An Improved Authentication Protocol for Mobile Communication based on Tripartite Signcryption

Hassan M. Elkamchouchi
Elec. Eng. Dept, Fac. of Eng,
Alexandria Univ.
Alexandria
Egypt

Eman F. Abou Elkheir
Elec. Eng. Dept, Fac. of Eng,
Kafr Elsheikh Univ.
Kafr Elsheikh
Egypt

Yasmine Abouelseoud
Eng. Math. Dept, Fac. of Eng,
Alexandria Univ.
Alexandria
Egypt

ABSTRACT
This paper introduces a new authentication protocol using the tripartite signcryption scheme without bilinear pairings that provides confidentiality and authentication between three entities. Mobile communication seems very attractive to users as well as operators and service providers. However, despite of its numerous advantages, mobile communication has been facing many security problems. In this paper, it is demonstrated how the proposed tripartite signcryption scheme can be used to provide authentication and to guarantee secure communication. The use of the proposed tripartite signcryption scheme helps reduce the signaling overhead compared to the scheme in [1].

General Terms
Cryptography, Security.

Keywords
Tripartite Signcryption, Mobile Communication, Mobile Security

1. INTRODUCTION
Wireless and mobile communication systems are very famous among the customers as well the operators and service providers. Unlike wired networks, the wireless networks provide anywhere and anytime access to users. The Global System for Mobile Communications (GSM) occupies almost 70% of the wireless market and is used by millions of subscribers in the world [2].

In wireless services, secure and secret communication is desirable. It is the interest of both the customers and the service providers. These parties would never want their resources and services to be used by unauthorized users.

The services like online banking, e-payment, and e/m-commerce are already using the Internet. The financial institutions like banks and other organizations would like their customers to use online services through mobile devices keeping the wireless transaction as secure as possible from the security threats. Smart cards (e.g. SIM card) have been proposed for applications like secure access to services in GSM, to authenticate users and secure payment using Visa cards and MasterCard [3]. Wireless transactions are facing several security challenges. Data sent through air face almost the same security threats as the data over wired networks and even more. However, the limitations in wireless bandwidth, battery, computational power and memory of wireless devices impose further restrictions to the security mechanisms implementation [4]. The use of mobile communication in e/m-commerce has increased the importance of security. An efficient wireless communication infrastructure is required in every organization for secure voice/data communication and users authentication. Among the main objectives of an efficient infrastructure is to reduce the signaling overhead and to reduce the number of HLR/AuC (Home-Location Register/Authentication Center) updates as the Mobile Station (MS) changes its location frequently [4].

Tripartite security mechanisms are of particular importance as 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].

Signcryption combines the functionalities of encryption and digital signing in a single logical step. It provides various security services including confidentiality, integrity, message origin authenticity and non-repudiation. Y. Abouelseoud proposed a tripartite Signcryption scheme from bilinear pairings in [6]. This tripartite signcryption scheme is used to reduce the signaling overhead in the secure electronic transaction (SET) protocol.

This paper introduces an efficient tripartite signcryption scheme without bilinear pairings. It can be used to provide confidentiality and authentication in mobile communication networks in an efficient way as it enables reducing the signaling overhead.

The rest of the paper is organized as follows. In the next section, the desirable security features that a signcryption scheme should provide are summarized. In Section 3, the proposed tripartite signcryption scheme is described and the security properties of the scheme are analyzed in Section 4. An overview of the architecture of GSM is given in Section 5 and in the section that follows the use of public key cryptography in mobile communication protocols is reviewed. The use of the proposed tripartite signcryption scheme to provide authentication in mobile communications is examined in Section 7. Finally, Section 8 concludes the paper.

2. SECURITY REQUIREMENTS FOR ANY SIGNCRYPTION SCHEME
Here, the security requirements for any signcryption scheme are provided [7,8,9]:

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 need 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 TRIPARTITE SIGNCRYPTION SCHEME
In this section, the four modules of the tripartite signcryption scheme in [13]. This scheme used to reduce the signaling over head in the authentication protocol in GSM.

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 $F_q : y^2 = (x^3 + ax + b) \bmod q$. R 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 *R*, with n being a prime number, $n.R = O$ 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: $\{k, a, b, E, R, H\}$. Additionally, a secure symmetric key encryption mechanism should be agreed upon between the communicating parties.

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 $Q = dR$. The key pairs for entities A, B and C are given as $Q_a = d_a R$, $Q_b = d_b R$ and $Q_c = d_c R$ respectively. The signcryption and unsigncryption phases of the proposed scheme are shown in Figure1.

