An efficient Secure Electronic Mail System based on Elliptic Curve Certificateless Signcryption

Roayat Ismail Abdelfattah
Electronics and Communication
Dept, Faculty of Engineering,
Tanta University
Tanta, Egypt

Lamiaa Abdelsalam Telb
Electronics and Communication
Dept, Faculty of Engineering
Tanta University
Kafrelsheikh, Egypt

Mahmoud Ahmed Attia
Electronics and Communication
Dept, Faculty of Engineering
Tanta University
Tanta, Egypt

ABSTRACT

Electronic Mail or E-mail is an important development in the communication world. Therefore, the email security and efficiency has become a critical issue. Most of the existing email systems use either S/MIME (Secure/Multipurpose Internet Mail Extensions) or PGP (Pretty Good Privacy) which depend on Public Key Infrastructure (PKI) or Identity-Based Cryptography (IBC) and use inefficient signature-then-encryption techniques. Each one of these techniques has its own drawbacks. Recently, Certificateless Cryptography (CLC) and Elliptic Curve (EC) based signcrption which combines both signature and encryption in logically one step are developed to overcome these drawbacks with efficient methods. In this paper, a CLC-EC- signcryption based secure E-mail system is proposed. To make the system more efficient, the encryption key is hidden in the transmitted ciphertext itself. The system is highly secure as it uses multi-factor authentication technique includes IP address, password and fingerprint for registration and login. It provides all the security services: confidentiality, integrity, authentication, non-repudiation and forward secrecy with high efficiency compared with other recently existing schemes. Also, it is optionally for the user to send his email in clear form or signcrypted. Finally, it is practically implemented by C# programming language and it can work on the real network system without changing in the existing network architecture.

General Terms

Security

Keywords

Certificateless Cryptography; signcryption; Elliptic Curve Cryptography; multi-factor authentication.

1. INTRODUCTION

The importance of E-mail is summarized in that the exchange of messages and sensitive documents using computer technology and the Internet easily, instead of paper mail and fax. E-mail started in 1965 at the Massachusetts Institute of Technology (MIT) and it was called MailBox to exchange messages among computers. In 1971, an email system appeared by Ray Tomilson in the department of defense (DoD) and succeeded in sending an email to himself [1]. The existing email system uses the Internet as a transmission medium with standard protocols such as Simple Mail Transfer Protocol (SMTP), the Internet Mail Access Protocol (IMAP) and the Post Office Protocol (POP). But these e-mails can be accessed by attackers, so it has to be protected such that no one can access these messages except the desired people. Any protocol for securing email has to achieve four basic and necessary security requirements, namely, authentication, confidentiality, integrity and nonrepudiation. The existing e-mail security systems as S/MIME and PGP which based on PKI or IBC are inefficient and suffer from some limitations. For example, PKI suffers [2] from key management problems, complex, expensive certificate management and problems in scalability. To overcome the key management drawback, some email protocols using IBC have been introduced [3-5] .In IBC, the user's email address is used as his public key while a trusted third party named Private Key Generator (PKG) generates private key for each user then transmitted it to users on a secure channel. So IBC has a drawback which is the key escrow problem as the PKG know users' private keys and hence it is able to decrypt any message which violates the nonrepudiation service. In this paper, an email system using a CL-EC signcryption will be introduced to overcome drawbacks of both PKI and IBC based mailing systems and achieves all the required security services [6]. The encryption key is hidden in the transmitted cipher text itself by using an ideas originated from steganography [7-10]. The security of proposed scheme is enhanced using a multi-factor authentication technique for registration and login to the system is used. . The rest of this paper is organized as follows: section 2 presents preliminaries to the CLC, ECC and signcryption, section 3 introduces the proposed system, section 4 introduces simulation results, section 5 gives security analysis, section 6 gives comparison analysis. Finally, section 7 gives conclusions.

2. PRELIMINARIES

2.1 Certificateless Public Key Cryptography (CL-PKC)

In 2003, CL-PKC has been introduces by Al-Riyami and Paterson [11] to address the drawback of IBC as it has a different scenario. A trusted third party, named the Key Generation Center (KGC) generates the partial private key for each user who then chooses a secret value and combines it with the partial private key to obtain his private key. So the user's private key is unknown to the KGC. By Comparing CL-PKC to IB-PKC, the trust level in the third party is reduced. The KGC has no chance to replace a user's public key due to the used blinding method by the user. CL-PKC [12-15] has more advantages than PKI and IBC so it is an ideal alternative to them.

