Electronic Journal of Differential Equations, Vol. 2017 (2017), No. 20, pp. 1–8.
ISSN: 1072-6691. URL: http://ejde.math.txstate.edu or http://ejde.math.unt.edu

APPLICATION OF DIFFERENTIAL CRYPTOGRAPHY TO A GN AUTHENTICATION HIERARCHY SCHEME

ALIN IONUŢ GOLUMBEANU

Communicated by Vicentiu Radulescu

Abstract. Starting from the classical differential cryptography, we describe how to construct particular parameters for elliptic curves with application to the domain of information security. These results conclude to a key used on symmetrical encryption. The article will review a solution in which the parties are authenticated based on a secret knowledge and a random parameter.

1. Introduction

Communication secrecy mainly depends on the generation and distribution of the master key. The keys generation stage relies on the computation of some differential parameters over a particular elliptic curve.

This system is useful when a symmetrical encryption key is used for the messages, and an agreement on a ciphering key (the session key), based on public keys encryption, is made. The initial idea which led to the development of the identity based system belongs to Shamir [5, 8], whose aim was to create a method that ensures confidentiality. Let Alice and Bob be the two parties who want to communicate. Both have an e-mail address. When Alice wants to send a message to Bob, she will be accessing a server which stores Bob's public key, and she will use this key to encrypt information. The server will store for both parties the private and public keys. A key request will take place when the server receives a message which contains the e-mail address of the one who's public key is asked for. Shamir simplified the system by introducing a function, denoted by χ, which generates a public key based on a random string (e-mail address). In this way, Alice will not be requesting the key from the server anymore, instead she will use the key which was generated by the χ function. The usefulness of the system resides in the fact that one can encrypt and send messages to somebody on the network even if the password server is unavailable. It also eliminates the need to gain access to the password server for the dialog's counterpart. A series of algorithms and protocols which are based on this system have been developed [4, 6, 7, 9, 19]. Not all of them can be used in real life due to the burden that some of these algorithms and protocols impose on modern computing systems.

2010 *Mathematics Subject Classification.* 35H20, 35S15, 12H20, 11G07.
Key words and phrases. Agreed session key; elliptic curves; public key based encryption; identity based encryption.

Submitted August 12, 2016. Published January 16, 2017.

2. Proposed Scheme

The description of identity is based on the confidentiality of the system. In [2, 3, 14, 20], there have been elaborated some series of identity based systems. Those solutions are composed of the following parts:

(1) *The system's setup.*
To each dialoguing party the Password server assigns a control key, called ID. This key is used by the Password server to communicate with its users. The Password server will be called PKG (*Public Key Generator*) from now on.

(2) *Encryption.*
A participant, called A, who wants to communicate with another (called B), will encrypt the message, which will be sent out with a public key, called p_k, obtained from the morphing, through function χ, of a string s which contains B's identifier (which can also be B's address).

(3) *Decryption.*
A system user who will receive such messages will access the PKG and, based on his ID, will obtain the private key with which he can decrypt the message.

In the eventuality in which the line is listen to, the eavesdropper will gain access only to the encrypted message.

2.1. Elliptic curve based system.

We consider the function

$$f(x) = \int \frac{dx}{\sqrt{4x^3 - ax - b}} \tag{2.1}$$

where a and b are constants. The inverse of this function is called an elliptic curve. Let γ_1 and γ_2 be two constants, and a double periodic function over $\mathbb{R}$. Then the Weierstrass function is of the form

$$(\alpha')^2 = 4\alpha^3 - \gamma_1\alpha - \gamma_2. \tag{2.2}$$

The pair (α, α') defines in space a point on the elliptic curve

$$y^2 = 4x^3 - \gamma_1 x - \gamma_2. \tag{2.3}$$

We refer to [3] for more results.