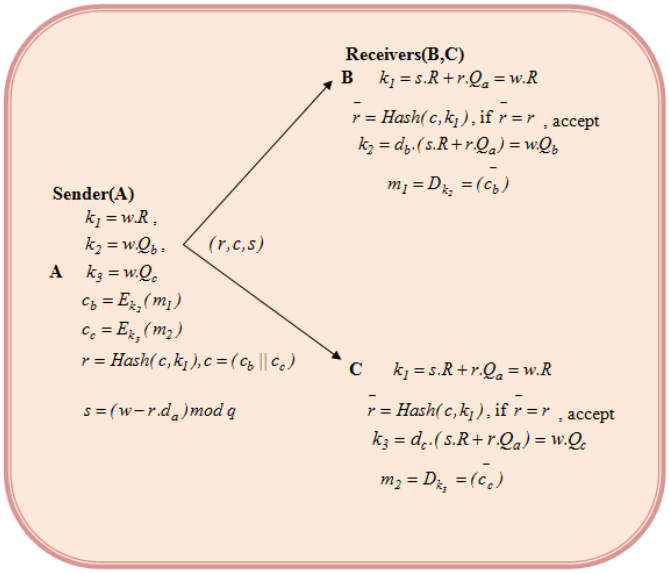

Fig.1 The tripartite signcryption scheme configuration

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 $w \in [1, n-1]$ and computes:

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

3.4 Unsigncryption phase
– 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 support the public verifiability in the proposed scheme where $k_1 = s.R + r.Q_a = w.R$

– B computes $\bar{r} = Hash(c, k_1)$. Then, if $\bar{r} = r$, B accepts the signcrypted-text and otherwise aborts the protocol.

– 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 by computing $k_1 = s.R + r.Q_a = w.R$. Then, entity C computes $\bar{r} = Hash(c, k_1)$, and if $\bar{r} = r$, C accepts the signcrypted-text.

– Finally, C recovers the message $m_2 = D_{k_3} = (\bar{c}_c)$.

3.5 Public verifiability

Any third party can recover k_1 without using any secret keys supporting public verifiability 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 $\bar{r} = r$, it accepts the signcrypted-text.

4. GSM OVERVIEW

GSM (Group Special Mobile) originally was a group formed by the European Conference of Post and Telecommunication Administrations (CEPT) in 1982 to develop cellular systems for replacement of already incompatible cellular systems in Europe. Later in 1991, when the GSM started services, its meaning was changed to Global System for Mobile Communications (GSM) [2].

The entire architecture of the GSM is divided into three subsystems: Mobile Station (*MS*), Base Station Subsystem (*BSS*) and Network Subsystem (*NSS*) as shown in Figure 2.

1. The *MS* consists of a Mobile Equipment (*ME*) (e.g. mobile phone) and Subscriber Identity Module (*SIM*) card which stores secret information like International Mobile Subscriber Identity (*IMSI*), secret key (K_i) for authentication and other user related information.
2. The *BSS*, the radio network, controls the radio link and provides a radio interface for the rest of the network. It consists of two types of nodes: Base Station Controller (*BSC*) and Base Station (*BS*). The *BS* covers a specific geographical area (hexagon) which is called a cell. Each cell comprises of many mobile stations. A *BSC* controls several base stations by managing their radio resources.
3. The *BSC* is connected to a Mobile services Switching Center (*MSC*) in the third part of the network NSS, also called the Core Network (*CN*). In addition to MSC, the NSS consists of several other databases like Visitor Location Register (*VLR*), Home Location Register (*HLR*) and Gateway *MSC* (*GMSC*) which connects the GSM network to Public Switched Telephone Network (*PSTN*). The *MSC*, in cooperation with the *HLR* and the *VLR*, provides numerous functions including registration, authentication, location updating, handovers and call routing.

The *HLR* holds administrative information of subscribers registered in the GSM network. Similarly, the *VLR* contains only the needed administrative information of subscribers currently located/moved to its area. The Equipment Identity Register (*EIR*) and Authentication Center (*AuC*) contain a list of valid mobile equipments and subscribers' authentication information respectively [2, 11].