2.2 Elliptic Curve Cryptography (ECC)

PKC system depends on using two separate keys, one public and the other is private for encryption and decryption respectively. The larger the key size the more secure the system is. The most common mathematical hard problems used in PKC are integer factorization and discrete logarithm. These two hard problems are used in RSA and DSA algorithms respectively. In 1985, Miller [16] and Koblitz [17] introduced a new public key cryptography called elliptic curve (EC) which improves the efficiency of various techniques. Actually, cryptographers have found that they can achieve computational efficiency in performance and higher security with very low key-size compared to other algorithms. ECC [18-20] uses smaller parameters compared with other competitive algorithms as RSA [21], with the same levels of security. This achieves fewer computations, processing power and storage space. An EC is defined as the set of points given as

$$y^2 = x^3 + ax + b \qquad (1)$$

Where$4a^3 + 27b^2 \neq 0$ (modp). This is named EC Weierstrass normal form as shown in Fig. 1.

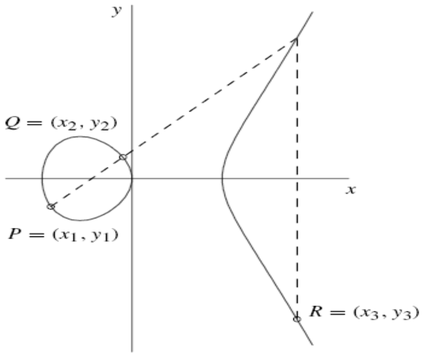


Figure 1: Addition: R=P+Q

- *EC point addition:*

If P(x_1, y_1) and Q(x_2, y_2) are two points on an EC and P(x_1, y_1) ≠ Q(x_2, y_2), by drawing line between P and Q it will intersect the EC at a third point R(x3,y3).The addition of P and Q is reflection of this point about x-axis. It is calculated using following equations:

$$x_3 = \lambda^2 - x_1 - x_2 \qquad (2)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \qquad (3)$$

$$\text{And } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{if } P \neq Q \qquad (4)$$

EC Discrete Logarithm Problem EC-DLP:

For a point P □□E(Fq) of order n, where E is an EC defined over a finite field Fq, and another point Q□□E(Fq), the EC-DLP is to find the integer k □□[0, n −1] such that Q = k P. The integer k is named the DL of Q to the base P, denoted k = logP Q.

Q = kP is called scalar point multiplication, which consume the most time in ECC computations. The private key of each user is chosen randomly while the public key is the multiplication of the private key with a generator point G on the EC.

2.3 Signcryption

Zheng in 1997 [22] introduces a cryptographic scheme, called signcryption, that merges the digital signature and the encryption into one logical step, so requires a smaller computational cost compared to encryption then signature systems. This signcryption achieved 50% fewer computational cost and 85% fewer communication overhead. Since then, many signcryption schemes have been introduced [23-29].

2.4 Multi-factor authentication (MFA) Technique

MFA achieves a second level of security during logging in. It prevents unauthorized users from logging into the accounts and hence protects identities, data, money…etc. When logging in, a user is required to enter a password and also authenticate him using a second factor. There are many types of authentication factors as passwords, smart cards, biometrics (face-eye-hand-fingerprint…ect) and a user's location information (example: GPS, IP address). The proposed scheme uses IP address; password and fingerprint as MFA.

3. THE PREPOSED SYSTEM

The proposed scheme includes three parties: Key Generator Center (KGC) calculates the partial private key for all users when they register in the system, the sender who signcrypt the desired message and the receiver who unsigncrypt the received message. It consists of two phases:

- Offline phase: the users do it without having a message to send.
- Online phase: the users do it when they have a message to send.

The block diagram of sending and receiving a message with the proposed scheme is shown in Figure 2 and Figure. 3.