Definition 2.1 ([5])**.** Let $p > 3$ be a prime integer. The elliptic curve $y^2 = x^3 + \gamma_1 x + \gamma_2$, defined over $\mathbb{Z}_p$, is being defined as the solution set of the form $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ with respect to the congruence relation

$$y^2 \equiv x^3 + \gamma_1 x + \gamma_2 \mod p \tag{2.4}$$

where the coefficients $\gamma_1, \gamma_2 \in \mathbb{Z}_p$ are constants which respect the relation

$$4\gamma_1^3 + 27\gamma_2^2 \not\equiv 0 \mod p \tag{2.5}$$

together with a special point, called point at infinity

Lemma 2.2 ([13])**.** Let E be an elliptic curve defined as

$$Y_2 + \gamma_1 XY + +\gamma_3 Y = X^3 + \gamma_2 X^2 + \gamma_4 X + \gamma_6 \tag{2.6}$$

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

$$-A_1 = (x_1, -y_1 - \gamma_1 x_1 - \gamma_3) \tag{2.7}$$

and

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \gamma = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \tag{2.8}$$

where x_1, x_2 satisfy the condition $x_1 \neq x_2$ and from here results

$$\lambda = \frac{3x_1^2 + 2\alpha_2 x_1 + \alpha_4 - \alpha_1 y_1}{2y_1 + \alpha_1 x_1 + \alpha_3}, \quad \gamma = \frac{-x_1^3 + \alpha_4 x_1 + 2\alpha_6 - \alpha_3 y_1}{2y_1 + \alpha_1 x_1 + \alpha_3}. \tag{2.9}$$

In the case x_1 equals x_2, the points A_1 and A_2 being unequal, the addition of the two points will be done as

$$x_3 = \lambda^2 + \alpha_1\lambda - \alpha_2 - x_1 - x_2, \; y_3 = -(\lambda + \alpha_1)x_3 - \gamma - \alpha_3 \tag{2.10}$$

With respect to this lemma, we distinguish the following two cases:

(1) $x_2 = x_1$ and $y_2 = y_1$. In this case, $A_1 + A_2 = O$.
(2) In all other cases we have $A_1 + A_2 = B = B(x_3, y_3)$, where

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1 \tag{2.11}$$

and

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & A_1 \neq A_2; \\ (3x_1^2 + a)(2y_1)^{-1}, & A_1 = A_2. \end{cases} \tag{2.12}$$

Optimization of Elliptic Curves Parameters. In practice there are used elliptic curves defined over a finite field F_q, which means that the study will be made on an Abelian group.

Let s be 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

$$\varphi = \begin{cases} E(\overline{F}_q) \to E(\overline{F}_q) \\ (x, y) \to (x^q, y^q) \\ \mathbf{O} \to \mathbf{O} \end{cases} \tag{2.13}$$

An approximation of the number of points on an elliptic curve is given by the Hass theorem. In this way, t must fulfil the condition

$$|t| \leq 2\sqrt{q} \tag{2.14}$$

To compute the addition of two points on a elliptic curve in finite fields one of the solutions will be Weil pairing implementation. Let K be a finite field and an elliptic curve defined over 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 2.3 ([14]). *Let E be an elliptic curve over F_q and m be 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 if m divides $q^k - 1$*

According to [10, 15, 23] 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

$$\operatorname{div}(g) = \sum_{D \in E[m]} (B_1' + D) - (D) \tag{2.15}$$

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

$$e_m = \begin{cases} E[m] \times E[m] \to \gamma_m \\ (B_1, B_2) \to \frac{g(X+B_1)}{g(X)} \end{cases} \tag{2.16}$$

In the case of the implementation in computing systems of a subfield curve, of type F_{q^n}, n must be greater than 1 and the coefficients from F_q. We will define [12, 13] 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 satisfy equation

$$\varphi^2 - [t]\varphi + [q] = [0] \tag{2.17}$$

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 $|K| \leq \lfloor q/2 \rfloor$.

Model implementation. Regarding the implementation of an hierarchical information's access, a function which would generate a public key based on the conjugated information, from the corresponding hierarchy level and the communication channel's user's custom string, must be defined. Let be a function of the form

$$\varphi(\text{level}, \text{string}) = \text{public key} \tag{2.18}$$

where level represents the access level of an user and string represents a character string which characterizes the communication's participant.