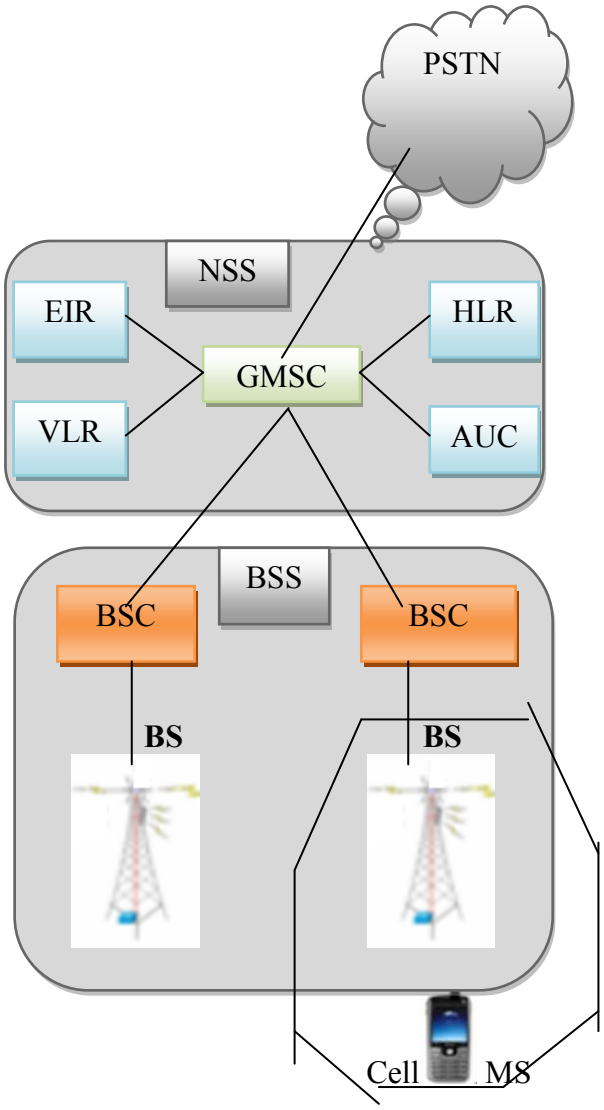

Fig.2 Components of GSM

5. RELATED WORK: AUTHENTICATION AND ENCRYPTION IN GSM, GPRS AND UMTS USING PUBLIC KEY CRYPTOGRAPHY

This section reviews the authentication protocol in [2].The three main entities, MS, VLR and HLR, are using four pairs of public/private key pairs as follows:

- V_H_{PrK} : *VLR - HLR link' s private key*
- V_H_{PuK} : *VLR - HLR link' s public key*
- M_V_{PrK} : *MS - VLR link' s private key*
- M_V_{PuK} : *MS - VLR link' s public key*
- H_{PrK} : *HLR private key*
- H_{PuK} : *HLR public key*
- M_{PrK} : *Mobile station' s private key*

- M_{PuK} : *Mobile station's public key*

These three entities exchange four messages with each other as shown in Figure 3. The detail of the elements in each of these messages is given below.

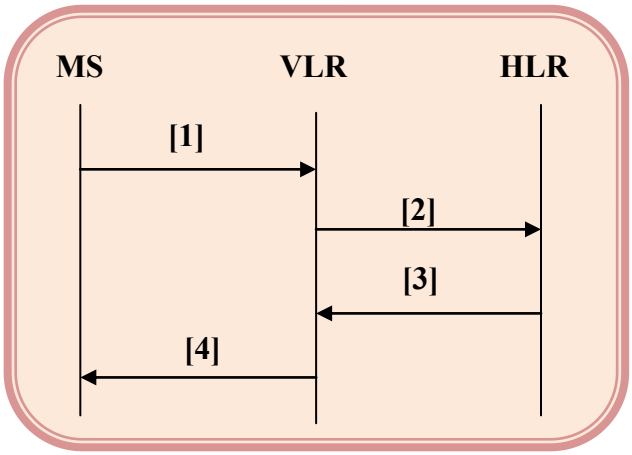

Fig.3 Authentication process using public key cryptography

- *Identity message* $= E_{M\_V_{Puk}}(IK \,||\, SK \,||\, RAND) \,||\, E_{H_{Puk}}(IMSI \,||\, K_i)$
- *Authentication Information* $= E_{H_{Puk}}(IMS \,||\, K_i)$
- *Authentication Acknowledge* $= M_{Puk}$
- Forward Authentication Acknowledge $= E_{M_{Puk}}(RAND)$

The symbol '||' represents the concatenation of two elements. The MS creates secret keys SK, IK and a random challenge RAND. It starts the authentication exchange by sending an Identity Message to the visited VLR. This message consists of the concatenation of RAND, SK and IK encrypted using the public key M_V_{PuK}. The IMSI and K_i encrypted using the public key H_{PuK} is also part of the Identity message.