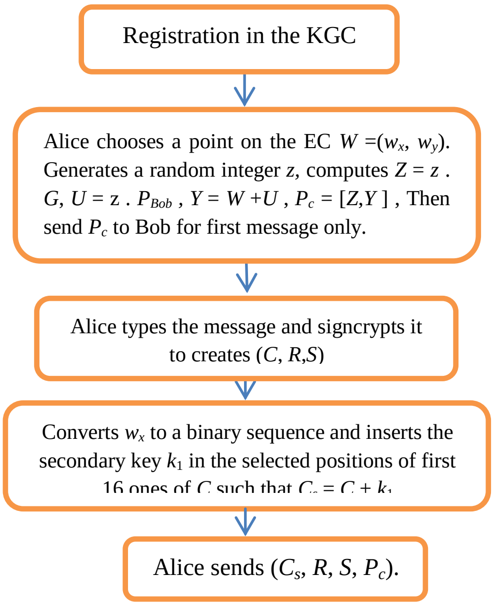

Registration in the KGC
Alice chooses a point on the EC $W = (w_x, w_y)$. Generates a random integer z, computes $Z = z \,.\, G$, $U = z \,.\, P_{Bob}$, $Y = W + U$, $P_c = [Z, Y]$, Then send P_c to Bob for first message only.
Alice types the message and signcrypts it to creates (C, R,S)
Converts w_x to a binary sequence and inserts the secondary key k_1 in the selected positions of first 16 ones of C such that $C_s = C + k_1$
Alice sends (C_s, R, S, P_c).

Figure 2: Sending secure email

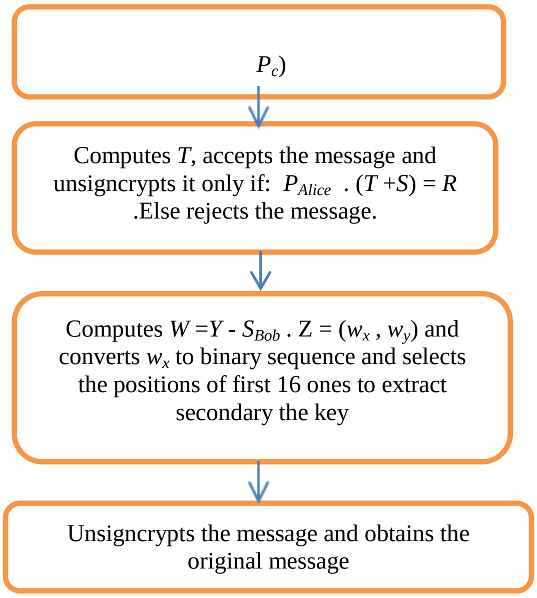

P_c)
Computes T, accepts the message and unsigncrypts it only if: P_{Alice} . (T +S) = R .Else rejects the message.
Computes $W = Y - S_{Bob}$. Z = (w_x , w_y) and converts w_x to binary sequence and selects the positions of first 16 ones to extract secondary the key
Unsigncrypts the message and obtains the original message

Figure 3: Receiving secure email

3.1.Offline phase

This phase makes the proposed scheme more efficient. It consists of three sub phases: registration, key generation, and transmission of master secret key

3.1.1. Registration phase

All users have to register to the KGC sever by providing multifactor authentication (user ID, password and finger print) to enable the user to login every time.

Key generation phase

It includes two major steps: selection of domain parameters and key generation.

3.1.1.1. Selection of domain parameters

The parameters are:

p	a large prime integer with $p > 2^{160}$
a ,b	Two integer's elements that satisfy the equation: $4a^3+27b^2 \bmod p \neq 0$.
F	The EC over finite field ($y^2 = x^3+ax+b \bmod p$) where x and y both lie in [1, 2 …... p-1].
∞	A point (x, y) of F at infinity.
G	A base point on F (a generator of Elliptic curve).
n	The order of point G such that $n.G = \infty$ And $n > 2^{160}$.
H	One way hash function which is SHA-256.
$E_k(.)/D_k(.)$	The encryption/decryption scheme which is AES-128 bit.

3.1.1.2. Key Generation

The proposed scheme uses the same steps of Al-Riyami and Paterson Scheme [11]; which consists of five steps: setup, secret value set, extraction of partial private key, private and public keys set.

Setup: This step is performed by the KGC which do the following:

1. Select a generator $G \in F$.
2. Select a master secret-key $s < p$, and compute public key of KGC

$$P_0 = s.G \tag{5}$$

Secret value set: This step is performed by the user who do the following:

1. User m that has identifier ID_m selects $x_m < p$.
2. Computes his/her public key:

$$X_m = x_m .G \tag{6}$$

and sends X_m to the KGC.

a. Extraction of partial private key: The KGC constructs the partial private key for user m whose identifier ID_m as following:

1. Calculate:

$$Q_m = H(ID_m \| X_m) \tag{7}$$

2. Calculate the partial private key:

$$D_m = s . Q_m \tag{8}$$

b. Private key set: In this step the user m does the following:

Compute the private key S_m from the partial private key D_m as following:

$$S_m = x_m . D_m = x_m s . Q_m \tag{9}$$

c. Public key set: the user m constructs his public key as: $P_m = S_m . G$ (10)

Finally the user m has one key pair (S_m, P_m)

Assume Alice is the receiver who with a private key, $S_{Alice} = x_{Alice} . D_{Alice}$, and a public key $P_{Alice} = S_{Alice} . G$, while the receiver Bob with a private key, $S_{Bob} = x_{Bob} .D_{Bob}$, and a public key, $P_{Bob} = S_{Bob} .G$. All users' public keys are available on the KGC's secure web site.