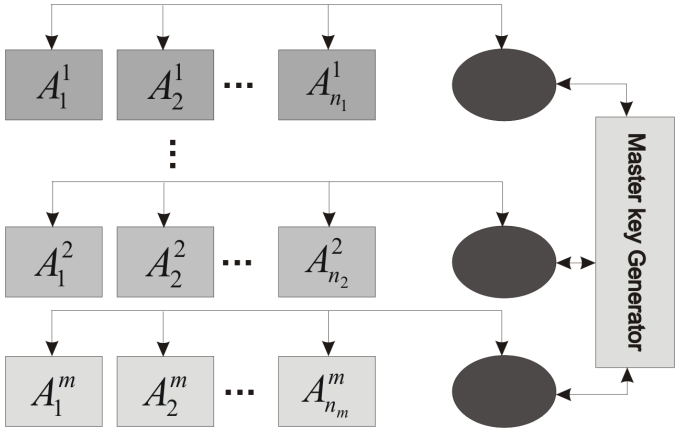

FIGURE 1. Users grouped in a hierarchical order

In Figure 1 is being shown the way in which users are being grouped in a hierarchical order. The basic principle of the hierarchy is to respect the information's access rights by the users from the same level. Every member of the network will define a point $A_i^j \in E$, where j represents the hierarchical level of each user. For every session, in order to obtain the private key from the key server, it will be used the GN_1 algorithm, and resulting from the creation of a session key, the private key will also be generated. One must take into account the security facts described in [1, 16, 17, 18].

GN_1 **Group Protocol.** Now we present the way to achieve the agreed key, for each (A_i, A_j) participants pair and from it will be created a common key group, in the assumption of security level which are presented and proved in a previous work, detailed in [11, 21, 22]. To describe those cases let as consider the following:

- $\pi_{K_{A_i}}$ - the secret key of A_i
- $\pi_{P_{A_i}}$ - the public key of A_i
- $\eta^d_{A_i}(\pi_{K_{A_i}}, m)$ - the encryption of message m with A_i's secret key
- $\eta^e_{A_i}(\pi_{P_{A_i}}, m)$ - the encryption of message m with A_i's public key
- $\text{enc}(s_K, m)$ - the symmetric key encryption of message m with key s_K
- $\inf_{A_i}$ - the pseudorandom generated value by A_i for every session
- $E(\mathbb{Z}_p)$ - the elliptic curve defined over $\mathbb{Z}_p$
- M - the messages space
- $hf(\cdot)$ - the $SHA-1$ hash function
- $m_1|m_2$ - the concatenation of the m_1,m_2 messages, when m_1, $m_2 \in M$

A system user, denoted as A_i, has the next public parameters:

- $(\pi_{P_{A_i}}, E(\mathbb{Z}_p), P, Q, n)$, where $P, Q \in E(\mathbb{Z}_p)$

Also, the function $\eta^d_{A_i}(\pi_{K_{A_i}}, m)$, $\eta^e_{A_i}(\pi_{P_{A_i}}, m)$ and $hf(\cdot)$ are public. For the user A_i, the following are private:

- $\pi_{K_{A_i}}$ and $\inf_{A_i}$

From those, the steps are defined in the next manner:
The Protocol

- A_i
  (1) generates a pseudo-random number $\inf_{A_i} \in [1, n-1]$
  (2) calculates $A_i^1 = \inf_{A_i}(P^{-1} + Q) = (x_1^{A_i}, y_1^{A_i})$. Let $x = x_1^{A_i}$ *mod* n. If $x = 0$ then *goto* step 1
  (3) calculates $A_i^2 = hf(P_{A_i}|A_i^1)$
  (4) calculates $A_i^3 = \eta^d_{A_i}(\pi_{K_{A_i}}, A_i^2)$
  (5) **The first communication step (from A_i to A_j)**
  A_i sends to A_j $(A_i^1|A_i^2)$
- A_j
  (1) calculates $A_j^1 = hf(P_{A_i}|A_i^1)$
  (2) calculates $A_j^2 = \eta^e_{A_i}(\pi_{P_{A_i}}, A_i^2)$. If $A_j^1 \neq A_j^2$ terminates the protocol run with failure.
  (3) Generates pseudo random number $\inf_{A_j} \in [1, n-1]$
  (4) calculates $A_j^1 = \inf_B(P^{-1} + Q) = (x_1^{A_j}, y_1^{A_j})$. If $x_1^{A_j} = 0$ go to step 3 of A_j's steps
  (5) calculates $A_j^2 = hf(P_{A_j}|A_j^1)$
  (6) calculates $A_j^3 = \eta^d_{A_j}(\pi_{K_{A_j}}, A_j^2)$
  (7) $K_{A_j} = \inf_{A_j} A_i^1 = (x_2^{A_j}, y_2^{A_j})$
  (8) $x = x_2^{A_j} \bmod n$. If $x = 0$ then go to step 3 of A_j's steps
  (9) **The second communication step (from A_j to A_i)**
  A_j sends to A_i $(A_j^1|A_j^3)$
- A_i

6 calculates
$s_1^{A_i} = hf(P_{A_j}, A_j^1)$
$s_2^{A_i} = \eta_{A_j}^e(\pi_{P_{A_i}}, A_j^3)$
7 if $s_1^{A_i} \neq s_2^{A_i}$ terminates the protocol run with failure
8 $K_{A_i} = \inf_{A_i} A_j^1$

Three step protocol. Starting from the exposed protocol, as follows the three-steps protocol which assures the confirmation of the key by A_i. This protocol is analogous with the previous one, adding a supplementary step.

Therefore, A_i will compute $hf((\inf_{A_i}(P^{-1}+Q))|\operatorname{enc}(K_{A_i}, \inf_{A_j}(P^{-1}+Q)))$ and send it to A_j. At this point, A_j will check the equality:

$$\begin{aligned} &hf((\inf_{A_i}(P^{-1}+Q))|\operatorname{enc}(K_{A_i}, \inf_{A_j}(P^{-1}+Q))) \\ &= hf((\inf_{A_i}(P^{-1}+Q))|\operatorname{enc}(K_{A_j}, \inf_{A_j}(P^{-1}+Q))). \end{aligned}$$

If the equality returns successfully, the key is confirmed.

In the implementation, we used a *confirmation step*, in order to increase the sped, because in case of fail the protocol will restart from the beginning. Statistically, the necessary time to do this step is less than the spent time for restart the protocol.

Therefore we define

$$h'_{int}(h(K)) \tag{2.19}$$

with $h'_{int} : M \to N$, where h' will generate an integer: $h'_{int}(h(K)) = t, t \in N$, and t must accomplish $t \leq \sqrt{2}n$

Let $L_{t;0\leq t\leq m}$ be the hierarchy levels. The key for each user A_i^t will be made in two steps. First, the authentication step, which is done in the first protocol, and second, by authenticated key, made by the supplementary step from the second protocol. The assumption of this scheme is that the key will be established from M_t^i (the master key from the server, where t is the level and i is the user) and the user A_i knowledge.

2.2. **Conclusions.** In this article it is described a way in which the communication channel of the user access to information can be grouped in a leveled hierarchy. The problems known to this type of system are related to the length of the messages exchanged by the participants, based on the same string structure. In fact, in practice a time-stamp is used, but this is not always the case because when wide-band consumers are involved the most important thing is about thing is the computing time and the way to produce the time-stamp for each group. The proposed model limits the number of valid messages that can be transmitted, with the same personalization string of an user, by a amplification factor which takes into account the frequency of the communication between the Key Generator and the control points of each level.

Acknowledgments. The author acknowledges the support through Grant of The Executive Council for Funding Higher Education, Research and Innovation, Romania-UEFISCDI, Project Type: Advanced Collaborative Research Projects - PCCA, Number 23/2014.

References

[1] N. Constantinescu; The agreement of the common key, *Annals of the University of Craiova - Mathematics and Computer Science Series*, Vol. **30**(2), pp. 59–65, 2003.

[2] N. Constantinescu, G. Stephanides; Identification of parts in identity-based encryption, *Research Notes in Data Security, Wessex Institute of Technology*, UK, developed with University of Bergen, Norway, ISBN 1-85312-713-2, 2004.

