Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 41(2), 2014, Pages 292–299
ISSN: 1223-6934

Nonlinear analysis on elliptic curves subspaces with cryptographic applications

Oana Adriana Ţicleanu

Abstract. Defining an adequate and well secured system is the ideal solution to protect the data against online attacks. With respect for this, one of the methods which are used is the double authentication in order to reduce the likelihood that a user presents false evidence of identity. In this article, we present cryptographic systems based on elliptic curves defined over finite space F_{p_t}. The security of the cryptosystems is given by a set of numbers, chosen from an elliptic curve and the calculation difficulty for the attack on the encryption system, taking an effective approach by establishing a common secret key required for group authentication. Also we present a complete description of the necessary system for the double authentication scheme.

2010 Mathematics Subject Classification. Primary 60J05; Secondary 60J20.
Key words and phrases. elliptic curves cryptography, nonlinear equations, group authentication.

1. Introduction

The only defense against online attacks and combating online identity theft is by securing access to data where authentication occurs. Authentication represents the process of verifying a user identity that is to accessed the database.

Accessing data can be done either through a virtual private network (VPN), remote desktop connection, e-mail application (Outlook Anywhere) or an online portal that are authorized to access the data. Traditional authentication systems includes a lower security level authentication such as a password.

In this article we propose to improve the process of authentication for access to the database by double authentication, key exchange security on both sides. Two-factor authentication adds stronger security for users to authenticate with additional accreditations in addition to a password. Double authentication requires two of the following factors: something he knows (password, PIN), something he has (identity card, keys), and something that uniquely represents the user (fingerprint, retinal image).

However, the choice of an adequate and well secured two-factor authentication system can be difficult and expensive, compared with an unified authentication system, so it is easier to use and computational cost-effective. Two-factor authentication is a security process in which the user has two means of identification, one of which is usually physical, such as a card, and the second is something memorized, such as a security code. The two factors involved in the authentication process are something that the user knows and something he owns. Integrity is the assurance that the data which a user refers to can be accessed and modified only by those authorized to do so.

Received November 24, 2014.

Double authentication is used to reduce the likelihood that the user provides false evidence of identity. To reduce the number of stored keys and broadcasted messages, the researchers inserted the group key distribution protocol [13, 20] which is based on DLP (Discrete Logarithm Problem) assuming several public-key cryptosystems.

For a group double authentication, elliptic curve cryptosystems can be used to perform digital signature schemes and encryption schemes. Cryptosystems based on elliptic curve encryption systems refer to use numbers generated by an elliptic curve. It has been demonstrated over time that the cryptographic systems that are encrypted with the numbers generated by an elliptic curve are safer.

Cryptographic systems based on elliptic curves are defined equally well in any finite group (such as a group of points on a elliptic curve) and have stronger cryptographic security per bit than of any other public key encryption system known at the time. Memory requirements and bandwidth are substantially lower. Systems based on elliptic curves are easier to implement, being more efficient than any other public key system.

These systems are ideal for small hardware implementations such as cards, furthermore, encryption and signing can be performed in separate steps with an significant speed compared to other systems, which simplifies the security problem at login.

The security of cryptosystems based on elliptic curves consists in the difficulty of calculating discrete logarithms in discrete fields (DLP). The group key protocol has a major role in securing data and is divided into two categories: session key protocol and broadcast management key between the group members.

A group transfer key protocol is KGC, reliable key generation center (trusted key generation center) [2, 18, 23] is responsible for the generation and transport of the key to each involved member in the authentication process. For each distribution there is a registration process for users to subscribe group key, randomly selecting a private key.

The first step to a secured group authentication is to establish a secret code that is sent to group members. It establishes a protocol that ensures data security against active attacks. Of course, the cryptographic security levels can be achieved in various ways.

To transmit the confidentiality data, an effective approach is to establish a common secret key, obtained only by group members, required by the authentication. Recoding the group key is required whenever there is a change in the group, for data confidentiality. The confidentiality of the group key distribution is theoretically secure information and the security group key transfer depends on the members actions not an calculation hypothesis.

2. State of the art

For a secure communication between two or more users in an insecure network, it is necessary to establish common session keys. For communication between two users, things are somewhat simpler than in the case of multiple users, in which is more difficult to establish a rigorous communication with no problems.

The best known protocol for establishing a common session key using a hostile communication channel is Diffie-Hellman protocol. It also aims for exponential key exchange, the protocol is resistant to passive attacks, any active malevolent person can intervene and establish a session key with both involved parties in the communication.

