A PAIRING-FREE IDENTITY BASED TRIPARTITE SIGNCRYPTION SCHEME

Hassan M. Elkamchouchi [1], Eman F. Abou Elkheir[2] and Yasmine Abouelseoud[3]

[1] Elec. Eng. Dept, Fac. of Eng., Alexandria University.
[2] Elec. Eng. Dept, Fac. of Eng., Kafr El-Sheikh University.
[3] Math. Eng. Dept, Fac. of Eng., Alexandria University.

ABSTRACT

The certificate-based cryptosystems is traditional way in providing the system parameters. Identity-based cryptography is more efficient than certificate-based cryptosystems. Each user in identity-based cryptography uses any arbitrary string that uniquely identifies him as his public key. This paper proposes a new identity-based tripartite signcryption scheme based on the elliptic curve discrete logarithm problem. The proposed id-based tripartite signcryption scheme does not use the bilinear pairings in both the Signcryption and unsigncryption phases. The proposed scheme used to reduce the communication over head when three entities wants to communicate securely as in authentication protocol in GSM and in e-commerce. The proposed scheme satisfies various desirable security properties. Also, the performance of the proposed scheme is tested.

KEYWORDS

Tripartite, Signcryption, Without Bilinear Pairing, ECDLP, Identity Based, Security Requirements

1. INTRODUCTION

Confidentiality and authenticity are the most important security goals. Traditionally, these two goals are separately examined, the encryption schemes supports the confidentiality and digital signature schemes provide the authenticity [1]. The sender first digitally signs the message using his private key then encrypts the digitally signed message using his public key, under the consideration of using public key cryptography. The encrypted (message + signature) is then sent together with the receiver that decrypt the message then verify the signature [2].

In 1997, Zheng [3] proposed using a single cryptographic primitive to achieve both confidentiality and authenticity. He called this primitive 'signcryption'. A signcryption scheme typically consists of three algorithms: Key Generation (Gen), Signcryption (SC), and Unsigncryption (USC). Key generation phase in which each user generates his key pairs that used in the Signcryption and unsigncryption phases, signcryption (SC) is normally a probabilistic algorithm in which the message is signed and encrypted in a single logical step, and unsigncryption (USC) is almost certainly to be deterministic in which the receiver authenticates the sender then decrypt the message. Any signcryption scheme should provide the correctness, accuracy and security requirements as it will demonstrated in the rest of the paper [4].

In 2002, Malone-Lee proposed the first ID-based signcryption scheme [5]. Figure 1 shows the basic structure of an ID-based signcryption scheme [6]. Since then, many ID-based signcryption schemes [7-10] have been proposed.

DOI:10.5121/ijcis.2013.3401

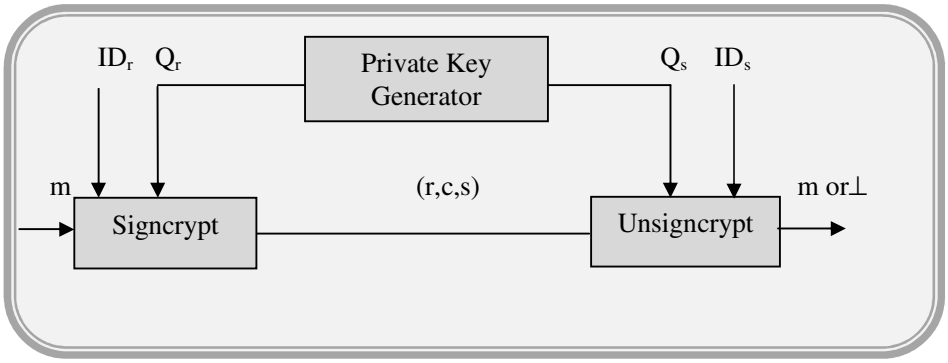

Figure 1. ID-based signcryption scheme structure

When three entities involved in an application as in e-commerce secure electronic transaction (SET) protocol who are the merchant, the customer and the bank , the tripartite key agreement protocols are important in providing essential security[11].