[3] N. Constantinescu, G. Stephanides; Secure Key-Exchange, *Recent Advances in Communications and Computer Science*, Vol. **7**, pp. 162–166, Greece, 2003.

[4] A. Miyaji, M. Nakabayashi, S. Takano; New explicit condition of elliptic curve trace for FR-reduction, *IEICE Trans. Fundamentals*, Vol. **E84 A**(5), May 2001.

[5] A. Shamir, Identity-based cryptosystems and signature schemes, *Advances in Cryptology, LNCS*, Vol. **196**, Springer-Verlag, pp. 47–53, 1984.

[6] I. Iancu, N. Constantinescu, M. Colhon; Fingerprints Identification using a Fuzzy Logic System, *International Journal of Computers, Communications & Control*, Vol. **5**(4), pp. 525–531, 2010.

[7] H. Tanaka; A realization scheme for identity-based cryptosystem, *Advances in Cryptology, LNCS*, Vol. **293**, Springer-Verlag, pp. 341–349, 1987.

[8] E. Simion, N. Constantinescu; Complexity Computations in Code Cracking Problems, *Concurrent Engineering in Electronic Packaging, IEEE Communication*, May 05-09, pp. 225–232, ISSE 2001.

[9] N. Constantinescu, G. Stephanides, M. Cosulschi, M. Gabroveanu; RSA-Padding Signatures with Attack Studies, *International Conference on Web Information Systems and Technologies: Internet Technology/Web Interface and Applications*, Portugal, ISBN 978-972-8865-46-7, pp. 97–100, 2006.

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

[11] N. Constantinescu, G. Stephanides; The GN-authenticated key agreement, *Journal of Applied Mathematics and Computation*, Elsevier, London, Vol. **170**, pp. 531–544, 2006.

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

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

[14] N. Constantinescu; Authentication ranks with identities based on elliptic curves, *Annals of the University of Craiova, Mathematics and Computer Science Series*, Vol. **XXXIV**(1), pp. 94–99, 2007.

[15] O. Ticleanu, N. Constantinescu, D. Ebanca; Intelligent data retrieval with hierarchically structured information, *KES-IIMS*, Vol. **254**, pp. 345–351, Jun 26-28, Portugal, 2013.

[16] O. Ticleanu; Endomorphisms on elliptic curves for optimal subspaces and applications to differential equations and nonlinear cryptography, *Electronic Journal of Differential Equations*, Vol. **2015**(14), pp. 1–8, 2015.

[17] O. Ticleanu, N. Constantinescu; Studying models issues on e-commerce cashing, *International Conference on Applied Mathematics and Computational Methods in Engineering II* (AMCME '14), pp. 116–128, 2014.

[18] O. Ticleanu; Nonlinear analysis on elliptic curves subspaces with cryptographic applications, *Annals of the University of Craiova, Mathematics and Computer Science Series*, Vol. **41**(2), pp. 292–299, 2014.

[19] N. Constantinescu; Security System Vulnerabilities, *Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science*, Vol. **13**(2), pp. 175–179, 2012.

[20] R. Alsaedi, N. Constantinescu, V. Radulescu; Nonlinearities in Elliptic Curve Authentication, *Entropy*, Vol. **16**(9), pp. 5144–5158, 2014.

[21] O. Ticleanu; Mathematical models in cryptography, *Journal of Knowledge Communication and Computing Technologies*, Vol. **4**(1), pp. 1–7, 2013.

[22] O. Ticleanu; Differential operators over particular elliptic curves spaces with cryptographic applications, *Electronic Journal of Differential Equations*, Vol. **2015**(303), pp. 1–9, 2015.

[23] N. Constantinescu; Authentication hierarchy based on blind signature, *Journal of Knowledge Communication and Computing Technologies*, Vol. **1**(1), pp. 77–84, 2010.

Alin Ionuţ Golumbeanu
University of Craiova, Street: A.I. Cuza 13, 200585 Craiova, Romania
E-mail address: alin.golumbeanu@inf.ucv.ro