BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Tomul XLV (IL), Fasc. 1–2, 1999
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

D.C. 621.394.9

SECURE COMMUNICATION BASED ON ELLIPTIC CURVE PUBLIC KEY CRYPTOSYSTEMS (I)

BY

EUGEN PETAC

Public-key systems (two-key or asymmetric) differ from conventional systems in that there is no longer a single secret key shared by a pair of users. Each user has his proper cryptographic key. The key of each user is divided into two portions: a private component and a public one. The public component generates a public transformation, E, and the private component generates a private transformation, D. E and D can be termed encryption and decryption functions, respectively. In a system we may have $D(E(MM)) = M$, $E(D(M)) = M$ or both.

The cryptographic importance of the *Elliptic Curve Public Key Cryptosystems* (ECPKC) consists in the difficulty to determine discrete logarithms over extentions of finite fields [7]. This is much harder than factorization of integers or calculating discrete logarithms in $\mathcal{F}_q$. Another most important aspect consists in the forms for the private keys and for the public ones: the private keys are ordinary integers and the public keys are points on an elliptic curve. Elliptic curve systems are very advantageous for applications with smart cards and in distributed systems, where computational power and integrated circuit space are limited, because computations are easily performed and bandwidth requirements are minimal.

The paper presents a proposal for the implementation of privacy enhancement in a packet-switched local area network, using *Elliptic Curve Public-Key Cryptography* for key management and authentication.

For computing in finite extensions over finite rings we have used the ZEN-new toolbox [5]: there are some computing routines implementing the *group law* defined for an elliptic curve. We have implemented in ZEN the conversions between bit string, integer, point-to-octet string, octet string-to-point, field element and point of the elliptic curves.

1. A Short Presentation of the Public Key Cryptosystems

The procedures of encryption and decryption, according to some Public Key Cryptosystems (PKC) [2], contain the public algorithms, noted by E and D. These are initialized by the public key, KeI, and by the secret key, KdI, for each user of the system, I. The keys KeI and KdI become from the initialization key, KiI, after the application of F and G algorithms. The emitter $\mathcal{A}$ receives the cryptogram $C = E(M) = E_{KeB}(M)$ on the basis of the public key KeB and of E algorithm, where M is the plaintext. The receiver, $\mathcal{B}$,works with the algorithm D under the action of the secret key, KdB. Because the encryption key is a public one and anyone can use it, through such an implementation can't be done also the authentication of the send message.

adaptively chosen ciphertext attacks depending on the enemy access to the decryption algorithm, before or after the arrival of the ciphertext. For each kind of attack there are developed specific security actions [13]. The adaption of some security actions against the chosen plaintext attacks and chosen ciphertext attacks being used is necessary for PKC.

The security services of our paper are *authentication, secrecy, integrity, nonrepudiation.*

a) *Authentication* refers to verification of the identity of the sender or receiver of a communication.

b) *Secrecy* refers to protection against interception of data.

c) *Integrity* refers to protection against manipulation of data.

d) *Nonrepudiation* refers to protection against denial of sending (or possibly receipt) of a message.

2. Elements of Elliptic Curve Algebra in Finite Fields

Let be $\mathcal{F}_q$ a finite field containing q elements, with q prime number. For $\mathcal{K} = \mathcal{F}_q$ we note with $\overline{\mathcal{K}}$ its algebraic closure: $\overline{\mathcal{K}} = \bigcup_{m\geq 1} \mathcal{F}_{q^m}$, where m is a nonnegative integer number. Let be $\mathcal{K}^3 = \mathcal{K} \times \mathcal{K} \times \mathcal{K}$. The projective plane $\mathcal{P}^2(\mathcal{K})$ is the set of the equivalence classes of the relation $\sim$ which operate on $\mathcal{K}^3 \backslash \{0,0,0\}$, where $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$, if and only if exists $\lambda \in \mathcal{K}^*$ so that $X_1 = \lambda X_2$, $Y_1 = \lambda Y_2$, $Z_1 = \lambda Z_2$. We note the equivalence classes which contain (X, Y, Z) through $(X : Y : Z)$.

A homogeneous equation of third degree with the form

$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3, \tag{1}$$

where a_1, a_2, a_3, a_4, $a_6 \in \overline{\mathcal{K}}$, is called the Weierstrass equation.