The VLR uses the corresponding private key M_V_{PrK} to decrypt its part of the message and extract the needed information RAND, SK and IK. The VLR forwards the rest of message $(E_{H_{PuK}}(IMS \,||\, K_i))$ unchanged as an Authentication Information message to the HLR. The keys SK and IK are used later for confidentiality and integrity of both the data and signals, respectively.

The HLR decrypts the Authentication Information message with its private key H_{PrK} and gets the IMSI and K_i sent from MS. The secret key K_i is used as a random challenge for user/MS authentication. The MS and the HLR have the same secret key K_i. The HLR compares the received K_i with its own K_i. If they match, the user is authenticated.

Using the IMSI, the HLR finds the corresponding user's public key M_{PuK} and is sent to VLR in the Authentication Acknowledge message. This message acts as an indication to the VLR that the user has been authenticated by the HLR. The VLR uses the public key M_{PuK} to encrypt the RAND challenge received from MS in the Identity Message. The MS decrypts it with its own private key. The result is compared with the RAND stored at the MS. If they are equal, the VLR is authenticated as it ensures the MS that the VLR is the only entity having the MS-VLR link's private key M_V_{PrK}.

The problem with this protocol is that a denial-of-service attack may be possible if the attacker changes the signaling contents based on which the user and network authenticate each other. For example, if the encrypted content of RAND challenge is modified or if IMSI or K_i is changed during transmission, the network and user authentication will fail even if the user and network are legitimate. To cope with this problem, a digital signature can be used. The end-to-end integrity of the authentication parameters should be ensured because the end entities, the VLR/HLR and the MS, make the decision of authentication. Moreover, the protocol involves four exchanged messages and this causes signaling overhead.

The proposed protocol based on the tripartite signcryption is more efficient than encryption then signature[12]. Moreover, the number of exchanged messages becomes three rather than four messages. The next section discusses the proposed improvement in details.

6. THE PROPOSED AUTHENTICATION PROTOCOL BASED ON THE TRIPARTITE SIGNCRYPTION SCHEME

Using signcryption achieves both confidentiality of message contents and authentication. Signcryption will solve the denial of service attack in [1]. Also, using a tripartite scheme reduces the number of exchanged signals between the entities. Figure 4 shows the exchanged messages in the proposed authentication protocol.

[1]Identity message and authentication information =
[Signcrypt$(m_1 = IK//SK//RAND), (m_2 = IMSI//K_i)$*],*
MS sends this message to both VLR and HLR

[2] Authentication Acknowledge $= Q_{MS}$

[3]Forward Authentication Acknowledge
= Signcrypt (RAND)

The signcryption set up is done as in Section 3.2 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 $Q = dR$. The key pairs for entities MS, VLR and HLR are given as $Q_{MS} = d_{MS}.R$, $Q_{VLR} = d_{VLR}.R$ and $Q_{HLR} = d_{HLR}.R$ respectively.

The *MS* creates secret keys *SK*, *IK* and a random challenge *RAND*. It starts the authentication process by sending an Identity Message to the visited *VLR*. This message includes two parts. The first part (denoted as m_1) is used by *MS* and *VLR*, which is the concatenation of *RAND*, *SK* and *IK* . The second part (denoted as m_2), which is the concatenation of *IMSI* and K_i. Both m_1 and m_2 are signcrypted by the tripartite scheme in Section 3 using the public keys of *VLR* and *HLR* and the private key of MS.

