Due to its strong points by respect to the classical symmetric cryptosystems, it became indispensable for secure communication in the Internet, for implementing smart cards etc. Moreover, the public key cryptography provides the foundation for secure digital signatures or key distribution for symmetric cryptosystems.

Nevertheless, an important disadvantage of the public key algorithms by respect to the classical ones is the dimension of the keys by respect to those of classical cryptosystems, for reaching a similar security level. The dimension of the keys requires, on one hand, larger memory, and more time for computations on the other hand. Finding public keys algorithms requiring smaller keys and being more efficient has been an important research challenge in this area. The first generation cryptosystems have been

*partially supported by CNCSIS Grant 1338/2007

in the dominant position in the field for more than twenty years, and are still widely used. However, significant progresses have been made and new algorithms have been proposed.

Most of the first cryptosystems using public keys were constructed around the integer arithmetics and the finite multiplicative group of a finite field (the typical example being $(\mathbb{F}_p^*, \cdot) = ((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$, where p is a prime positive integer). In 1986 KOBLITZ [6] and MILLER [8] suggested the construction of cryptographic algorithms using the group of points of an elliptic curve defined over a finite field. Due to the short key length, when compared to the safety level, this class of cryptosystems have become an important issue in modern cryptography.

This paper is a short presentation of some relevant geometric and arithmetic properties of elliptic curves, from the cryptographic point of view. We illustrate the use of elliptic curves in cryptography by basic cryptographic aspects like key generation and digital signature algorithms. Moreover, we are concerned with group-based protocols, when both the secret key and the signature of a message are shared by several participants. In particular, in this situation one must take care in validating a qualified group of participants and in detecting eventual cheaters.

Secret-sharing is a cryptographic protocol about a group of n users, each of whom have a part of a secret (a share). Having a group of entities with equal rights in encrypting/decrypting a message or signing a public message is common nowadays in every corporation. Any k persons from the group can put together their shares to reveal the secret, and any k-1 persons do not have this power. Secret sharing schemes were proposed independently by BLAKLEY [1] and SHAMIR [10].

In this paper the shared secret will be the secret key of a public key cryptosystem. The classical protocols are based on a trusted third party or on memorizing the secret keys and using them for decrypting. These presumptions can be eliminated in the case we describe by secret keys distribution and the creation of key "shadows", in fact, a modified version of a secret key. Such a scheme was proposed by TANG [13]. We extend this scheme by describing a shared digital signature protocol based on the elliptic curve digital signature algorithm [5].

2. Elliptic curves: a short review. The literature concerning the theory of elliptic curves is particularly rich. We review here only some

basic definitions and properties. For more details, the reader may consult, for example, [11].

Definition 2.1. Let K be a field. The nonsingular plane curve $E \subset K^2$ described by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

with $a_1, \ldots, a_6 \in K$, is called elliptic curve.

The equation 2.2 is called the Weierstrass equation of E.

If we embed the affine plane K^2 in the projective plane $\mathbb{P}^2$ by adding a line of points at infinity, then the projective curve $\overline{E}$ obtained by completing the curve E is described by the homogeneous equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{2.3}$$

$(a_1, \ldots, a_6 \in K)$.

One can notice that the projective curve $\overline{E}$ has one point at infinity: $O = (0 : 1 : 0)$.

The following theorem provides an alternative definition of an elliptic curve:

Theorem 2.4 ([11]). *Let (E, O) be a smooth projective algebraic curve of genus 1 over K with a distinguished K-rational point. Then there exists a regular map $\phi : E \to \mathbb{P}^2$ such that the curve E is isomorphic to the projective curve given by an equation (2.3), and $\phi(O) = (0 : 1 : 0)$.*

Conversely, every smooth projective curve given by an equation (2.3) has genus 1.

This allows us to give a more geometrical definition: an elliptic curve is a couple (E, O), where E is a smooth projective algebraic curve of genus 1 defined over K, and O is a distinguished K-rational point (called origin or base point).

Let E be an elliptic curve defined over the field K and O be the point at infinity. Then there exists a group structure on the set of K-rational points on $\overline{E}$, given by regular maps, such that O is the identity element of the group.

Conversely, if $\overline{E}$ is a nonsingular projective curve such that $\overline{E}(K)$ is endowed with a group structure given by regular maps, and O is the identity element, then $\overline{E}$ is isomorphic to an elliptic curve (2.3).