A new tripartite signcryption scheme from bilinear pairings based on elliptic curve discrete logarithm problem developed by Y. Abouelseoud [12]. This tripartite signcryption scheme is used to reduce the communication overhead in the secure electronic transaction protocol (SET). Also, H. M. Elkamchouchi, E. Abou El-kheir and Y. Abouelseoud developed a tripartite signcryption scheme without bilinear pairings [13].

In this paper, a new Id-based tripartite signcryption scheme without bilinear pairings is proposed and its security and performance are analyzed.

The rest of the paper is organized as follows. Section 2 discusses the security requirements for any signcryption scheme. Section 3, presents the proposed identity based tripartite scheme without bilinear pairing is. Section 4, introduces the security analysis of the proposed scheme followed by section 5 that discusses the proposed scheme performance. Finally, Section 6 concludes the paper.

2. SECURITY REQUIREMENTS FOR ANY SIGNCRYPTION SCHEME

Here, the security requirements for any signcryption scheme are provided [1, 13, 14 ,15]:

2.1 Confidentiality

It means that only the intended recipient of a signcrypted message should be able to read its contents. That is, upon seeing a signcrypted message, an attacker should learn nothing about the original message, other than perhaps its length.

2.2 Unforgeability

It refers to the inability of any entity to produce a valid message-signature pair except the designated signer.

2.3 Public Verifiability

It means that any third party or judge can verify that the signcrypted text is valid or not, without any requirement for the private key of the sender or the recipient.

2.4 Non-Repudiation

The sender of a message cannot later deny having sent the message. That is, the recipient of a message can prove to a third party that the sender indeed sent the message.

2.5 Integrity

This means that the recipient should be able to verify that the received message is the original one that was sent by the sender and it has not been tampered with during transmission.

2.6 Authentication

The receiver needs to authenticate the sender. This identity of the sender is verified through the key recovery process and the message integrity is checked using a suitable one-way hash function.

2.7 Forward Secrecy

It refers to the inability of an attacker to read signcrypted messages, even with access to the sender's private key. That is, the confidentiality of signcrypted messages is protected, even if the sender's private key is compromised.

3. THE PROPOSED PAIRING FREE ID-BASED TRIPARTITE SCHEME

3.1 Setup

Given security parameter *l* (usually 160), the PKG chooses q a large prime number with $q > 2^k$, (a, b) is a pair of integers which are smaller than q and satisfy $(4a^3 + 27b^2) \bmod q \neq 0$. E is the selected elliptic curve over the finite field $F_q : y^2 = (x^3 + ax + b) \bmod q$. P is the base point or generator of a group of points on E, denoted as G. Also, O is the point at infinity and n is the order of the point P, with n being a prime number, $n.P = O$ and $n > 2^k$. The PKG selects a cryptographic one way hash function $H : \{0,1\}^* \rightarrow Z_q$. The PKG selects a random number mk_{PKG} as the master key and computes the master public key $R = mk_{PKG}.P$. The PKG keeps mk_{PKG} secret and publishes the system parameters params: $\{k, E, P, G, R, H\}$

3.2 Key generation

The PKG generates the secret and public key pairs for the three communicating parties. The PKG sends the secret keys via a secrete channel and publishes the public keys with user the identities. The PKG calculates the secret keys of the three communicating parties as follows:

$d_a = (H(ID_a).mk_{PKG}) \bmod q$, $d_b = (H(ID_b).mk_{PKG}) \bmod q$

and $d_c = (H(ID_c).mk_{PKG}) \bmod q$.

The PKG calculates the public keys for entities A, B and C as follows: $Q_a = d_a.R$, $Q_b = d_b.R$ and $Q_c = d_c.R$ respectively. Figure 2 shows the id-based tripartite signcryption and unsigncryption phases.

