Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 5 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# Identity-based Cryptosystem based on tate Pairing

By Ramesh Ch, K Venugopal Rao & D Vasumathi
*GNITS*

*Abstract-* Tate Pairings on Elliptic curve Cryptography are important because they can be used to build efficient Identity- Based Cryptosystems, as well as their implementation essentially determines the efficiency of cryptosystems. In this work, we propose an identity-based encryption based on Tate Pairing on an elliptic curve. The scheme was chosen ciphertext security in the random oracle model assuming a variant of computational problem Diffie-Hellman . This paper provides precise definitions to encryption schemes based on identity, it studies the construction of the underlying ground field, their extension to enhance the finite field arithmetic and presents a technique to accelerate the time feeding in Tate pairing algorithm.

*Keywords: identity-based crytosystems, tate pair, elliptic curves and digital certificates.*

*GJCST-E Classification : E.3 D.4.6*

# Identity-based Cryptosystem based on tate Pairing

Ramesh Ch [α], K Venugopal Rao [σ] & D Vasumathi [ρ]

*Abstract -* Tate Pairings on Elliptic curve Cryptography are important because they can be used to build efficient Identity-Based Cryptosystems, as well as their implementation essentially determines the efficiency of cryptosystems. In this work, we propose an identity-based encryption based on Tate Pairing on an elliptic curve. The scheme was chosen ciphertext security in the random oracle model assuming a variant of computational problem Diffie-Hellman . This paper provides precise definitions to encryption schemes based on identity, it studies the construction of the underlying ground field, their extension to enhance the finite field arithmetic and presents a technique to accelerate the time feeding in Tate pairing algorithm.

*Keywords: identity-based crytosystems, tate pair, elliptic curves and digital certificates.*

## I. Introduction

The advent of asymmetric encryption represented a great advances in safety of computers, especially because it solved the problem of key exchange algorithms for symmetric encryption. But attacks have been taking the advantage of the fact that it does not have a guarantee on who and the true owner of a public key, so that a user can impersonate another easily by making use of a necessary mechanism of association between a public key and its owner.

To resolve this problem was created the mechanism of certified digital, that uses a hierarchical structure of certifying authorities, able to ensure properly the possession of a given public key. This mechanism works very well in open organizations such as the internet.

In 1984 a model-based cryptographic identities was proposed by Shamir [1]. This model was intended to prevent the use of Digital Certificates, using the identity of the user as its public key. This identity could be an address of e-mail, Social Security number, full name, or a combination is of these elements. The private key would be obtained through a trusted third party(TA - trust authoraty). With this, digital certificates would be necessary only in identification of this central authority, drastically reducing their use. A problem that exists in this idea is the knowledge of the private key by the central authority, needed a total expectations by the user, which requires a lot of care from practical and legal point of view.

On the other hand, does not need the entire infrastructure of hierarchical authorities for the management of the keys by making the model more simple and suitable for organizations where hierarchy and its limitations are well controlled.

Shamir developed a signature scheme based on identities, whose operation is similar to the RSA. He also speculated on the existence of a scheme that has a problem that has been solved in practice by the cryptosystem of Boneh and Franklim [2], whose safety has been rigorously demonstrated.

### a) Signature Scheme Based on Identities of Shamir

The signature scheme of Shamir based on Identities and all other forms of encryption based on identities, being divided into four steps:

1. *Setup:* this step and held by authority of expectations to generate the global parameters of the system and the master key, which will underpin that only the TA can generate private keys.
2. *Generation of private key:* this algorithm receives as input the master key and the identity of a user, returning the associated private key.
3. *Signature:* given a private key and a message, the algorithm returns the signature.
4. *Checking:* given an identity, a message and a signature, the algorithm returns true if the signature of that message matches the identity supplied, and returns false if contradicts.