The composition law on the set $\overline{E}(K)$ can be described geometrically: let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two distinct points on an elliptic curve given by (2.2). Then the sum of P_1 and P_2 is defined as follows: one considers first the line through P_1 and P_2. According to Bézout's Theorem, this line intersects the elliptic curve in three points defined over the algebraic closure of K (counted with multiplicities). As two of these points, P_1 and P_2, are defined over K, the third point P_3 also is. Similarly, the line through O and P_3 intersects $\overline{E}$ in a third point of $\overline{E}(K)$ which is $P_1 + P_2$. We notice that in this description, if two points on the elliptic curve coincide, the line determined by these two points must be understood as the tangent line to the curve.

If the characteristic of the field K is different not 2 or 3, then the equation (2.2) can be reduced to

$$y^2 = x^3 + ax + b \ , \tag{2.5}$$

with $a, b \in K$, $\Delta := 4a^3 + 27b^2 \neq 0$. If $\operatorname{char} K = 2$, then the equation (2.2) can be reduced to either

$$y^2 + cy = x^3 + ax + b \text{ or } y^2 + xy = x^3 + ax + b \ , \ a, b, c \in K \tag{2.6}$$

and if $\operatorname{char} K = 3$ to

$$y^2 = x^3 + ax^2 + bx + c \ , \tag{2.7}$$

with $a, b, c \in K$ such that the cubic polynomial on the right hand side has no multiple roots.

For simplicity we suppose that the characteristic of K is not 2 or 3, hence the elliptic curve is described by the equation (2.5). Then, if $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$, then $P_1 + P_2$ has the coordinates

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1 \tag{2.8}$$

where

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if} \quad P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if} \quad P_1 = P_2 \end{cases}$$

We denote, for $P \in E$ and $n \in \mathbb{Z}, n > 0$,

$$nP = \underbrace{P + P + \ldots + P}_{n \text{ times}} .$$

If there exists a positive integer r such that $rP = O$ we say that P is a torsion point of E. If this is the case, then the order of P is the smallest positive integer r, such that $rP = O$. Notice that if K is a finite field, then all the points of E are torsion points.

Recently Edwards proposed another approach for explicitly describing the elliptic curves and the group composition law [3]. We briefly describe hereafter the curves known as Edwards curves. They are interesting from the point of view of this note because this approach provides a time-efficient addition formula.

Definition 2.9. The plane curve C_a described by the equation

$$x^2 + y^2 = a^2 + a^2x^2y^2 \ , \ a \in K^* \tag{2.10}$$

is called an Edwards curve.

We denote, as before, $\overline{C}_a$ the projective curve obtained by completing the affine curve C_a. The proof of the following proposition is straightforward:

Proposition 2.11. *For every $a \in K^*$ the curve $\overline{C}_a$ is singular. More precisely, if $a^4 \neq 1$ the curve $\overline{C}_a$ has two double points: $P_1 = (0 : 1 : 0)$ and $P_2 = (1 : 0 : 0)$. If $a^4 = 1$, then $\overline{C}_a$ contains six double points (including P_1 and P_2 hereinbefore).*

One can also easily see that, if $a^4 \neq 1$, by solving the singularities the curve $\overline{C}_a$ is birationally isomorphic to a non-singular curve of genus 1, hence to an elliptic curve. The next proposition identifies the Edwards curves that are birationally isomorphic to the same elliptic curve:

Theorem 2.12 ([3]). *The Edwards curves $\overline{C}_a$ and $\overline{C}_b$ ($a, b \in K^*$, $a^4 \neq 1$, $b^4 \neq 1$) are birationally isomorphic (hence induce, by resolution of singularities, isomorphic elliptic curves) if and only if b has one of the following 24 values:*

$$i^\varepsilon a \ , \ i^\varepsilon \frac{1}{a} \ , \ i^\varepsilon \frac{a-1}{a+1} \ , \ i^\varepsilon \frac{a+1}{a-1} \ , \ i^\varepsilon \frac{a-i}{a+i} \ , \ i^\varepsilon \frac{a+i}{a-1}.$$

Here i is a square root of unity in K (after eventually enlarging K if necessary) and $\varepsilon \in \{0, 1, 2, 3\}$.

Even if an Edwards curve $\overline{C}_a$ is not an elliptic curve, one can define a composition law on the set of points of $\overline{C}_a$:

Theorem 2.13 (addition formula). *If $a \in K^*$, $a^4 \neq 1$, the formulas*

$$X = \frac{1}{a}\frac{xy' + yx'}{1 + xyx'y'} \ ; \ Y = \frac{1}{a}\frac{yy' - xx'}{1 - xyx'y'} \tag{2.14}$$

describe a composition law on the Edwards curve $\overline{C}_a$. Moreover, this composition law is compatible, via the birational morphism described above, with the group law of the associated elliptic curve.