3.3 Signcryption Phase

A wants to send a message m_1 to B and a message m_2 to C. A signcrypts the messages as follows:

The sender A generates a random number $w \in [1, q-1]$ and computes:

- $k_1 = ID_a.w.R$, $k_2 = ID_b.w.Q_b$, and $k_3 = ID_c.w.Q_c$, the key used is the x-coordinate value of the points k_1, k_2, k_3
- $c_1 = E_{k_2}(m_1)$, and $c_2 = E_{k_3}(m_2)$
- $r = Hash(ID_a \| ID_b \| ID_c \| c \| k_1), c = (c_1 \| c_2)$
- $s = (w - r.d_a) \bmod q$
- A sends (r, c, s) to both A and B

3.4 Unsigncryption

Receiver B proceeds as follows:

- The receiver B uses his/her secret key d_b to recover the encryption key $k_2; k_2 = d_b.ID_b.(s.R + r.Q_a) = ID_b.w.Q_b$.
- B recovers k_1 where $k_1 = ID_a.(s.R + r.Q_a) = ID_a.w.R$. Thus any third party can authenticate the sender.
- B computes $\bar{r} = Hash(ID_a \| ID_b \| ID_c \| c \| k_1)$, if the equation $\bar{r} = r$ holds B accepts the signcrypted-text.
- B computes $m_1 = D_{k_2}(c_1)$

The receiver C does the same steps as B:

- The receiver C uses his/her secret key to recover the encryption key $k_3; k_3 = d_c.ID_c.(s.R + r.Q_a) = ID_c.w.Q_c$.
- C recovers k_1 where $k_1 = ID_a.(s.R + r.Q_a) = ID_a.w.R$.
- Then C computes $\bar{r} = Hash(ID_a \| ID_b \| ID_c \| c \| k_1)$, if the equation $\bar{r} = r$ holds B accepts the signcrypted-text.
- Finally, C computes $m_2 = D_{k_3}(c_2)$

3.5 Signature Verification by Any Third Party

Any third party can recover k_1 where $k_1 = ID_a.(s.R + r.Q_a) = ID_a.w.R$ without using any short or long term secret keys. Then, the third party computes $\bar{r} = Hash(ID_a \| ID_b \| ID_c \| c \| k_1)$, if $\bar{r} = r$ accepts the signcrypted-text.