## II. Introductory Concepts

### a) Security

We will now define some important issues to determine the security of an algorithm based on an additive group, as is the case of elliptic curves encryption [4]:

- *Problem of discrete logarithm:* Given Q = nP, determine n .
- *Problem Computational Diffie-Hellman:* three Data points P, aP, bP, determine abP .
- *Problem of decision Diffie-Hellman:* four Data elements P, aP, bP and cP belonging to a group G, answer true if and only if C$\cong$ ab(Mod #G).

One of the first uses of pairings was made by Joux [5]. In this article he showed how the decision has

*Author α: Dept. of Computer Science G.Narayanamma Institute of Technology and Science Hyderabad. e-mail: chramesh@gmail.com*
*Author σ: Dept. of Computer Science G. Narayanamma Institute of Technology and Science Hyderabad.*
*Author ρ: Dept. of Computer Science Jawaharlal Nehru Technological University Hyderabad.*

to be taken to issue the Diffie-Hellman can be easy through the bilinear maps, thus managed to produce an application for key sharing among three parties in a single round.

### *b) Elliptic Curves*

An elliptic curve E defined over a finite field $F_p^m$ and a set of points P = (x, y) with x,y ϵ $F_p^m$ such that $y^2 + a_1 xy+a_3y +a_2 = x^3 + a^2x^2 + a^4x + a^6$ (standard medium Weierstrass) for $a_i$ ϵ $F_p^m$ there, beyond the point at infinity, denoted by ∞.

Setting up an operation in an appropriate sum, the elliptic curve form an additive Abelian group with neutral element given by the point at infinity.

An operation widely used in elliptic curve cryptography and scalar multiplication, where a point P and coupled with it own times k to k ϵ Z. A point of order n such that an extent NP = ∞ and n the smallest positive integer this property.

## III. Identity-based Encryption

The central idea of the public key cryptographic system based on Identity is very simple, because of the fact that the public key is a numeric value without explicit direction and which can be calculated from string of any significance?. In [ 1], it was proposed that the public key can be the user's identity, such as name , email address , social security number, cell phone number, IP address , serial number of electronic devices, etc.

Is the public key is predetermined ( equal to the identity), and then calculate the secret key ? The answer to this question comes with the first model of security assumptions: there is a CA, with the following main responsibilities :

- Create and maintain safe custody of a secret master key $S_{AC}$
- Identify and record all users of the system
- Calculate the secret keys of the users
- Deliver the secret keys securely (with confidentiality and authenticity)

In 1984, Shamir described the model and algorithms for digital signature. It took almost two decades until efficient encryption algorithms were discovered and demonstrated for the identity -based model to create interest among researchers and industry.

For comparison, in Table 1, we see that the secret key is calculated according to the secret system of authority and the user's identity. For a convenient f, it is not feasible to recover the master key from the ID values . And just the authority is able to generate secret keys, so that secret itself is a guarantee that the use of ID will work in cryptographic operations involving the owners identity.

To encrypt a message to the owner ID or verify a signature ID, user ID using the identity over the public parameters of the system, They include the public key of the authority (see Figure 1).

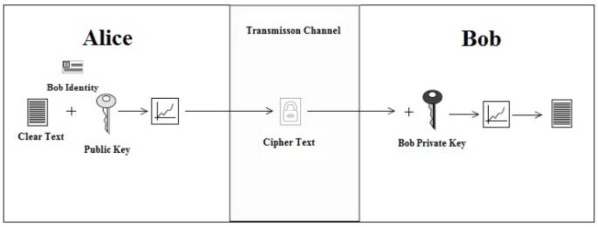
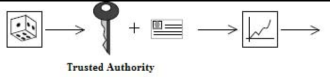


*Figure 1 :* Encrypting the model based on the identity

*Table 1 :* Attributes of cryptographic identity -based public key style

| Secret key | Public key | Warranty |
|---|---|---|
| S= f (ID, $S_{AC}$ ) | ID | S |
|  | | |
| Calculated by the authority and chosen by the user or shared with the user | Chosen by the user or shared with the user formatted for authority | |

To decrypt a message to ID or to create a signature, the secret key ID is required.