Proof. See [3]. We also point out that the group law on an elliptic curve can be described only in terms of the function field of the curve, whence the compatibility in the statement. □

In particular we have:

Corollary 2.15 (point doubling). *If $a \in K^*$, $a^4 \neq 1$, the formulas*

$$X = \frac{1}{a}\frac{2xy}{1 + x^2y^2} \ ; \ Y = \frac{1}{a}\frac{y^2 - x^2}{1 - x^2y^2} \tag{2.16}$$

describe the doubling formula for the elliptic curve birationally isomorphic to the Edwards curve $\overline{C}_a$.

3. Elliptic curves and cryptography. The "classical" public key cryptosystems are based on finite fields arithmetic. The security of such a cryptosystem relies on the hardness of a problem that should be solved for breaking the system. More specifically, one should have an efficient algorithm (i.e. running in polynomial time) for solving this problem in order to obtain the private (decyphering) key starting with the public information. The well-known RSA cryptosystem relies on the intractability of the integer factorization, whereas the Diffie-Hellman key exchange system or the El Gamal cryptosystem are based on the discrete logarithm problem. Neither of these problems can be solved in polynomial time. However, there exist sub-exponential algorithms for both of them. For obtaining a convenient security level one should use large keys and this affects the efficiency of the encrypting and decrypting procedures, as well as other cryptographic operations.

Koblitz [6] and Miller [8] introduced a new class of cryptographic schemes, based on elliptic curve arithmetic. Instead of using a hard problem

in a finite field for constructing a cryptosystem, they suggested to use such problems in the group of points of an elliptic curve defined over a finite field.

Definition 3.1 ([4]). The elliptic curve discrete logarithm problem (ECDLP) is: given an elliptic curve E defined over the finite field $\mathbb{F}_q$, a rational point $P \in E(\mathbb{F}_q)$ and a point $Q \in E(\mathbb{F}_q)$ belonging to the orbit of P, find the minimal positive integer l such that $Q = lP$. The integer l is called the discrete logarithm of Q to the base P, $l = \log_P Q$.

As we saw in the previous section, we dispose of explicit formulas for computing the multiple of a rational point P of an elliptic curve. The efficiency of the corresponding algorithms depends on the equation used for the elliptic curve. In this context, using, instead of the Weierstrass equation for the elliptic curve E, one of the Edwards curves birationally isomorphic to E leads to a significant gain in efficiency. We refer to [7] for a comparative study of the different choices for the equation of an elliptic curve and the efficiency of the corresponding algorithms.

On the other hand, the best algorithms known to this day, that solve the elliptic curve discrete logarithm problem are exponential, in contrast to the sub-exponential algorithms known for the integer factorization or for the discrete logarithm problem in finite fields. Hence a similar level of security is attained with much smaller keys. For example, a comparable level of security is reached with 160-bit keys for a cryptosystem based on ECDLP and with 1024-bit keys for RSA. Among the advantages gained from having smaller keys are improved speed or smaller storage capacity needed.

Another feature that worth mentioning is the set of possible keys. When constructing an elliptic curve cryptosystem, one has to choose not only the base finite field, but also a particular elliptic curve to work with. This gives a wide class of possibilities for choosing the keys.

Of course, there are several points to take care of, when choosing the elliptic curve, in order to avoid security failures and known attacks. These problems originate in the arithmetic and geometric properties of the elliptic curves. We mention hereafter some of the aspects to be taken into consideration.

The first one is the number of rational points of the curve. For avoiding a solution of the ECDLP by exhaustive search or collision search, the curve must have many points. Obviously, an elliptic curve E defined over the finite field $\mathbb{F}_q$ has at most $q^2 + 1$ rational points. On the other hand, one

can heuristically argue that, by considering for example the Weierstrass equation 2.5, the quantity $x^3 + ax + b$ is a square in $\mathbb{F}_q^*$ for, more or less, half of the possible values of x. Hence we expect that $\#E(\mathbb{F}_q) \approx q + 1$.

The following theorem, due to Hasse, gives an estimation of the error made by this heuristic approximation:

Theorem 3.2 (Hasse, 1922). *Let E be an elliptic curve defined over the finite filed $\mathbb{F}_q$, given by the Weierstrass equation* 2.5. *Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q} \ .$$

A direct consequence is the following: if q is large enough, then E has many rational points.