The algorithm that has as input a prime number p big enough and a generator g.

- U_1 picks randomly a number, a number such that $0 \leq a \leq p-2$;
- U_1 computes $c = g^b$ and sends c to U_2;
- U_2 picks randomly a number b, such hat $a \leq b \leq p-2$;
- U_2 computes $d = g^b$ and sends d to U_1;
- U_1 computes the key $k = d^a = (g^b)^a$;
- U_2 computes the key $k = c^a = (g^b)^b$.

Starting from this algorithm, A. Jaux introduced another protocol called "A one round protocol for tripartite Diffie-Hellman", this protocol establishes a shared session key for three users.

With the growth of networks, the need for communications between more than three users becomes evident. There have been many attempts to establish a shared secret key for communication between n users [13, 20].

The protocol for establishing the session keys is divided into distributed commune keys establishment protocols and centralized key establishment protocols. The distributed mode have a higher cost in case of a large number of users, because each must participate in establishing process of the common communication key. As computer networks are increasing in terms of user growth, management protocols of centralized communication keys seems as an adequate choice.

Among the latest and ones of the most used protocols are presented in [3, 5, 12, 14, 16, 19] protocol that is to satisfy the three most important properties of a communication key:

- key authentication (assures the users that they use the correct key);
- key freshness (the key used in that moment wasn't used in the past);
- key confidentiality (protects the current key that isn't alienated to other users).

The advantage of these centralized protocols is that they use a common key generation center. At every entrance or exit of a user from a group, the generation center reconstructs this session key based on the new user or the removed user.

3. Background on Elliptic Curves Cryptography (ECC)

Let E_ϑ be an elliptic curve over a finite field K. E_ϑ is defined by Weierstrass equation, as follows:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$. This request, $\Delta \neq 0$, ensure the existence of the differential coefficients in every point of the elliptic curve, for detailed information, see [8], [9], [11]. For E_ϑ, Δ will be computed as:

$$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = a_1a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 \\ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \end{cases}$$

According with [15], the curve points set together with infinity point $\mathcal{O}$ and an addition operation (as defined below) construct an abelian group.

Let $P, Q \neq 0$ be two points defined over an elliptic curve E_ϑ over a finite field K, and k a natural number. Then, for nonzero points with values $P = (X_1, Y_1)$, $Q = (X_2, Y_2)$, $R = (X_3, Y_3)$, we have:

(1) Inverse of a point:

$$-P = (X_1, -Y_1 - a_1X_1 - a_3)$$

(2) Two points sum: $R = P + Q$

$$\begin{cases} X_3 = \lambda^2 + a_1\lambda - a_2 - X_1 - X_2 \\ Y_3 = -(\lambda + a_1)X_3 - \nu - a_3 \end{cases}$$

where

$$\lambda = \begin{cases} \dfrac{Y_2 - Y_1}{X_2 - X_1} & \text{if } P \neq Q \\ \dfrac{3X_1^2 + 2a_2X_1 + a_4 - a_1Y_1}{2Y_1 + a_1X_1 + a_3} & \text{if } P = Q \end{cases}$$

$$\nu = \begin{cases} \dfrac{Y_1X_2 - Y_2X_1}{X_2 - X_1} & \text{if } P \neq Q \\ \dfrac{-X_1^3 + a_4X_1 + 2a_6 - a_3Y_1}{2Y_1 + a_1X_1 + a_3} & \text{if } P = Q \end{cases}$$

(3) Scalar multiplication:

$$Q = k \cdot P = \underbrace{P + P + \ldots + P}_{k \text{ times}}$$

For big values of k, from cryptographically point of view is usefully to define an algorithm for exponentiation, with applications for [1], [10], [17]. In the particular case of $k = \sum_{\theta=0}^{\kappa} \lambda_\theta 2^\theta, \lambda_\theta \in \{0, 1\}$, then

$$kP = \sum_{\theta=1}^{\kappa} \lambda_\theta (2^\theta P)$$

where doubling of it is necessary to obtain $2P, 2^2P, 2^3P, \ldots, 2^\kappa P$, and the most of complementary values κ depends by $\lambda_\theta = 1$.

3.1. ECC for message authentication. Elliptic Curves Cryptosystems for certain subspaces has some advantages, like key dimension and generating time, beside classical ones, because if the elliptic curve subspace is carefully chosen, ECDLP (Elliptic Curve Discrete Logarithm Problem) will define the attack complexity according with:

Let E be an elliptic curve defined over the F_{p_t}, where $F_{p_t} \in F_p$ (F_p a finite space), a point $P \in E$ (F_{p_t}) of order n, and a point $Q \in E$ (F_{p_t}), we have to found a point $k \in [0, n-1]$ such that $Q = kP$. The integer k is named the discrete logarithm of Q with P base, noted with $k = log_P Q$.