### *a) Advantages*

The identity -based model is attractive because it has many interesting advantages. The first is that the public key can in most cases be easily remembered by humans. Very different from the conventional public key, which is usually a binary string with hundreds or thousands of bits? The identity can be informed by the user to their partners and there is no requirement to maintain key directories.

To be able to view the saving processing time, storage costs and data transmissions, we will recall, for example, as It is generally a cryptographic operation with PCI. If Bob wants to encrypt a message to Alice, first of all, he must obtain the certificate that was issued to Alice (consulting a public directory or Alice itself). Bob needs check the validity period and the signature contained in the certificate. The signature verification is a process that sometimes runs the certification path of the certifying authorities involved in the hierarchy until they reach the root certification authority. If nothing goes wrong, Bob can save the Alice certificate for future use. However, before each use, Bob need to consult a validation authority to verify that the certificate has not been revoked (often, a referral to a server that is online). Once the certificate is valid and not revoked, Bob extracts the public key of Alice, encrypts the message and transmits.

In identity -based model, just if the system parameters are authentic Bob can encrypt a message based on the identity of Alice and send (considering that identity withdrawal is treated as explained below ).

A peculiarity of identity -based model is that the public key can be used before the secret key calculation. Thus, it is possible to encrypt a message for those who have not registered with the system authority or has secret key for decryption. In contrast to the model based on certificates, the user must first register and get the certificate, and then to receive an encrypted message under your public key.

### *b) Disadvantages*

The first disadvantage, which is characteristic of identity -based systems is the custody of keys. As explained above, the system authority has the ability to generate secret keys of all users under their responsibility. This implies that the authority reaches to the level of confidence that defined in [10]. Consequently, you can decrypt any encrypted texts that have access (if you can identify the recipient's identity). You can also sign on behalf of any user and there is no irreversibility guarantee. Therefore, it is essential that the system of authority is reliable enough for eavesdropping of shares or counterfeiting as these are controllable.

Custody of property keys, referenced by key escrow in English texts is not always undesirable. Within a company, for example, if all sensitive documents and data are encrypted by the employee who created it , the board may have access to decryption in case of death or termination of the employee . When there is need for monitoring the content of encrypted e-mail, it can also be justifiable custody of keys. However, for most applications, custodial key is a disadvantage.

Another point unfavourable to identity -based model is the need for a secure channel for distribution of secret keys. If delivery occurs in networked and remote environment, it is necessary to ensure mutual authentication and delivery with secrecy.

Another concern that one must have in identity -based model is the possibility of identity revocation. If the secret key of a user is compromised, its identity should be repealed. Therefore, it is not recommended to simply use the number of CPF or mobile phone, for example, as a user identifier.

### *c) Additional features*

As noted by [1], the identity -based model is ideal for groups of users, such as executives of a multinational company or branch of a bank, once the headquarters of these corporations can serve as system authority in all trust. Applications small scale, where the cost of deploying and maintaining an ICP are prohibitive, are candidates for the use of identity -based model. When the disadvantages cited above are not critical, the characteristics model allow interesting implementations.

Some examples of services with time availability confidential document that can be revealed to the press or to a particular group , only from certain date and time; bids an auction that should be kept secret until the end of negotiations ; or view a film that should be enabled only within the rental period contracted.

The identity -based model has also been the subject of studies in search for alternatives to SSL / TLS, to Web applications , as shown in [7]. With the elimination of certificates the process of distributing public keys and access control will be simplified. Similarly, the model has been explored to provide security in a number of other application areas , such as grid computing and sensor networks (see for example [5 ] and [8 ] ) and other applications.