We close this section by mentioning some of the special cases when the elliptic curve discrete logarithm problem can be reduced to more "classical" cases of the discrete logarithm problem (see, for example, [12]).

1. If the curve E, defined over the field $\mathbb{F}_q$ has exactly q rational points, then ECDLP can be reduced to the discrete logarithm problem in the additive group $(\mathbb{F}_q, +)$, and this is very easy.

2. If $\#E(\mathbb{F}_q) = N$, then ECDLP on E can be reduced to the discrete logarithm problem in $\mathbb{F}_{q^t}$, where t is the smallest positive integer such that $q^t \equiv 1 \pmod{N}$. Hence one should choose an elliptic curve for which q^t is very large.

Fortunately, by choosing randomly a (large) finite field and an elliptic curve there are good chances that the problems arising from the remarks hereinbefore are avoided. More precisely, a generic elliptic curve avoids the bad cases presented hereinbefore. Moreover, once the curve is chosen, one can efficiently check the size of the integer t.

4. A secret sharing and shared digital signature scheme. We illustrate the use of elliptic curve in cryptography by describing some protocols that combine a key generation protocol, that is shared by the members (called in the sequel players) of a group, and is meant to be used for decrypting a secret in a public key cryptosystem, and a digital signature scheme shared by the players.

To illustrate the problem, we shall consider an example: having a multinational organization, with n branches in n countries, each with a director,

it is required a protocol package that performs the following tasks: key generation for a public key cryptosystem, decrypting a message if k directors agree to do so, and signing a public message in the same conditions.

The algorithm must give equal power to each director, in such a manner that without the required number of persons, nothing is possible. It is also required that the protocols have the ability to eliminate an opponent or a cheater.

The protocols-package will include an algorithm for each of the following actions:

- **key generating protocols (public and secret keys)**, considering all the restrictions;
- **signing** a public message - performed by the valid members ;
- **verifying the digital signature**.

The keys generating protocols were proposed by Tang [13] (see also [14]). We briefly describe them for the sake of completeness. The last two are direct adaptation of elliptic curves digital signature schemes [5] to the case when the signature is shared by the members of a group, with a threshold for the number of persons that can generate the signature. We also mention that the key generating protocols do not need the intervention of a trusted third party (such a cryptosystem was introduced in [9]).

We work over the Galois field $\mathbb{F}_q$, where q is a prime or a power of a prime. We also fix a field representation F of $\mathbb{F}_q$. Moreover, we have a fixed correspondence that associates to each element $x \in \mathbb{F}_q$ an integer $\overline{x}$.

We consider a group of n players, each of them identified by an element of this field, d_i $(i = 1, \ldots, n)$, known by everyone. Hence we consider the group as being the set $\{d_1, d_2, ..., d_n\} \subset \mathbb{F}_q$.

Let E be an elliptic curve defined over $\mathbb{F}_q$, that was conveniently selected (taking into account the restrictions mentioned in the previous section, among others). We suppose that the number of elements of the set $E(\mathbb{F}_q)$ is a large prime or has a large prime cofactor, that we will further denote by p. We can identify E with an Edwards curve, without mentioning this explicitly, and in this case we use the formulas (2.14) and (2.16) for implementation. The elliptic curve is determined by a couple of parameters $a, b \in \mathbb{F}_q$ that fix the Weierstrass equation of E.

Let $T(x_T, y_T)$ be a point in $E(\mathbb{F}_q)$ and let $l \in \mathbb{Z}$ be its order. We suppose that l is a large prime or has a large prime factor (eventually p hereinbefore). We also denote $h = \#E(\mathbb{F}_q)/l$.

The data (q, F, a, b, T, l, h) are called the domain parameters [4].

If one chooses to work with Edwards curves one could consider the domain parameters as (q, F, a, T, l, h), where the symbols preserve their meaning except for a, which is a parameter that defines the equation of the Edwards curve (2.9).

If $r \in \mathbb{F}_q$ and $P \in E(\mathbb{F}_q)$, then rP has the following meaning: we consider the associated integer $\overline{r}$, we determine the residue $\rho = \overline{r} \pmod{l}$ and then $rP := \rho P$.