The algebraic curve according to this equation can be:

a) *smooth or nonsingular*, if for all points $P = (X : Y : Z) \in \mathcal{P}^2(\overline{\mathcal{K}})$ which fulfil the relation $F(X, Y, Z) = 0$ at least one of the partial derivatives $\partial F/\partial X$, $\partial F/\partial Y$, $\partial F/\partial Z$ is different from zero in the point P;

b) *singular*, if all partial derivatives are null in the points noted P, where P is called singular point. According to equation (1) there is a point on the algebraic curve with $Z = 0$, noted $\mathcal{O} = (0 : 1 : 0)$, called *point at infinity.* We show the equation (1) in affine coordinates based on relations $x = X/Z$, $y = Y/Z$ and we get:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{2}$$

An *elliptical curve* $\mathbf{E}$ (called algebraic curve of first genus) is formed by the solutions of the equation (2), according to a *smooth curve* from the affine plane $\mathcal{P}^2(\overline{\mathcal{K}}) = \overline{\mathcal{K}} \times \overline{\mathcal{K}}$, together with the *point at infinite*, noted $\mathcal{O}$, expressed in affine coordinates.

Let be the points $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P, Q \in \mathbf{E}$. We define the algebraic operation $+ : \mathbf{E} \times \mathbf{E} \to \mathbf{E}$, $P + Q = R$, with $R = (x_3, y_3)$, $R \in \mathbf{E}$. The algebraic compromised; b) an individual user lasses control over algorithms used.

2. In end to end encryption a message is encrypted and decrypted only at end points. Some address information (data link leaders) must be left unencrypted to allow nodes to route packets. High-level network protocols must be augmented with a separate set of cryptographic protocols.

In terms of OSI (*Open System Interconnection*) model encryption can occur at various levels: *application, presentation, network, transport.* Integration at the application layer gives the individual user complete control over the algorithms used.

3.1. Cryptosystem with Public Keys

EPPKEC is an *Encryption Protocol* with *Public Keys* that uses *Elliptic Curves.* It generates the cryptogram, C, for the message, M, both of them considered as sequences of octets. Users $\mathcal{A}$ and $\mathcal{B}$ of the system know SECP and the format mode of the message, M, operation by which it is obtained $m^* := F(M) : \{\mathcal{M}\} \rightarrow \sum_{\{0,1\}}$. $\{\mathcal{M}\}$ is the set of the messages, M, and $\sum_{\{0,1\}}$ is the set of binary sequences. The users $\mathcal{A}$ and $\mathcal{B}$ choose at random and each of them keep secretly the integer number d_A, respectively d_B, with $d_A, d_B \in [2, r-2]$. They apply the *procedure* CdP and each of them obtain by computation the points $Q_A = d_A \bullet P = (x_{QA}, y_{QA})$ and $Q_B = d_{AB} \bullet P = (x_{QB}, y_{QB})$ of the elliptic curve. The binary representations Q_A^* and Q_B^*, obtained following the application of one of the *procedures* CPBTC or CPBFTC, depending on the situation in which it is used or not a compression technique, are registered in a public register, PR. We note with t the number of bits corresponding to the binary transformation of an element of the field $\mathcal{F}_p$ and with l the number of octets, $l = [[t/8]]$. We note with $[[x]]$ the smallest integer great or equal with x. The message M, that is to be sent secretly from $\mathcal{A}$ to $\mathcal{B}$, contains at least $l-2$ octets. We note the number of octets of the message M with $\|M\|$. EPPKEC (Fig. 1) contains three phases: *of format of the message M, of encryption and of transmitting of the cryptogram C, of decryption of the received cryptogram.*

EPPKEC

a) *The format Phase of the Message*

1. To message M a number of $l-2-\|M\|$ octets, that have alternatively the values FF and 00, is associated on the left. A sequences of octets, noted with M, of length $l-1$ octets, of the size $M' = (00/FF)\|00\|M$ is obtained.

2. The user $\mathcal{A}$:

2.1. Chooses at random an integer number $e_A \in [2, r-2]$.

2.2. Read Q_B^* from PR and apply one of the *procedures* CBPTC or CBPFTC, to obtain the point Q_B of the elliptic curve.