## IV. Pairings

A pairing and a pair of mapping linearly independent points of an elliptic curve elements of a finite field is not cyclic. We denote the pairing of two points P and Q e(P, Q). The properties listed below are very interesting for cryptographic applications, are present both in pairing as Weil pairing Tate:

- *Identity:* Pairing a pair of matched points and mapped to the neutral element of the underlying finite field
- *Bilinearidade:* data three points P, Q, R, pairing P + Q and R and the multiplication of the P and R pairing by pairing Q and R. This property is the most important of all, because through it we get the following:

$$e(P,nQ) = e(P,Q)^n = e(nP,Q)$$

- *Do not degeneration:* If P and Q are linearly independent, so their pairing and distinct from the neutral element of the underlying finite field.
- *Efficiency:* data any two points, its pairing can be calculated efficiently by a computer.

### *a) Tate Pairing*

K is an integer such that $F_q^k$ contains the n nth roots of unity. Pairing Tate and defined through the following mapping:

$$e : E[n] \times E/nE \rightarrow F_q^k/(F_q^k)^n$$

where E [n] are the points P of the curve such that nP = ∞.The Tate pairing can be calculated as e(P, Q) = g (D) where D and a divider point Q associated with a function whose rational divider n[P] - n [∞]. The Miller algorithm [Mil04] can be used to calculate the function g.

Menezes, Okamoto, and Vanstone [6] pairings used to perform a transformation of an elliptic curve points supersingular to elements of a finite field generated by the unitary roots of unity. This transformation has allowed a large reduction in the difficulty of the discrete logarithm problem for these curves.

Sakai, Ohgishi and Kasahara [8] made possible the construction of a ciframento protocol based on identities using pairings, this solved the problem proposed by Shamir in his article.

## V. Proposed Scheme

Now we can describe in detail the proposed scheme.

*Configuration:* Given k, the PKG singles groups of bilinear maps, $G_1$, $G_2$ and $G_t$, of prime order $p> 2^k$ generators $Q \in G_2$ ,$P=Ø(Q) \in G_1$ ,$g=e(P,Q) \in G_t$ Select s random belonging to $Z^*_p$ a public key of $Q_{pub} = SQ \in G_2$ system summary cryptographic functions $H_1$, $H_2$ and $H_3$.

*Generation of key pair:* For an identity ID, the private key and $S_{ID} = \frac{1}{H1(ID)+S}$ $Q \in G_2$.

*Encryption:* Given a message M , the identity of the sender $ID_r$ and the identity of the recipient $ID_d$, random x is used belonging to $Z^*_p$ to calculate
$r=g^x$ ,$C=M \oplus H_3$ ( r) and $h =H_2$ (M,r).
It is estimated $S=(x + h)\ \varphi\ (S_{ID})$ and $T = x(H_T (ID_r )P + \varphi(Q_{pub)}$.
The ciphertext and the triple (c, S, T).

*Deciphering and verification:* Given the triple (c, S, T) and the identity of the $ID_R$ sender is calculated as
$r = e(T, S_{IDd})$, $M = c \oplus H_3 (r)$ and $h = H_2 (M, r)$.

Accept message if $r = e(S, H\text{-}1\ (ID_r)Q+Q_{pub})g^{-h}$, in which case the message M and signature (h, S) are returned.

## VI. Review

This proposed scheme is interesting because their safety was demonstrated by Barreto semantically, in order to not be subject to attacks that occur when they are used some optimizations of Weil and Tate pairings. Also, please note that the simple junction of the features of this scheme and signature represents a gain of security.

But there is a problem that has not been discussed, which is the abrogation of the private key. This question this open and represents a major problem for the security of any key establishment protocol, because the User can and should change your private key regularly. The problem is in the fact that the private key calculation is deterministic, that is, given the master key sea identity ID, the algorithm always returns the same private key. As the public key and the very identity, the User can not change your identity to obtain a new private key, and needed some other solution. Other asymmetric encryption schemes do not have this problem because the public key is published and revoked with its corresponding private key.

