An Efficient Tripartite Signcryption Scheme Without Bilinear Pairings

Hassan Elkamchouchi[1], Eman Abou El-kheir[2], and Yasmine Abouelseoud[3]
Alexandria University[1,3], Kafr El-Sheikh University[2], Egypt

Abstract— Authentication and confidentiality are the most important security goals to be achieved. This paper proposes a new tripartite signcryption scheme without bilinear pairings. The proposed tripartite signcryption scheme is efficient when three entities want to perform secure transactions as in mobile communication or in e-commerce. The proposed scheme is based on the elliptic curve discrete logarithm problem (ECDLP) and achieves the seven security requirements; confidentiality, unforgeability, public verifiability, non-repudiation, integrity, authentication, and forward secrecy. Also, the proposed scheme supports public verifiability without using any short or long term keys. The performance of the proposed scheme is examined.

Index Terms— Tripartite, Signcryption, Without Bilinear Pairing, ECDLP, Confidentiality, Authentication, Security Requirements

1 Introduction

Of the many goals which the study of cryptography sets out to achieve, the most important and widely studied are confidentiality and authenticity. Traditionally, these two goals have been studied separately. In the case of public-key cryptography, confidentiality is provided by encryption schemes, while authenticity is provided by digital signature schemes [1]. First, a message is digitally signed with the private key of the sender then the message is encrypted together with the signature using a randomly chosen key using a symmetric cipher. The random key is then encrypted using the public key of the receiver. The encrypted (message + signature) is then sent together with the encrypted random key [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 produces a pair of keys for each user, signcryption (SC) is normally a probabilistic algorithm, and unsigncryption (USC) is almost certainly to be deterministic. Any signcryption scheme should possess correctness, accuracy and security as main properties [4].

Tripartite key agreement protocols are of particular importance. They are useful in providing essential security in several vital applications such as in e-commerce where the three entities involved in the protocol are the merchant, the customer and the bank. Other interesting applications include a third party being added to chair or referee a conversation for the purpose of ad hoc auditing, data recovery or escrow purposes[5].

Y. Abouelseoud developed a tripartite signcryption scheme from bilinear pairings in [6]. This tripartite signcryption scheme used to reduce the signaling overhead in the secure electronic transaction protocol (SET).

In this paper, a new tripartite signcryption scheme without bilinear pairings is proposed with its security and performance analyzed. Additionally, a comparative study is provided.

The rest of the paper is organized as follows. Section 2 discusses the security requirements for any signcryption scheme. In Section 3, the proposed tripartite scheme without bilinear pairing is introduced. In Section 4, the security analysis of the proposed scheme is presented. Section 5 discusses the performance of the proposed scheme and a comparative study is also presented in this section. Finally, Section 6 concludes the paper.

2 Security Requirements For Any Signcryption Scheme

Here, the security requirements for any signcryption scheme are provided [1, 7 ,8]:

- *Hassan Elkamchouchi : Elec. Eng. Dept, Fac. of Eng., Alexandria University.E-mail: helkamchouchi@ieee.org*
- *Eman Abou El-kheir: Elec. Eng. Dept, Fac. of Eng., Kafr El-Sheikh University. E-mail: eman.abouelkhair@eng.kfs.edu.eg*
- *Yasmine Abouelseoud: Eng. Math. Dept, Fac. of Eng., Alexandria University. E-mail: yasmine.abouelseoud@gmail.com*

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
It involves confirming the identity of a system user. Authentication often involves verifying the validity of at least one form of identification. Also, it allows the legitimate recipient alone to be convinced that the ciphertext and the signed message it contains were crafted by the same entity.

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 TRIPARTITE SCHEME

3.1 Setup
Given security parameter k (usually 160), the CA (certificate authority) 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 CA selects a cryptographic one way hash function $H : \{0,1\}^* \rightarrow Z_q$. The CA publishes the system parameters: $\{k, a, b, E, P, H\}$

3.2 Key generation
The private/public key pairs for the three communicating parties are generated as follows. Each member picks a random number d and then computes the corresponding public key as $Q = dP$. The public keys for entities A, B and C are given as $Q_a = d_a P$, $Q_b = d_b P$ and $Q_c = d_c P$ respectively. Figure 1 shows the signcryption and unsigncryption phases of the proposed scheme.