Encryption/Decryption

Let A and B be two entities which should communicate by sending the message P_{m_ϖ}. The entity A will send the message P_{m_ϖ} to the entity B by choosing first a pseudoaleator number k and private key χ_A. A will generate a public key $P_A = \chi_A \times \beta$, from that will compute the encrypted message $'C'_{m_A}$ which consist of points pair $C_{m_A} = \{k\beta, P_{m_\varpi} + k_{P_B}\}$, where β is the basic point, selected from the elliptic curve. In the next step, the entity B will choose a public key $P_B = \chi_B \times \beta$, respectively a private one, χ_B.

In order to decrypt the message, B must extract the result of the next equation:

$$P_{m_\varpi} + kP_B - \chi_B(k\beta) = P_{m_\varpi} k(\chi_B\beta) - \chi_B(k\beta) = P_{m_\varpi}$$

In encryption and decryption elliptic curves model, and for Digital Declaration, the basic parameters will define the elliptic curve subspace type. The strength of the cryptographic system is determined by the $D = (q, \alpha_a, \alpha_b, G, \beta, \tau)$, in the next algorithm.

- Let be the subspaces of parameter p.
- The parameters α_a, α_b defines the elliptic curve E over E_q, and the equations

$$Y^2 = X^3 + AX + B(p > 3) \text{ or } Y^2 + XY = X^3 + AX + B(p = 2).$$

- G - a generator point.
- β elliptic curve order.
- τ - co-factor, where $\tau = \#E(F_p)/\beta.\#E(F_p)$ represents the points number from the elliptic curve.

In order to implement the mathematical model, the previous enunciated parameters should achieved the next conditions, named general parameters:

- $q = p$ or $q = 2^{\sigma_x}$, where σ_x is a prime number.
- The elliptic curve should be non-singular.
- β should be $q^{\partial} - 1(1 \leq \partial \leq \pi)$, where π usually is 20.
- The elliptic curve should be non-anomalous, which means $|E(F_q)| \neq q$.

The main security parameter is β, and the key length is β.

4. F_{p_t} subspaces for ECC

Starting from [21] studies, below we present a method to transfer information by encrypting it with a public key known only to those who are authorized to access information through the communication channel. This system of information security requires each group participant to expose a parameter that will be part of the session key construction.

The group may be formed of 2, 3, 4, ..., t participants. Each participant selects an unique parameter, as an ID, known to himself and the key generator, which will be used to provide secure communication. Parameters will form a function $f(2,\ 3,\ 4,\ ...,\ t)$ resulting a public key, noted as k_t.

To extract the key, the user personal parameter is used and an using control key will communicate the private key to the participants. The private key will be generated by the public key generator at the request of a participant authenticated with his personal parameter, the ID.

Using an algorithm for transforming a sequence (ST) in a public key$k_t \in \{0,1\}^*$ will encrypt a plain text with that key and the encrypted text will be transferred through a secure channel. The message decryption will be done by an user using the regular private key obtained from the public key generator. However, the encrypted message must be intended to him so he can decrypt it.

For such a cryptographic system the following steps are defined:

- *configuration* - the unique parameters are generated for each user/member of the group for group identification and to create the common private key;
- *extraction* - according to the corresponding sting of the ID (ST) the master key is used to generate the private key corresponding to the public key needed for group authentication
- *encryption* - the encryption algorithm is described that will encrypt the message using the public key;
- *decryption* - using the private key the message will be decrypted using the decryption algorithm;

The algorithm used to obtain the private key from the public key generator is a type of challenge-response system. Because it is part of this category, for construction we will use, in the same way as in [6, 7] the following steps:

Definitions:

The expression x^3+1 is a permutation for F_{p_t}, where E is an elliptic curve given by the equation $y^2 = x^3 + 1$, defined over F_{p_t}, and p_t is a number through which will satisfy $p_t = 6m - 1$, where m is a prime number, and $m > 3$.

Let $G \in E/F_{p_t}$ be a group generator of points of order $m = (p_t + 1)/6$.

Selection stage:

Let $y_0 \in F_{p_t}$ be a point than there is a unique point x_0, so that $(x_0, y_0) \in E/F_{p_t}$.