## VII. Conclusion

In this work it was possible to see that cryptosystems based on Identities are very interesting and represent an area of research that is growing. However the joint utilization of digital certificates and Identity-Based Protocols can be even more interesting as these two possible solutions to the problem of ensuring association between public key and its owner seem to be complementary.

## References Références Referencias

1. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology - Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 196 (1985), 47–53.
2. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", Advances in Cryptology – CRYPTO 2001, Lecture Notes in Computer Science, 2139 (2001), 213–229. Full version: SIAM Journal on Computing, 32 (2003), 586–615.
3. K. Paterson and G. Price, "A comparison between traditional public key infrastructures and identity-based cryptography", Information Security Technical Report, 8(3) (2003), 57–72.
4. W. Mao. Modern Cryptography - theory and practice. Prentice Hall, 2004.
5. Joux. A one round protocol for tripartite Diffie-Hellman. In W. Bosma, editor, Algorithmic Number Theory, IV-Symposium (ANTS IV), LNCS 1838, pages 385–394. Springer-Verlag,2000.
6. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to a finite field. In IEEE Trans. Info. Theory, number 39, pages 1636–1646, 1983.
7. L. Adleman and M. Huang, "Function field sieve methods for discrete logarithms over finite fields", Information and Computation, 151 (1999), 5–16.
8. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystem based on pairing. In Symposium on Cryptography and Information Security, Okinawa, Japan, January 2000.
9. O. Ahmadi, D. Hankerson and A. Menezes, "Software implementation of arithmetic in F3m", International Workshop on Arithmetic of Finite Fields (WAIFI 2007), Lecture Notes in Computer Science 4547 (2007), 85–102.
10. ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, 1999.
11. Atkin and F. Morain, "Elliptic curves and primality proving", Mathematics of Computation, 61 (1993), 29–68.
12. R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has

subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm", Journal of Cryptology, 11 (1998) 141–145.

13. P. Barreto, S. Galbraith, C. ´O h´Eigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties", Designs, Codes and Cryptography, 42 (2007), 239–271.
14. P. Barreto, H. Kim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems", Advances in Cryptology – CRYPTO 2002, Lecture Notes in Computer Science, 2442 (2002), 354–368.
15. P. Barreto, B. Lynn and M. Scott, "Efficient implementation of pairing-based cryptosystems", Journal of Cryptology, 17 (2004), 321–334.
16. P. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order", Selected Areas in Cryptography – SAC 2005, Lecture Notes in Computer Science, 3897 (2006), 319–331.
17. den Boer, "Diffie-Hellman is as strong as discrete log for certain primes", Advances in Cryptology – CRYPTO '88, Lecture Notes in Computer Science, 403 (1996), 530–539.
18. Boldyreva, "Efficient threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme", Public Key Cryptography – PKC 2003, Lecture Notes in Computer Science, 2567 (2003), 31–46.
19. Boneh, X. Boyen and H. Shacham, "Short group signatures", Advances in Cryptology – CRYPTO 2004, Lecture Notes in Computer Science, 3152 (2004), 41–55.
20. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano, "Public key encryption with keyword search", Advances in Cryptology – EUROCRYPT 2004, Lecture Notes in Computer Science, 3027 (2004), 506–522.
21. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", Advances in Cryptology – CRYPTO 2001, Lecture Notes in Computer Science, 2139 (2001), 213–229. Full version: SIAM Journal on Computing, 32 (2003), 586–615.
22. D. Boneh, C. Gentry, H. Shacham and B. Lynn, "Aggregate and verifiably encrypted signatures from bilinear maps", Advances in Cryptology– EUROCRYPT 2004, Lecture Notes in Computer Science, 2656 (2003), 416–432.
23. D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing", Advances in Cryptology – ASIACRYPT 2001, Lecture Notes in Computer Science, 2248 (2001), 514–532. Full version: Journal of Cryptology, 17 (2004), 297–319.
24. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.