We denote by k the number of players necessary for generating the keys $(k < n)$. Let $T' = dT$ be a point in $E(\mathbb{F}_q)$ that can be generated by the players, whose discrete logarithm d is not known, however, by any of them. This can be done in the following manner: each person chooses $r_i \in \mathbb{F}_q$, then computes and broadcasts $r_i T$. Then:

$$T' = \sum_i r_i T \pmod{p}.$$

We shall also denote by Q the set of valid members. A valid member is a fair member who did not try to forge the system by sending wrong shares. Initially, $Q = \{d_1, d_2, ..., d_n\}$.

4.1. Public key generating protocol. Tang [14] described the following key generating and secret key recovery algorithms in a slightly different form.

The key generation algorithm is the following:

1. Each player from the group, d_i, chooses $2k$ random elements $a_{it}, b_{it} \in \mathbb{F}_q$, $t = 0, ..., k-1$, as coefficients for two polynomials of degree $k-1$:

$$f_i(z) = \sum_{t=0}^{k-1} a_{it} z^t \ ; \ f_i'(z) = \sum_{t=0}^{k-1} b_{it} z^t.$$

2. Each player d_i computes

$$s_{ij} = f_i(d_j) \in \mathbb{F}_q \quad ; \quad s_{ij}' = f_i'(d_j) \in \mathbb{F}_q$$

and sends these values, on a private channel, to d_j $(j = 1, \ldots, n, j \neq i)$.

3. Each player d_i computes k points of the curve E,

$$P_{it} = (a_{it}T) + (b_{it}T') \ ,$$

($t = 0, \ldots, k-1$) and makes them available to the other players.

4. Each player d_i verifies, using the data received from the player d_j, if:

$$(s_{ji}T) + (s'_{ji}T') = \sum_{t=0}^{k-1} d_i^t P_{jt}.$$

If this proves to be false for a certain j, then d_i gives a fine to d_j. A fine is a public warning message such as the other players know that a certain player tried to forge the system.

5. If d_j received a fine from d_i, d_j retransmits the values s_{ji}, s'_{ji} not only to d_i, but makes them available to all the valid players.

6. If d_j received more than k fines, then he is disqualified, because his secret information can be computed by Lagrange interpolation; d_j is also disqualified for retransmitting false values (if he receives two fines from the same player). The disqualification of d_j can be formally registered by transforming $Q := Q \setminus \{d_i\}$.

7. Using the set Q of valid players, the public key can be computed as follows:

   - Each $d_i \in Q$ computes the point

$$A_{i0} = a_{i0}T \in E(\mathbb{F}_q)$$

     and sends it to everybody (**personal share of the public key**);
   - By putting together the valid key shares, **the group's public key** is obtained as:

$$Y = \sum_{j \in Q} A_{j0} \ .$$

By construction, the algorithm is efficient due to the computational complexity of the ECDLP. Another efficiency measure is step 4 of the algorithm 4.1 that prevents adversaries from coming into possession of at least k shares, thus revealing the secret.

4.2. Secret key recovery. Considering another order, let us denote by $\{d_1, ..., d_t\}$ the players from the set Q. We consider the polynomial:

$$F(z) = \left(\sum_{i\in Q} a_{i0}\right) + \left(\sum_{i\in Q} a_{i1}\right) z + ... + \left(\sum_{i\in Q} a_{it-1}\right) z^{t-1}$$

The **personal share of the secret key** of each valid player d_j is

$$s_j = F(d_j) = \sum_{i\in Q} s_{ij} \ .$$

The **group' secret key** is

$$y := F(0) \ .$$

Notice that $Y = yT$, hence the secret key y is the discrete logarithm of Y to the base T. By means of Lagrange interpolation, if one knows the personal shares of the secret key he is able to compute all the coefficients of F(z), hence the value of F(0), hence the group' secret key.

We refer to [13] for a message decryption algorithm in this context.

The calculus of the secret is never necessary for the group members, however it is not to be neglected how it could be done because, from an adversary's point of view this is the utmost important action.

4.3. Signing and signature validation algorithms based on secret sharing over elliptic curves (SS-ECDSA). We assume that every person from the signing group Q has a personal share of the public key and a personal share of the secret key, as defined hereinbefore. For each $d_i \in Q$ we can compute a shadow

$$u_i = \left(\prod_{j\in Q,\ j\neq i} \frac{d_j}{d_i - d_j}\right) s_i \ .$$

In the remaining of this section H denotes a cryptographic hash function whose outputs have bit-length no more than that of l (if this condition is not satisfied, then the outputs of H can be truncated).