First transformation stage:

Let $1+\delta \in F_{p_t^2}$ be a solution for the equation $x^3 - 1 = 0 \bmod p_t$. A transformation of the equation $\gamma(x, y) = (\delta x, y)$ is an automorphism of groups on elliptic curve E. If $G = (x, y) \in E/F_{p_t}$ then $\gamma(G) \in E/F_{p_t}$.

Determination stage:

The points $G, \gamma(G)$ generates a group morphism $Z_m \times Z_m$. We note this group of points as being $E[m]$. These points can be computed as in [6, 7].

Second transformation stage:

In order to encrypt the plain text will be made a concatenation between the ID of whom will receive the message and the string obtained from the encryption function. To transform the key K_T we need a string of code. For this the beginning sequence of the code (according to ASCII code) will be $ST^{(1)} \in \{0,1\}^*$. Using a cryptographic function, noted with $Q : \{0,1\}^* \to F_{p_t^*}$ we construct the point $A : y_0$ which will be equal to $Q(ST^{(1)})$ and $x_0 = (y_0^2 - 1)^{1/3} = (y_0^2 - 1)^{(2p_t-1)/3} \bmod p_t$. So $A = (x_0, y_0) \in E/F_{p_t}$, and we compute $A_{ST^{(1)}} = 6A$ in order to get the necessary order for A.

4.1. Transmission and validity of the key. Following the ideas from the previous paragraphs, ST is made by concatenating the full name of a participant. This means that the key exchange is required at a certain time and when a participant leaves the group to deny unauthorized access to information. The validity period for a key pair (public key and private key) is very small if we want as result a high-level security.

4.2. Functional scheme. Next we want to describe the four steps of the algorithm which ensure privacy and data integrity.

Setup

As we previous described, we chose an elliptic curve E generated by the instrumentality of an prime number $p_t, p_t = 6m - 1$, where the prime number is $m, m > 3$. We chose $G \in E/F_{p_t}$ in accordance with the key transformation $ST - K_T$. Also, we select $s \in Z_*^{p_t}$ and $G_{pub} = sG$. The master key is $s \in Z_*^{p_t}$.

The extraction

As we saw, the public key generator will construct a private key, through the expression: $Q(ST^{(1)}) = ST^{(2)} \in \{0,1\}^*$. From this follows $A_{ST^{(2)}} \in E/F_{p_t}$ of order m. The private key will be $d_{ST^{(2)}} = sA_{ST^{(2)}}$, where s is the master key.

Encryption

Let M be a simple text used by an sender, participant to the encryption process. The encrypted text C will be obtained as being $(rG, M \oplus Q(A'))$, where $A = (A_{ST^{(2)}}, G_{pub}) \in F_{p_t}$ and r is chosen randomly, $r \in Z_{p_t}$.

Decryption

We have $B = (U, V)$, an encrypted text with a public key $A_{ST^{(2)}}$. We will again obtain the simple text from the encrypted text by the following method: $M = V + Q(J)$, where $J = (d_{ST^{(2)}}, U) \in F_{p_t^2}$.

4.3. The system's security. It has been shown that the security of the system is given by the security of the public key system based on elliptic curves. These aspects are described in detail and demonstrated in [4, 22]. The method used to create and generate the public key and the private key does not offer the advantage that attackers cannot break the security of various systems, but, given the fact that it is based on numbers generated by elliptic curves it will be an rather secured system. It has been shown that security systems based on numbers generated by an elliptic curve are currently the most secure cryptographic systems.

5. Conclusion

In this paper we presented the advantages of using the particular subspaces of elliptic curves, instead of the entire ones, in cryptographic applications, with the description of an encryption system based on elliptic curves for a particular space F_{p_t}. This system represented a higher level method for ensuring data confidentiality in a group communication by using a subspace which requires a larger volume of calculations in order to penetrate the encryption system.

Future studies will be made in the direction of defining the computation time for the keys in such subspace, for a certain nonsupersingular elliptic curve, which has direct application in Digital Declaration. The main point of the research is based on figure the nonlinearity of subspaces, from cryptographic point of view.

References

[1] R. Alsaedi, N. Constantinescu, and V. Rădulescu, Nonlinearities in Elliptic Curve Authentication, *Entropy* **16** (2014), no. 9, 5144-5158; doi:10.3390/e16095144.

[2] J. Alves-Focs, *An Eficient Secure Authenticated Group Key Exchange Algorithm for Large and Dynamic Groups*, grant from DOE.