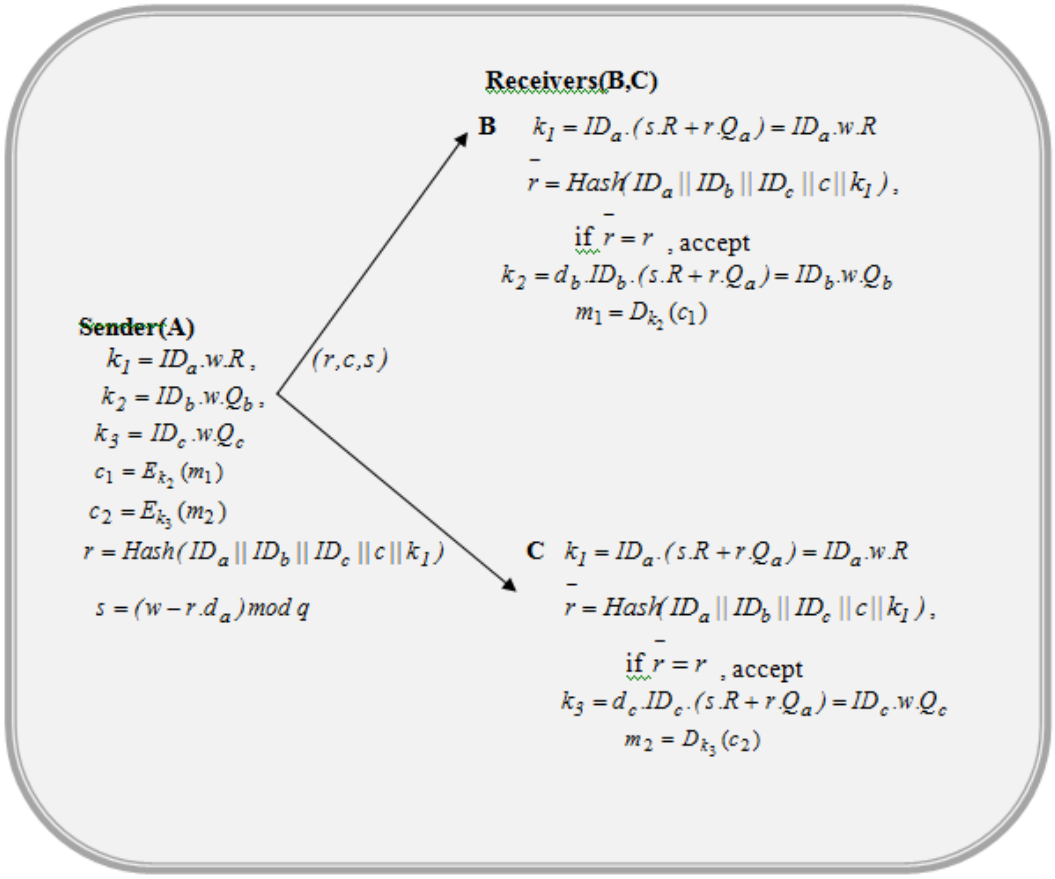

Figure 2 The proposed Id-based tripartite signcryption scheme.

4. SECURITY ANALYSIS OF THE PROPOSED SCHEME

4.1 Correctness

- The correctness of the signature verification:

$$k_1 = ID_a.(s.R + r.Q_a) = ID_a.w.R$$

$$k_1 = ID_a.((w - r.d_a).R + r.Q_a)$$

$$k_1 = ID_a.(w.R - r.d_a.R + r.Q_a) = ID_a.w.R$$

- For the receiver B:

$$k_2 = d_b.ID_b.(s.R + r.Q_a)$$

$$k_2 = ID_b.((w - r.d_a).d_b.R + r.d_b.Q_a)$$

$$k_2 = ID_b.(w.Q_b - r.d_b.Q_a + r.d_b.Q_a) = ID_b.w.Q_b$$

- For the receiver C:

$$k_3 = ID_c.d_c.(s.R + r.Q_a)$$

$$k_3 = ID_c.((w - r.d_a).d_c.R + r.d_c.Q_a)$$

$$k_3 = ID_c.(w.Q_c - r.d_c.Q_a + r.d_c.Q_a) = ID_c.w.Q_c$$

4.2 Security Properties

This section demonstrates that the proposed id-based tripartite signcryption scheme provides the seven security functions that defined in section 2. The security of the proposed scheme relies on the elliptic curve discrete logarithm problem (ECDLP) that considered hard computational problem till now [16].

Definition 1: The Elliptic Curve Discrete Logarithm Problem (ECDLP) is defined as follows. Let G and Q be two points on an elliptic curve and G is of order n and n is a prime. The point $Q = k.G$, where $k < n$. Given these two points G and Q, find the discrete logarithm of Q to the base G; that is, k [16].

4.2.1 Confidentiality

If an adversary wants to derive the original message, he must be able to recover k_2, k_3 to encrypt the messages or the key k_1. However, to obtain the secret keys k_1, k_2, k_3 is equivalent to solving the ECDLP. Assume that an adversary tries to compute any of the keys $k_1 = ID_a.(s.R + r.Q_a) = ID_a.w.R$, $k_2 = d_b.ID_b.(s.R + r.Q_a)$, $k_3 = ID_c.d_c.(s.R + r.Q_a)$, he must be able to derive the random number w to get the correct k_1, the receiver's secret key d_b, where $Q_b = d_b.R$, and the receiver's secret key d_c, where $Q_c = d_c.R$. Therefore to derive w, d_b, d_c one needs to solve the ECDLP. Without knowing the secret key of the receiver, no one can recover the message encryption key. It is only the valid receiver with valid identity with secret key d_b, d_c who can recover the key and unsigncrypt the message.

4.2.2 Unforgeability

The signcrypted text is generated using the sender's secret key d_a. Also, the sender's secret key is computed as $Q_a = d_a.R$, but computing d_a is another elliptic curve discrete logarithm problem under Definition 1.So, no one can forge signcrypted text without knowing the sender's secret key d_a.