We describe hereafter a joint signing algorithm that adapts the classical elliptic curve digital signature scheme ([5]; see also [4]) to a collective user. We notice however that, unlike the previous algorithms, the computations

here must be performed by a trusted third party (TTP), who knows the personal shares of the players. It is likely that combining the ideas of this algorithm with those of the message decryption algorithm in [13] a signature algorithm that needs no TTP can be constructed.

Joint signing of a public message M by the valid players

1. Each player $d_i \in Q$ chooses c_i, $1 \leq c_i \leq l-1$.
2. TTP computes $c = \sum_{i \,|\, d_i \in Q} c_i \pmod{l}$.
3. TTP computes $cT = (x_1, y_1)$ and converts x_1 into the integer $\overline{x_1}$ (we recall that $\overline{x_1}$ is an integer associated to $x_1 \in \mathbb{F}_q$).
4. TTP computes $r = \overline{x_1} \pmod{l}$; if $r = 0$, reiterate step 1.
5. TTP computes $c^{-1} \pmod{l}$.
6. TTP computes $H(M)$ and converts it to an integer e.
7. TTP computes $s = c^{-1}(e + \sum_{i \,|\, d_i \in Q} u_i r) \pmod{l}$.
8. The digital signature of the message M is (r, s).

Validation of a digital signature of a group

1. Reject the signature if r and s are not in $[1, n-1]$.
2. Compute $H(M)$ and convert it to an integer e.
3. Compute $w = s^{-1} \pmod{l}$.
4. Compute $v_1 = ew \pmod{l}$ and $v_2 = rw \pmod{l}$.
5. Compute $X = v_1 T + v_2 Y$, where $Y = \sum A_{j0}$ is the public key of the group.
6. If $X = O$ reject the signature. Else, if x_1 is the first coordinate of X, compute $v = x_1 \pmod{l}$.
7. Accept the signature if $v = r$.

We refer to [4] for some security issues regarding ECDSA in general, thus applicable for SS-ECDSA.

REFERENCES

1. Blakley, G.R. – *Safeguarding cryptographic keys*, Proceedings of the National Computer Conference, 48, 313-317.
2. Diffie, W.; Hellman, M. – *New directions in cryptography*, IEEE Trans. Inform. Theory, 22(1976), 644–654.
3. Edwards, H. – *A normal form for elliptic curves*, Bull. Amer. Math. Soc., 44(2007), 393–422.
4. Hankerson, D.; Menezes, A.; Vanstone, S. – *Guide to Elliptic Curve Cryptography*, Springer Verlag, New York, 2004.
5. Johnson, D.; Menezes, A.; Vanstone, S. – *The elliptic curve digital signature algorithm (ECDSA)*, International Journal on Information Security, 1(2001).
6. Koblitz, N. – *Elliptic curve cryptosystems*, Mathematics of Computation 48(1987), 203-209.
7. Lange, T. – *Explicit formula database* http://hyperelliptic.org/ EFD/g1p/auto-edwards.html.
8. Miller, V. – *Use of elliptic curves in cryptography*, Advances in Cryptology - CRYPTO'85, LNCS 218 [483], 1986, 417–426.
9. Pedersen, T.P. – *A Threshold Cryptosystem Without A Trusted Party*, Advances in Cryptology–Eurocrypt 91 Proceedings, vol. 547, Lectures Notes in Computer Science, Springer-Verlag, 1991, 129–140.
10. Shamir, A. – *How to share a secret*, Communications of the ACM, 22(11) (1979), 612–613.
11. Silverman, J.H. – *The Arithmetic of Elliptic Curves*, GTM 106, Springer Verlag, New York, 1986.
12. Silverman, J.H. – *Elliptic Curves and Cryptography*, in "Public-KeyCryptography" (Eds.: P. Garrett, D. Lieman), Proc. of Symp in Appl. Math. 62, AMS, Providence, 2005, 91–112.
13. Tang, C. – *ECDKG: A Distributed Key Generation Protocol Based on Elliptic Curve Discrete Logarithm*, report, http://www.cs.usc.edu/Research/TechReports/04-838.pdf.
14. Tang, C.; Choronopoulus, A. – *An Efficient Distributed Key Generation Protocol for Secure Communications with Causal Ordering*. ICPADS (2) 2005, 285–289.

Received: 15.V.2008

"Al.I. Cuza" University,
Department of Mathematics,
Bd. Carol I 11, Iaşi 700506,
ROMANIA
litcanu@uaic.ro