

Identification of parts in identity-based encryption

G. Stephanides¹ & N. Constantinescu²

¹*Department of Applied Informatics, University of Macedonia, Greece*

²*Department of Informatics, University of Craiova, Romania*

Abstract

After Shamir proposed his scheme, other authors proposed many Identity-Based Encryptions. The models were assumed in the random oracle model with a variant of the computational Diffie-Hellman problem. In our paper we propose a new variant of Identity-Based Encryption (IBE), using elliptic curves schemes and prove his security completeness. Also, we are doing a complete description of the necessary system used in the present scheme in order to secure a communication. The performance of our system is comparable to the performance of ElGamal encryption in F_p^* and the security of the system is based on the elliptic curve calculus intractability.

Keywords: identity-based encryption, Diffie-Hellman problem, elliptic curves cryptography, Escrow ElGamal.

1 Introduction

In the last twenty years many authors have developed security algorithms of information based on making the Public Key System that has an equivalent in an identity system, Shamir [1]. Initially, this system was created in order to assure the confidentiality of the communication between a member of a group who knows some identity information of another member and is going to communicate with him. This is, for example, the email address, the surname, the first name, a code on the identity card, etc. Informally, this kind of scheme consists of the following algorithms:

- (a) Setup: generates the control parameters in order to identify the users and creates the master key.



- (b) Extract: it uses the master key in order to generate the private key corresponding to public key that was generated in function of the Identity String (IS).
- (c) Encrypt: the description of the encryption algorithm that will be applied on the plain text. It uses the public key.
- (d) Decrypt: the decryption algorithm of the ciphered message. It uses the corresponding private key.

Many of other proposed schemes, [2, 3, 4, 5], use a considerable quantity of processor-time in order to calculate the private key, or they consider a dedicated hardware as being pre-existent.

To describe in this paper our model, we'll first illustrate a general model of the scheme. This model is based on the creation of the public key, which is not necessary to be taken from a server. By convention, it considers that the public key is made by the concatenation of the complete name of the receiver and the current week. So, we obtain the IS (Identity String). It will create an algorithm that transforms some kind of string in a key and this key will become the encryption public key used to encrypt the plain text and it will be sent through the communication channel.

The receiver will request the private key from the Private Key Generator (PKG). This private key is corresponding to the public key that is characteristic to this user (receiver). The decryption will be produced with this key, so Private Key Generator holds the control of all the decryption keys and the public keys associated with every user. To communicate with Private Key Generator, any participant has a secret code that is also known by the PKG. It is used to assure the Challenge-Response algorithm in order to make the secure communication between PKG and any participant.

2 Our secure IBE scheme

In this part of the article we describe the modality of secure information that will be transferred to another participant through the communication channel. This scheme has four parts:

Setup

Every participant of the group has a control key, a personal parameter noted ID, known by himself and by a trusted authority, the Private Key Generator. It is used to assure the secure communication between him and PKG.

Extract

Using the personal parameter ID and a message key communicates the private key for the participant. The private key will be generated by the PKG at the request of a participant authenticated by an ID.

Encryption

Another participant, using the transformation algorithm of an identity string (IS) in a public key $pk \in \{0, 1\}^*$, will encrypt the plain text with this key and the cipher text obtained in such a way will be transferred through the communication channel.



Decryption

Using the private key, obtained from the Private Key Generator, one participant will decrypt a message that is destined to him.

As we already have mentioned, the algorithm used to obtain the private key from the Private Key Generator is of a Challenge-Response type. Therefore, for its construction we'll use, in the same way as in Boneh and Franklin [6, 7], the following phases:

Definition

The expression $x^3 + 1$ is a permutation of F_p , where E is an elliptic curve given by the equation $y^2 = x^3 + 1$, defined over F_p , and p is a prime number that satisfies $p = 6q - 1$, where q is a prime number, $q > 3$.

Let $P \in E / F_p$ be a generator in a group of points of order $q = (p+1)/6$.

Choice

For an integer coordinate $y_0 \in F_p$, there is a unique integer coordinate x_0 , so that $(x_0, y_0) \in E / F_p$.

Transformation

Let $(1 + \zeta) \in F_{p^2}$ be a solution of the equation $x^3 - 1 \equiv 0 \pmod{p}$. A transformation equation $\phi(x, y) = (\zeta x, y)$ is a group automorphism on the elliptic curve E . If $P = (x, y) \in E / F_p$, then $\phi(P) \in E / F_{p^2}$, but $\phi(P) \notin E / F_p$.

Determination

The points $P, \phi(P)$ generate an isomorphic group $Z_q \times Z_q$. We note this group of points by $E[q]$. These points can be calculated as in Boneh and Franklin [6, 7].