3.3 Signcryption generation
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:

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

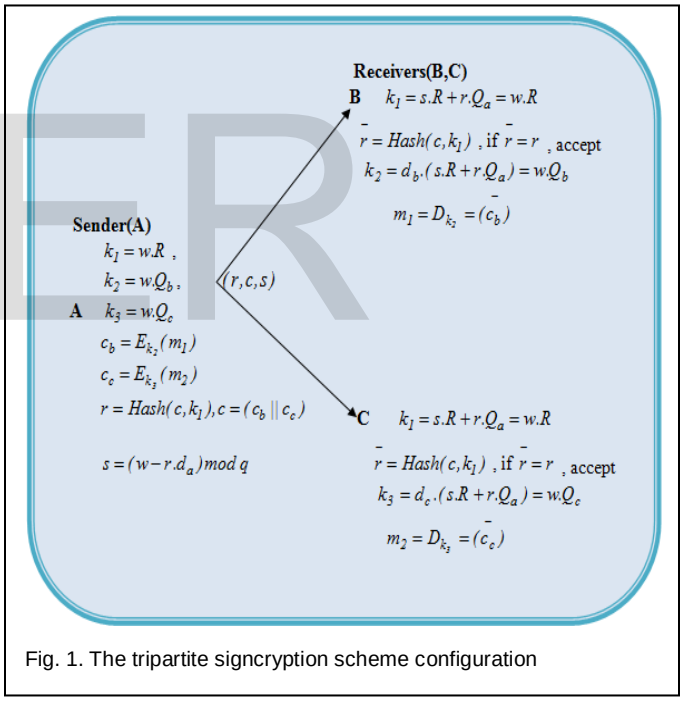

Fig. 1. The tripartite signcryption scheme configuration

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; $k_2 = d_b.(s.R + r.Q_a) = w.Q_b$.
- B recovers k_1 without using any secret keys and this supports public verifiability in the proposed scheme where $k_1 = s.R + r.Q_a = w.R$.
- B computes $\bar{r} = Hash(c, k_1)$, if $\bar{r} = r$ then B accepts the signcrypted-text.

- B computes $m_1 = D_{k_2} = (\bar{c}_b)$

The receiver C does the same steps as B:

- The receiver C uses his/her secret key to recover the encryption key $k_3; k_3 = d_c.(s.R + r.Q_a) = w.Q_c$.
- C recovers k_1 without using any secret keys and this support the public verifiability in the proposed scheme where $k_1 = s.R + r.Q_a = w.R$.
- Then C computes $\bar{r} = Hash(c, k_1)$, if $\bar{r} = r$ then C accepts the signcrypted-text
- Finally, C computes $m_2 = D_{k_3} = (\bar{c}_c)$

3.5 Signature Verification by Any Third Party

Any third party can recover k_1 without using any secret keys and this why public verifiability is supported in the proposed scheme where $k_1 = s.R + r.Q_a = w.R$. Then, the third party computes $\bar{r} = Hash(c, k_1)$, if $\bar{r} = r$ accepts the signcrypted-text.

4 Security Analysis

4.1 Correctness

- For the signature verification:

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

- For the receiver B:

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

- For the receiver C:

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

4.2 Security Properties

The proposed tripartite signcryption scheme provides seven security functions: message confidentiality, authentication, integrity, unforgeability, non-repudiation, forward secrecy and public verifiability. The security of the proposed scheme relies on the elliptic curve discrete logarithm problem (ECDLP) [9]. Up till now, the ECDLP is considered to be hard.

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.

4.2.1 Confidentiality

If the attacker wants to derive the original message, he must be able to recover the randomly generated session keys k_2, k_3 to encrypt the messages or the key k_1. However, the extraction of the secret keys k_1, k_2, k_3 is equivalent to solving the ECDLP. Assume that the attacker tries to compute any of the the points $k_1 = s.R + r.Q_a = w.R$, $k_2 = d_b.(s.R + r.Q_a) = w.Q_b$, $k_3 = d_c.(s.R + r.Q_a) = w.Q_c$, he should 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 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. Thus, no one can generate a valid signcrypted text without knowing 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.