[3] G. Balaiah, and Dr.V. Srinivasa Rao, *A protocol for Authenticated Group Key Transfer Based on Secret Sharing*, (IJAEST) *International Journal of advanced engineering sciences and technologies* **8** (2013), no. 2, 256–260.

[4] I.F. Blake, G. Seroussi, and N.P. Smart, *Elliptic Curves in Cryptography* Cambridge University Press, 2000.

[5] E. Bresson, O. Chevassut, and D. Pointcheval, *Provably Authenticated Group Diffie-Hellman Key Exchange The Dynamic Case*, C. Boyd (Ed.): ASIACRYPT 2001, **LNCS 2248**, 290–309, Springer-Verlag Berlin Heidelberg, 2001.

[6] D. Boneh, and M. Franklin, *Identity-Based Encryption from the Weil Pairing*, CRYPTO 2001, **LNCS 2139**, 213-229, Springer-Verlag Berlin Heidelberg, 2001.

[7] D. Boneh, and M. Franklin, *Identity based encryption*, Full version available at http://crypto.stanford.edu/ibe.

[8] N. Constantinescu, G. Stephanides, M. Cosulschi, and M. Gabroveanu, RSA-Padding Signatures with Attack Studies, In *International Conference on Web Information Systems and Technologies: Internet Technology/Web Interface and Applications*, INSTICC Press Setubal, Portugal, 2006, (J.A. Moinhos Cordeiro and V. Pedrosa, B. Encarnacao, and J. Filipe, eds.), 97–100.

[9] N. Constantinescu, C. Boldea and C. Boboila, Elliptic Curves Cryptosystems for ECommerce Applications, *Conference on Recent Advances in Mathematics and Computers in Business, Economics, Biology & Chemistry*, 2010, 216–221.

[10] N. Constantinescu, Security System Vulnerabilities, In *Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science* **13** (2012), no. 2, 175–179.

[11] M. Cosulschi, M. Gabroveanu, and N. Constantinescu, Usage of advanced data structure for improving efficiency for large (n;m) permutations inspired from the Josephus problem, *Romanian Journal of Information Science and Technology* **12** (2009), no. 1, 13–24.
[12] A. Chandrasekar, V.R. Rajasekar, and V. Vasudevan, Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography, *International Journal of Computer Science and Security* (IJCSS) **3** (2009), no. 4, 325–333.
[13] I. Duursma, and H.-Sook Lee, *A group key agreement protocol from pairings*, Elsevier, Applied Mathematics and Computation **167**, (2005.
[14] S. Han, W. Liu, and E. Chang, Deniable Authentication Protocol Resisting Man-in-the-Middle Attack, *International Journal of Information Technology* **1** (2004), no. 4, ISSN:1305-239X.
[15] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Crytography*, New York, USA:LNCS, Spring-Verlag, 2004.
[16] M. Hutter, RFID Authentication protocols based on elliptic curves. A Top-Down Evaluation Survey, SECRYPT 2009 - *International Conference on Security and Cryptography*, 2009, 101–110.
[17] I. Iancu, and N. Constantinescu, Intuitionistic fuzzy system for fingerprints authentication, *Applied Soft Computing* **13** (2013), no.4, 2136–2142.
[18] J. Kar, and B. Majhi, An Efficient Password Security of Multi-Party Key Exchange Protocol based on ECDLP, *International Journal of Computer Science and Security* (IJCSS) **3**, no. 5.
[19] S. Laur, and S. Pasini, *SAS-Based Group Authentication and Key Agreement Protocols*, (R. Cramer, Ed.): PKC 2008, **LNCS 4939**, 2008, 197–213, International Association for Cryptologic Research 2008.
[20] Y. Sun, Q. Wen, H. Sun, W. Li, Z. Jin, and H. Zhang, An Authenticated Group Key Transfer Protocol Based on Secret Sharing, *Procedia Engineering* **29** (2012), 403–408.
[21] G. Stephanides, and N. Constantinescu, Identification of parts in identity-based encryption, In *Advandces in Learning, Commerce and Security* (K. Morgan, and J.M. Spector, Eds.), **30**, 2004, 177–183.
[22] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, *Proc. Eurocrypt* 2001.
[23] A.E. Western and J.C.P. Miller, *Table of Indices and Primitive Roots*, Royal Society Mathematical Tables **9**, Cambridge Univ. Press, 1968.

(Oana Adriana Ţicleanu) Doctoral School of Exact Sciences, University of Craiova
Street: A.I. Cuza, No:13,
Craiova, Romania
E-mail address: oana.ticleanu@inf.ucv.ro