If an adversary wants to forge a signcrypted text he proceeds as follow:

- Generate random number w'
- $k_1' = ID_a.w'.R$, $k_2' = ID_b.w'.Q_b$, and $k_3' = ID_c.w'.Q_c$
- $c_1' = E_{k_2'}(m_1')$, and $c_2' = E_{k_3'}(m_2')$

- $r' = Hash(|ID_a.||ID_b.||ID_c.||c'||k_1'), c' = (c_b', c_c')$
- $s' = (w' - r'.d_{adv}) \bmod q$, d_{adv} is the attacker secrete key
- The attacker sends (r', c', s') to both A and B

The receiver B and C unsigncrypts the message by recovering the key k'_2, k'_3 respectively as follows:

For the receiver B: $k_2' = ID_b.d_b.(s'.R + r'.Q_a) = ID_b.w.Q_b$

$k_2' = ID_b.d_b.(s'.R + r'.Q_a) = ID_b.((w' - r'.d_{adv}).Q_b + d_b.r'.Q_a)$

$k_2' = ID_b.(w'.Q_b - r'.d_a.Q_b + r'.d_b.Q_a) \neq (k_2 = ID_b.w.Q_b)$

Then B computes $m_1 \neq D_{k_2'}(c_1)$. Also , the same steps are carried out by receiver C. Without knowing the sender's secret key, no one can generate a valid signcrypted text. Therefore, the proposed scheme achieves unforgeability.

4.2.3 Authentication

The receiver needs to authenticate the sender. The receiver authenticates the sender through the key recovery process and the message integrity is checked using a suitable one-way hash function.

4.2.4 Public Verifiability

Any third party can recover k_1 without using any secret keys as demonstrated in Section 3.5.

4.2.5 Non-Repudiation

The sender cannot deny sending the signcrypted text because any third party can make sure that the original sender is the one who signcrypted the message. So, the public verifiability property solves the problem of non-repudiation.

4.2.6 Integrity

The alteration or modification in the ciphertext by any third party can be easily detected because of the signature part that will need to be changed accordingly.

4.2.7 Forward Secrecy

If the attacker tries to derive the plaintext m, he has to decrypt the associated ciphertext c using the corresponding secret key. This secret session key involves a random number w that appears in the computation of the three keys: $k_1 = ID_a.w.R$, $k_2 = ID_b.w.Q_b$, and $k_3 = ID_c.w.Q_c$. Without knowing the random number w, even if the long term key of the sender is known, the encryption key cannot be recovered. In other words, he cannot decrypt the signcrypted text to get a previous message m. Even if the sender's private key is compromised, the proposed scheme supports the forward secrecy of message confidentiality.

5. PERFORMANCE OF THE PROPOSED SCHEME

First, in Table 1, the time abbreviations are listed as will be used in the performance evaluation table that follows. The performance of the proposed scheme is examined in Table 2, it shows the number of the computationally operations involved in the proposed identity based tripartite scheme. In the proposed scheme, the public key generator in set up phase performs 4 scalar point multiplications over an elliptic curve, 3 hash operations and 3 multiplications over a finite field. For the sender (A) , it performs 3 scalar point multiplications over an elliptic curve, 2 encryptions, one hash operation and 4 multiplications over a finite field in the signcryption phase. The receivers (B , C) , each receiver in unsigncryption phase performs 3 scalar point multiplications over an elliptic curve, one decryption operation, one hash operation , one addition operation over an elliptic curve and 2 multiplications over a finite field.

6. CONCLUSION

This paper introduces a new identity based tripartite signcryption scheme without bilinear pairings. The proposed scheme is efficient in case of sending two different messages. The security analysis have been proved. Also, the performance of the proposed scheme have been discussed. The proposed scheme may be used in various applications such as mobile communication , secure electronic transaction (SET) protocols and e-cash protocol to reduce computations and timing cost . The proposed Id-based tripartite signcryption scheme can be used between the mobile communication entities which will reduce the signaling overhead and the computations required.

Table.1Time Abbreviations

Symbol	Operation
$\mathbf{T_{EC\text{-}mult}}$	time required for executing the point multiplication operation on elliptic curve *E*
$\mathbf{T_{EC\text{-}add}}$	time required for executing the point addition operation on elliptic curve *E*
$\mathbf{T_{mult}}$	time required for executing modulus multiplication in a finite field
$\mathbf{T_h}$	time required for executing one way dispersed row function operation
$\mathbf{T_{encr}}$	time required by the system for executing encryption operation
$\mathbf{T_{decr}}$	time required by the system for executing decryption operation

TABLE.2 The performance of the proposed id-based tripartite Signcryption scheme.