Transformation IS-PK

The public key, which will encrypt the plain text, is made from a string obtained through the concatenation of the complete name of the receiver and the current weak. Once we have a string, it is necessary to transform it in a key, PK. For this reason, at the beginning, we code the string (in accordance with *ASCII*) to obtain $IS^{(1)} \in \{0, 1\}^*$. Using a cryptographic hash function, $H : \{0, 1\}^* \rightarrow F_p$, we construct the point $Q(x_0, y_0)$: y_0 will be equal to $H(IS^{(1)})$ and $x_0 = (y_0^2 - 1)^{1/3} \equiv (y_0^2 - 1)^{(2p-1)/3} \pmod{p}$. Thus, $Q(x_0, y_0) \in E / F_p$, and we compute $Q_{IS^{(1)}} = 6Q$ in order to obtain the necessary order of Q (this is denoted in [6, 7], as being a random oracle model).

2.1 Lifetime of key and key transmission

As we pointed out before, IS is made by the concatenation of the complete name of a participant and the current weak. This means that the key will be changed in



every weak. Therefore, the validity of a pair of the key (public key and private key) is maintained only for one weak.

2.2 The functional scheme

In this part of the article we will describe the four steps of the algorithm that assures the confidentiality of the communication.

Setup

As we described before, we chose an elliptic curve E generated through a prime number p , $p = 6q-1$, and a prime number q , $q > 3$. We chose $P \in E / F_p$ according to the transformation IS-PK. Also, we select $s \in Z_q^*$ and $P_{pub} = sP$. The master key is $s \in Z_q^*$.

Extract

Once we have $IS^{(1)} \in \{0, 1\}^*$, the Private Key Generator will construct a private key, therefore: $H(IS^{(1)}) = IS^{(2)} \in \{0, 1\}^*$. From this point it results that $Q_{IS^{(2)}} \in E / F_p$ of order q . The private key will be $d_{IS^{(2)}} = sQ_{IS^{(2)}}$, where s is the master key.

Encrypt

Let be T the plain text to be encrypted by a sender. The ciphered text C will be obtained as being $(rP, T \oplus H(Q^r))$, where $Q = (Q_{IS^{(2)}}, P_{pub}) \in F_{p^2}$ and r is chosen with random oracle, $r \in Z_q$.

Decrypt

We have $C = (U, V)$ a ciphered text with the public key $Q_{IS^{(2)}}$. We'll obtain again the plain text from the ciphered text as follows: $T = V + H(R)$, where $R = (d_{IS^{(2)}}, U) \in F_{p^2}$.

2.3 Security

The security of the system is given by the security of public keys system based on elliptic curves. These notions are described in detail and proved in Blake *et al* [8] and Verheul [9]. The mode of creation of the public key and private key doesn't offer advantages in the determinations of plain text to any attacker.

3 Conclusions and future work

In this paper, the authors proposed a new encryption scheme of *IBE* type based on elliptic curves. This scheme represents a powerful method to assure the confidentiality of communication in a group that has a *PKG*. The advantages are given by the facility of the generation of the private and public keys and by the fact that a user A that wants to send a message to another participant B , doesn't allow to establish a link with *PKG* in order to obtain the public key of B . It is



enough to know the name of B . Also, only PKG knows about the key system of every user and the code allocated to everyone.

As a first application, we want to implement this scheme in a network with 163 systems. The next step consists of the creation of an hierarchy system in the network, in order to have access to the information, so that any user is able to read all the messages that circulate in the tree, between the users who are hierarchies situated in their descendant nodes of the tree.

References

- [1] Shamir, A., Identity-based cryptosystems and signature schemes. *Advances in Cryptology - CRYPTO '84, Lecture Notes in Computer Science*, vol. 196, Berlin: Springer Verlag, pp. 47--53, 1985.
- [2] Desmedt, Y. & Quisquater, J. , Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?). *Advances in Cryptology - CRYPTO '86, Lecture Notes in Computer Science*, vol. 263, Springer Verlag: Heidelberg, pp. 111-117, 1986.
- [3] Tanaka, H., A realization scheme for the identity-based cryptosystem. *Advances in Cryptology - CRYPTO '87, Lecture Notes in Computer Science*, vol. 293, Springer Verlag: Heidelberg, pp. 341-349, 1987.
- [4] Tsuji, S. & Itoh, T., An ID-based cryptosystem based on the discrete logarithm problem. *IEEE Journal on Selected Areas in Communication*, vol. 7, no. 4, pp. 467-473, 1989.
- [5] Maurer, U. & Yacobi, Y., Non-interactive public-key cryptography. *Advances in Cryptology - EUROCRYPT '91, Lecture Notes in Computer Science*, vol. 547, Springer Verlag: Heidelberg, pp. 498-507, 1991.
- [6] Boneh, D. & Franklin, M., Identity-Based Encryption from the Weil Pairing. *Advances in Cryptology - CRYPTO '01, Lecture Notes in Computer Science*, vol. 2139, Springer-Verlag: Heidelberg, pp. 213-229, 2001.
- [7] Boneh, D. & Franklin, M., Identity based encryption. Full version available at <http://crypto.stanford.edu/ibe>.
- [8] Blake, I.F., Seroussi, G. & Smart, N.P., *Elliptic Curves in Cryptography*, Cambridge University Press, 2000.
- [9] Verheul, E., Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Advances in Cryptology - EUROCRYPT '01, Lecture Notes in Computer Science*, vol. 2045, Springer Verlag: Heidelberg, pp. 195-210, 2001.