If an attacker wants to generate a signcrypted text he does the following:

- Generate random number w'
- $k_1' = w'.R$, $k_2' = w'.Q_b$, and $k_3' = w'.Q_c$
- $c_b' = E_{k_2'}(m_1')$, and $c_c' = E_{k_3'}(m_2')$
- $r' = Hash(c', k_1'), c' = (c_b' || c_c')$
- $s' = (w' - r'.d_{adv}) \bmod q$, 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: $k_2' = d_b.(s'.R + r'.Q_a) = w.Q_b$

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

Then B computes $m_1 \neq D_{k_2'} = (\bar{c}_b)$. 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 $k_1 = w.R$, $k_2 = w.Q_b$, and $k_3 = w.Q_c$. 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. Therefore, our proposed scheme provides forward secrecy of message confidentiality even if the sender's private key is compromised.

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.

In Table 2, the proposed scheme is compared with the scheme in [6].
The comparison shows that in case of two different messages the proposed scheme is more efficient than the scheme in [6].

6 Conclusion

This paper introduces a new tripartite signcryption scheme without bilinear pairings. The security analysis and the performance of the proposed scheme have been discussed. The proposed scheme is compared with the scheme in [6] and the comparison shows that the proposed scheme is more efficient. The proposed scheme may be used in various applications such as mobile communication. The proposed tripartitesign-cryption scheme can be used between the mobile communication entities which will reduce the signaling overhead.

TABLE 1
TIME ABBREVIATIONS

Symbol	Operation
$T_{EC\text{-}mult}$	Time required for executing multiplication operation on elliptic curve E
$T_{EC\text{-}add}$	Time required for executing addition operation on elliptic curve E
T_{mult}	Time required for executing modulus multiplication in a finite field
T_h	Time required for executing one way dispersed row function operation
$T_{inverse}$	Time complexity required for executing inverse modulus over a finite field
$T_{pairings}$	Time of executing a bilinear pairing operation
T_{encr}	Time required by the system for executing encryption operation
T_{decr}	Time required by the system for executing decryption operation

TABLE 2
THE PERFORMANCE PROPOSED SCHEME

Phase	The scheme in [6] with pairings		The proposed without pairings	
No of messages	M=1	M=2	M=1	M=2
Signcryption	$1T_h+1T_{mult}+1T_{inverse}+2T_{pairings}+1T_{encr}$	$2T_h+2T_{mult}+2T_{inverse}+2T_{pairings}+2T_{encr}$	$3T_{EC\text{-}mult}+1T_h+1T_{mult}+2T_{encr}$	$3T_{EC\text{-}mult}+1T_h+1T_{mult}+2T_{encr}$
Unsigncryption (for each receiver)	$1T_{EC\text{-}mult}+1T_{EC\text{-}add}+1T_{mult}+2T_{pairings}+1T_h+1T_{decr}$	$1T_{EC\text{-}mult}+1T_{EC\text{-}add}+1T_{mult}+2T_{pairings}+1T_h+1T_{decr}$	$3T_{EC\text{-}mult}+1T_{EC\text{-}add}+1T_h+1T_{decr}$	$3T_{EC\text{-}mult}+1T_{EC\text{-}add}+1T_h+1T_{decr}$
Total	$1T_{EC\text{-}mult}+1T_{EC\text{-}add}+2T_h+2T_{mult}+4T_{pairings}+1T_{inverse}+1T_{encr}+1T_{decr}$	$1T_{EC\text{-}mult}+1T_{EC\text{-}add}+3T_h+3T_{mult}+4T_{pairings}+2T_{inverse}+2T_{encr}+1T_{decr}$	$6T_{EC\text{-}mult}+1T_{EC\text{-}add}+2T_h+1T_{mult}+2T_{encr}+1T_{decr}$	$6T_{EC\text{-}mult}+1T_{EC\text{-}add}+2T_h+1T_{mult}+2T_{encr}+1T_{decr}$

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] 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

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

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

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