Phase	The proposed ID-based tripartite scheme
Set Up	$4T_{EC\text{-}mult}+3T_h+ 3T_{mult}$
Signcryption	$3T_{EC\text{-}mult}+1T_h+ 4T_{mult}+ 2\ T_{encr}$
Unsigncryption (for each receiver)	$3T_{EC\text{-}mult}+1T_{EC\text{-}add}+2T_{mult}+ 1T_h+ 1\ T_{decr}$
Total	$10T_{EC\text{-}mult}+1T_{EC\text{-}add}+5T_h+9T_{mult}+2\ T_{encr} + 1\ T_{decr}$

REFERENCES

[1] C. D. Smith," Digital Signcryption ", A thesis presented to the University of Waterloo in fulfilment of the thesis requirement for the degree of Master of Mathematics in Combinatorics and Optimization, 2005.

[2] S. Khullar, V. Richhariya , and V. Richhariya," An Efficient identity based Multi-receiver Signcryption Scheme using ECC ",International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013 ISSN 2278-7763

[3] Y. Zheng, " Digital Signcryption or How to Achieve Cost (Signature and Encryption) Cost (Signature) + Cost (Encryption), " Advances in Cryptology, LNCS, Vol. 1294. Springer-Verlag, pp.165–179, 1997.

[4] M. Toorani, "Cryptanalysis of an Elliptic Curve-based Signcryption Scheme", International Journal of Network Security, Vol.10, No.1, pp.51–56, Jan. 2010.

[5] J. Malone-Lee, " Identity based Signcryption ", Cryptology ePrintArchive, 2002 http://eprint. iacr.org/2002/098.pdf.

[6] S. Khullar, V. Richhariya , and V. Richhariya," An Efficient identity based Multi-receiver Signcryption Scheme using ECC ",International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013 ISSN 2278-7763

[7] X. Boyen, " Multipurpose Identity-Based Sign cryption: a Swiss Army Knife for Identity-based Cryptography ", LNCS: Advances in Cryptology-Crypto2003, Berlin: Springer-Verlag Press, 2003, pp.383-399.

[8] M. S. S. Chow,M. S. Yiu, and K. C. Lucas, et al, " Efficient Forward and Provably Secure ID-based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity ", LNCS: information Security ande Cryptology-ICISC'03, Berlin:Springer-Verlag Press, , 2004, pp.352-269.

[9] L. Chen,and J. Malone-Lee ," Improved Identity-based Signcryption ", LNCS:PKC'05, Berlin: Springer-Verlag Press, 2005, pp.362-379.

[10] L. Fa-gen, H. Yu-pu and L. Gang, "An efficient identity-based signcryption scheme", Chinese Journal of Computers, Vol. 29, No. 6, 2006, pp:1641-1647.

[11] M. Nabil, Y. Abouelseoud, G. Elkobrosy, and A. Abdelrazek ," New Authenticated Key Agreement Protocols. Proceeding Of The International Multiconference Of Engineers And Computer Scientist (IMECS 2013) Vol. 1, March 13-15 ,2013 , Hong Kong

[12] Y. Abouelseoud.,"A Tripartite Signcryption Scheme with Applications to E-Commerce. International Journal of Computer Applications (0975 – 8887) Volume 76– No.15, August 2013

[13] H. Elkamchouchi, E. Abou El-kheir, and Y. Abouelseoud, " An Efficient Tripartite Signcryption Scheme Without Bilinear Pairings ", International Journal of Scientific & Engineering Research, ISSN 2229-5518, Volume 4, Issue 10, November-2013 X. Boyen, " Multipurpose Identity-Based Sign cryption: a Swiss Army Knife for Identity-based Cryptography ", LNCS: Advances in Cryptology-Crypto2003, Berlin: Springer-Verlag Press, 2003, pp.383-399.

[14] http://en.wikipedia.org/wiki/Authentication

[15] D. Johnson, A. Menezes, and S. Vanstone, " The elliptic curve digital signature algorithm (ECDSA) ",International Journal of Information Security 1 (1) (2001) 36–63.