2.3. Apply the *procedure* CdP and compute the points R_A and $S_A : R_A = (x_{RA}, y_{RA}) := e_A \bullet P$; $S_A = (x_{SA}, y_{SA}) := e_A \bullet Q_B$.

2.4. Apply one of the *procedures* CPOTC or CPOFTC and receive the sequence of octets R_A^{**} that correponds to R_A.

2.5. Apply the *procedure* CDECFB and obtain the binary representation x_{SA}^* of x_{SA}.

2.6. Obtain in two steps a binary sequence, m^*, of t bits:

2.6.1. Apply the *procedure* CDECFB and receive the binary representation $(M')^*$ of M'.

2.6.2. Complete $(M')^*$ with $8 - 8l + t$ bits of 0 on the left.

b) *The Encryption and Transmission of the Cryptogram C Phase*

1. Compute $CR^* = (m^* + x^*_{SA}) \bmod 2$.
2. Apply the *procedure* CDBO and obtain the sequence of octets CR^{**}.
3. Find the cryptogram C by a concatenation operation: $C = R^{**}_A || CR^{**}$.
4. The user $\mathcal{A}$ transmits the cryptogram C to $\mathcal{B}$ user.

If compression techniques $TCPF_p$ or $TCPF_{2^n}$ are used, the cryptogram C is represented on $2l + l$ octets and, to the contrary, on $3l + l$ octets.

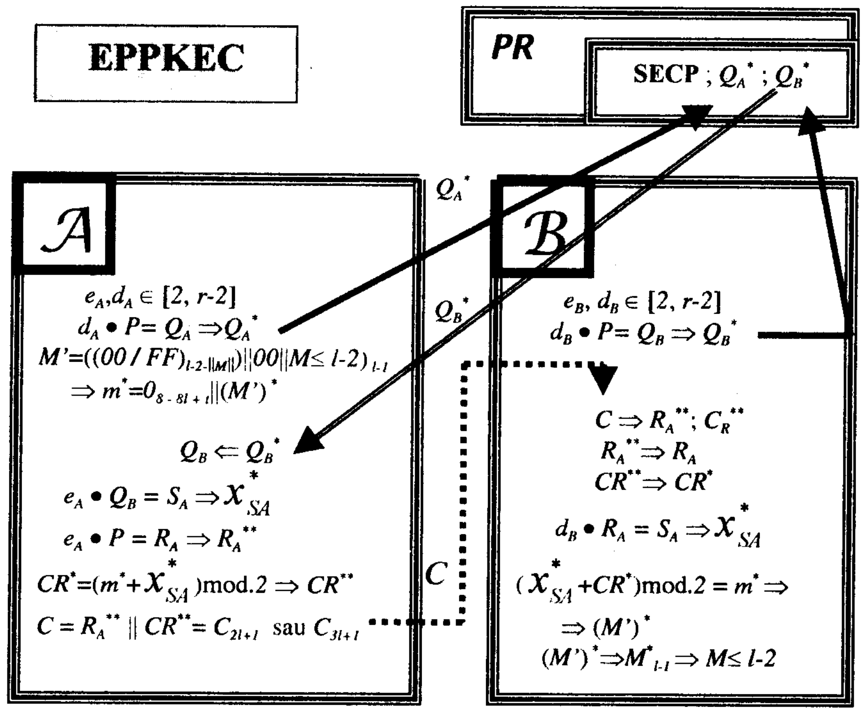

Fig. 1.- Encryption protocol with public keys that uses elliptic curves.

c) *The Decryption Phase of the Received Cryptogram*

The user $\mathcal{B}$:

1. If the most in the left bit of the cryptogram C, termed with $BS(C)$, is 1, then the cryptogram C corresponds to $l + 1$ octets in the left (note $S_{l+1}(C)$), and to the contrary to $2l + l$ octets in the left (note $S_{2l+l}(C)$). This depends on the using or not of some compression techniques in the encryption operation.
2. Apply the *procedure* COP and from R^{**}_A is received the point $R_A = (x_{RA}, y_{RA})$, that belongs to the elliptic curve.
3. Apply the *procedure* CDOB and from CR^{**} is received the binary sequence CR^*.
4. Apply the *procedure* CdP and compute $d_B \bullet R_A = S_A = (x_{SA}, y_{SA})$.