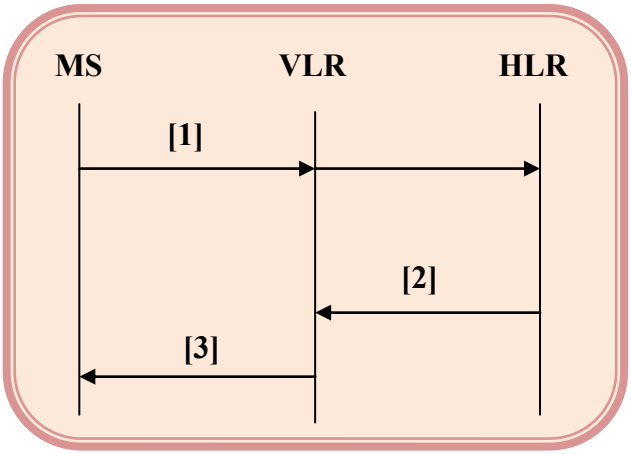

Fig. 4 The exchanged messages in the proposed protocol

The ciphers are

$c_{VLR} = E_{k_2}(RANND \,||\, SK \,||\, IK)$,

$c_{HLR} = E_{k_3}(IMSI \,||\, K_i)$

MS computes the signcrypted cipher $c = (c_{VLR} \,||\, c_{HLR})$, and the signature $r = Hash(k_1, c)$ and $s = (w - r.d_{MS}) mod\ q$ then sends them to both *VLR* and *HLR*.

The *HLR* uses the corresponding private key d_{HLR} with Q_{MS} and gets the *IMSI* and K_i sent from *MS*. The secret key K_i is used as a random challenge for user/*MS* authentication. The *MS* and the *HLR* have the same secret key K_i. The *HLR* compares the received K_i with its own K_i. If they match, the user is authenticated. It is difficult for a third party to change this secret without being detected by *HLR*. The *HLR* can easily detect it using *IMSI* of the requesting user sent in the Identity message and the signature verification fails.

Using the *IMSI*, the *HLR* finds the corresponding user's public key Q_{MS} and is sent to *VLR* in the Authentication Acknowledge message. This message acts as an indication to the *VLR* that the user has been authenticated by the *HLR*. The *VLR* uses the public key Q_{MS} with its private key d_{VLR} to unsigncrypt its part of the message and extract the needed information *RAND*, *SK* and *IK*. The keys *SK* and *IK* are again used for confidentiality and integrity of both the data and signals, respectively. It also uses the public key Q_{MS} to signcrypt the *RAND* challenge received from *MS* in the Identity message. The *MS* decrypts it with its own private key d_{MS} and the *VLR* public key Q_{VLR}. The result is compared with the *RAND* stored at *MS*. If they are equal, the *VLR* is authenticated as it ensures the *MS* that the *VLR* is the only entity having the same secret key.

This approach overcomes the denial of service attack using the signcryption primitive as discussed in the security analysis of the proposed tripartite scheme under the unforgeability property. The approach in [1] suffers from the denial of service attack and the author suggested adding a digital signature after encryption but it consumes time and involves a large number of computations. Therefore, using signcryption is more efficient than sign-then-encrypt primitive [12]. Moreover, this entire process involves three rather than four signaling messages compared to [1], thus signaling overhead is reduced.

7. CONCLUSION

In this paper, a new communication protocol used in GSM using tripartite signcryption scheme without using bilinear pairings that proposed in [13]. The proposed scheme is used to reduce the signaling overhead in the authentication step in mobile communication systems and combats the denial of service attack. The proposed protocol implemented by three steps to achieve the authentication between the three parties MS, HLR and VLR and this reduces the signaling overhead when compared with the protocol in [1] that implemented using four steps to achieve the authentication between the three parties MS, HLR and VLR

8. REFERENCES

[1] W. Khan and H. Ullah, "Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 9, May 2010 ,ISSN (Online): 1694-0784 ISSN (Print): 1694-0814

[2] Y. Li, Y. Chen, and T. MA, "Security in GSM", Retrieved March 18, 2008, from http://www.gsm-security.net/gsm-security-papers.shtml.

[3] N. T. Trask and M. V. Meyerstein, "Smart Cards in Electronic Commerce", A Springer Link journal on BT Technology, Vol. 17, No. 3, 2004, pp. 57-66.

[4] N. T. Trask and S. A. Jaweed, "Adapting Public Key Infrastructures to the Mobile Environment", A SpringerLink journal on BT Technology, Vol. 19, No. 3, 2004, pp. 76-80.

[5] M. Nabil, Y. Abouelseoud, G. Elkobrosy, and A. Abdelrazek , "New Authenticated Key Agreement Protocols", Proceeding of The International Multiconference of Engineers And Computer Scientists (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] 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.

[8] 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.

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

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

[11] V. Hassler and P. Moore, "Security Fundamentals for E-Commerce", Artech House London Inc., 2001, pp. 356-367.

[12] 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.

[13] H. Elkamchouchi, E. Abou El-kheir, and Y. Abouelseoud, " An Efficient Tripartite Signcryption Scheme Without Bilinear Pairings", International Journal of Scientific & Engineering Research, Volume 4, Issue 11, November-2013 1010, ISSN 2229-5518