It is checked if $d_B \bullet R_A = d_B \bullet (e_A \bullet P) = e_A \bullet (d_B \bullet P) = e_A \bullet Q_B = S_A = (x_{SA}, y_{SA})$.

5. Apply the *procedure* CDECFB and obtain the binary representation, x^*_{SA}, for x_{SA}.
6. From $(x^*_{SA} + CR^*) \bmod 2 = m^*$ it results $(M')^*$ by doing away with the $8 - 8l + t$ most bits that are in the left.
7. Apply the *procedure* CDBO for $(M')^*$ and obtain M' as a sequence of $l - 1$ octets.
8. Being given the known structure of M', it is obtained the message M, that contains at the most $l - 2$ octets.

End.

4. Conclusions

For the point $P(x_P, y_P)$ who is situated on the elliptic curve $\mathbf{E}/\mathcal{F}_q$, $q = 2^m$, $\mathbf{E}/\mathcal{F}_q : y^2 + xy = x^3 + a_2x^2 + a_6$, is possible to define the $\tilde{y}_P : \tilde{y}_P = 0$, for $x_P = 0$ and $\tilde{y}_P = RM(y_P x_P^{-1})$, for $x_P \neq 0$. With x_P^{-1} we have noted the *inverse element* for x_P in the field $\mathcal{F}_q$ and $RM(z)$ offer the right most bit of the field element z. Over the $\mathcal{F}_q$, $q = 2^m$, with an *optimal normal basis* representation, a point compression technique is used: the point $P = (x_P, y_P)$ represents by storing only the x-coordinate x_P and the $\tilde{y}_P$. For computing in finite extensions over finite rings we have used the ZEN-new toolbox.

The *exponential cryptographic* algorithms attain their security through the combined use of exponentiation modulus (with digital signature) and the difficulty of inventing the strong pseudo-random string generator, G. The total cost for the algorithm will be $O(n^3)$ elementary operations because each multiplication in finite fields requires n^2 elementary operations, and every exponentiation requires $O(n)$ multiplications. The best algorithm known for the discrete logarithm problem [1] in $\mathcal{Z}_q^*$ has an asymptotic running time of $\exp[(1.923 + O(1)](\log q)^{1/3}(\log\log q)^{2/3}$.

For the *elliptic curve public keys cryptographic* algorithms the cryptographic importance consists in the difficulty to determine discrete logarithms over finite fields. Another most important aspect consists in the forms for the private keys and the public ones. The private keys are ordinary integers and the public keys are points situated on an elliptic curve. Elliptic curve systems are very avantageous for applications with smart cards and in distributed systems, where computational power and integrated circuit space are limited.

A c k n o w l e d g e m e n t s. I wish to thank Professor Dr. Eng. Valeriu M u n t e a n u, from "Gh. Asachi" Technical University of Iaşi, Faculty of Electronics and Telecommunications, for their careful reading of the manuscript, helpful comments and for valuable discussions on this work.

Received, November 25, 1998

"Ovidius" University, Constantza

REFERENCES

1. A g n e w G., M u l l i n R., V a n s t o n e S., *An Implementation of Elliptic Curve Cryptosystems Over $F_{2^{155}}$*. IEEE J. on Selected Areas in Commun., **11**, *5*, 804-813 (1993).
2. D i f f i e W., H e l l m a n M., *New Directions in Cryptography*. IEEE Trans. on Inform. Theory, *22*, 644-654 (1976).
3. D i f f i e W., H e l l m a n M., *Privacy and Authentication: An Introduction to Cryptography*. IEEE Trans. on Inform. Theory, *67*, 397-427 (1979).
4. D i f f i e W., *The First Ten Years of Public Key Cryptography. Contemporary Cryptology: The Science of Information Integrity*. IEEE Press, New York, 1991, 135-175.
5. C h a b a u d F., L e r c i e r R., *ZEN - A New Toolbox for Computing in Finite Extensions over Finite Rings*. INRIA-ftp, July, 1996.
6. K o e l l e r J., M e n e z e s A., Q u M., V a s t o n e A., *Standard for RSA, Diffie-Hellman and Related Public-key Cryptography*. Certicom Corp., Ontario, Canada, 1996.
7. M e r k l e R., *A Certified Digital Signature*. Advances in Cryptology, CRYPTO'89, Lecture Notes in Computer Sciences, 1990, *435*, Springer-Verlag, New York, 218-238.

8. Menezes A., Vanstone S., *The Implementation of Elliptic Curve Cryptosystem*, Advances in Cryptology - AUSCRYPT'90, Lecture Notes in Computer Sciences, 1990, *453*, Springer-Verlag, New York, 2-13.
9. Miller V., *Uses of Elliptic Curves in Cryptography*, Advances in Cryptology - CRYPTO'85, Lecture Notes in Computer Sciences, 1986, *218*, Springer-Verlag, New York, 417-426.
10. Mullin R., Onyszchuk I., Vanstone S., Wilson R., *Optimal Normal Bases in $GF(p^n)$*. Discrete Appl. Math., *22*, 149-161 (1988-89).
11. Petac E., *Security Elements of Communications Using Elliptic Curve Cryptosystems*. Proc. of the Third Asia-Pacific Conf. on Commun. (APCC'97), Sydney, Australia, December 7-10, 1997, 1362-1365.
12. Petac E., *On the Construction of Elliptic Curve Cryptosystems*. Proc. of the Develop. a. Appl. Syst., "Ştefan cel Mare" University, Suceava, 1996, 93-96.
13. Petac E., *A New Public Key Encryption Scheme Using Elliptic Curves*. SCS'97 - Internat. Symp. on Signals, Circuits and Systems, The Faculty of Electronics and Telecommunications, "Gh. Asachi" Technical University, Iaşi, Oct. 2-3, 1997, 565-568.
14. Silverman J., *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.
15. Silverman J., Tate J., *Rational Points on Elliptic Curves*. Springer-Verlag, New York, 1992.

COMUNICAŢIE SIGURĂ BAZATĂ PE CRIPTOSISTEME CU CHEI PUBLICE CONSTRUITE PE CURBE ELIPTICE (I)

(Rezumat)

Sistemele cu chei publice (cu două chei sau asimetrice) diferă de cele convenţionale prin faptul că nu există o singură cheie secretă, partajată un timp îndelungat, de o parte din utilizatori. Cheia fiecărui utilizator conţine două componente: una privată şi alta publică. Componenta publică iniţiază o transformare publică, E, iar componenta privată iniţiază o transformare privată, D. E şi D pot fi identificate ca funcţii de criptare şi decriptare. Într-un astfel de sistem trebuie să fie îndeplinite cel puţin una din relaţiile $D(E(M)) = M$, $E(D(M)) = M$, unde M este mesajul transmis.

Importanţa criptografică a *criptosistemelor cu chei publice construite pe curbe eliptice* constă în dificultatea de a calcula logaritmi discreţi peste extensii ale unor câmpuri finite [7]. Aceasta este o operaţie mult mai complexă decât factorizarea unor numere întregi sau calculul logaritmilor discreţi în $\mathcal{F}_q$. Un alt avantaj foarte important este conferit de structura cheilor publică şi privată; cheia privată este un simplu număr întreg în timp ce cheia publică este un punct situat pe o curbă eliptică. Sistemele criptografice construite pe curbe eliptice sunt indicate pentru aplicaţii care folosesc cartele inteligente şi în sistemele distribuite, unde sunt limitate puterea de calcul şi spaţiul fizic necesar implementării.

Se prezintă un sistem cu un grad mărit de secretizare a informaţiei transmise într-o reţea locală de calculatoare cu comutare de pachete, folosind metode criptografice dezvoltate pe curbe eliptice, în scopul administrării cheilor şi autentificării mesajului transmis.

Pentru calculul în extensii finite, construite peste inele finite, s-a folosit toolbox-ul ZEN; acesta prezintă rutine de calcul ce implementează grupul finit de tip *law* pentru o curbă eliptică. S-au implementat în ZEN conversiile dintre diferite forme de reprezentare a informaţiei: număr întreg, şir de biţi, şir de octeţi, punct al unei curbe eliptice, element al unui câmp finit.