In the proposed scheme two secret keys will be used for encryption: the primary key and the secondary key. The primary key is constant for all the messages and is used to determine the positions of the ciphertext where the secondary key is hidden, while the secondary key is a varying with each message and it is hidden in the ciphertext. The message will be encrypted with the secondary key.

3.1.2. Transmission of primary secret

EC encryption is used once for transmission of primary secret key as follows:

At the sender (Alice)

1. Select a random point on the elliptic curve $W = (w_x , w_y)$ where w_x is used as the primary secret key.
2. Convert w_x to binary sequence then determine the positions of first 16 ones. this places will be the positions in the ciphertext where the secondary key bytes will be inserted. In every position of ones in w_x insert one byte of the secondary key in the ciphertext. To send the primary key w_x securely to the receiver, EC encryption will be used as following:

Generate a random number z and compute:

$$Z = z . G \tag{11}$$

$$U = z . P_{Bob} \tag{12}$$

$$Y = W + U \tag{13}$$

$P_c = [Z, Y]$ is the encrypted primary secret key which Alice sends to Bob only one time before the existence of any message.

At the receiver: Upon receiving $P_c = [Z, Y]$, Bob compute $W = Y - (S_{Bob}. Z) = (w_x , w_y)$ (14)

Then convert w_x to binary sequence to determine the ones positions.

3.2.Online phase

This phase consists of two sub phases: signcryption and unsigncryption.

3.2.1. Signcryption

When Alice has a message M to send in an E-mail to Bob, she does the following:

1. Choose a random integer $x < p$.
2. Compute Hash value of x with SHA-256 and divide it into two blocks k_1 and k_2 each of 128 bit length. k_1 will be used as the secondary secret key for message encryption with AES-128:

$$C = E_{k_1}(M) \qquad (15)$$

3. k_1 will be hidden in the ciphertext by using the primary w_x as follow : k_1= 128 bit = 16 byte, these bytes will be inserted in the ciphertext C in the first 16 positions of ones in w_x . If number of ones in w_x less than 16 in this case insert the reminder of 16 bytes of k_1 in the end of C. Now the transmitted ciphertext will be $C_s = C + k_1$.

4. Select random number v < p.

5. Compute:

$$R = v . G = (R_x, R_y) \qquad (16)$$

$$T = Hash\ (C_s\ //\ R_x) \qquad (17)$$

The symbol // means the concatenation.

$$S = (v / S_{Alice} - T) \bmod p \qquad (18)$$

Then Alice sends (C_s, R, S) to Bob.

3.2.2. UnSigncryption phase

Upon receiving (C_s, R, S), Alice does the following:

1. Compute:

$$T = Hash\ (C_s\ //\ R_x) \qquad (19)$$

2. Accept (C_s) only if: P_{Alice} . (T + S) = R else reject the message.

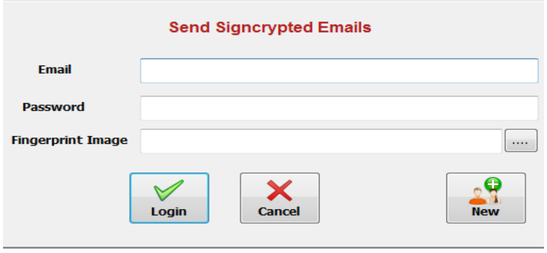
3. Extract(k_1)from (C_s) where $C = C_s – k_1$

4. Decrypt (C) to obtain the message as:

$$M = E_{k_1}(C) \qquad (20)$$

4. SIMULATION RESULTS

Proposed scheme is implemented in software using C# programming language with windows 64-bit operating system, processor Intel (R) Core(TM) i5-3340M CPU @2.70 GHz and memory (RAM) 4.00 GB. The results are displayed in the figures from Figure 4 to Figure 15.

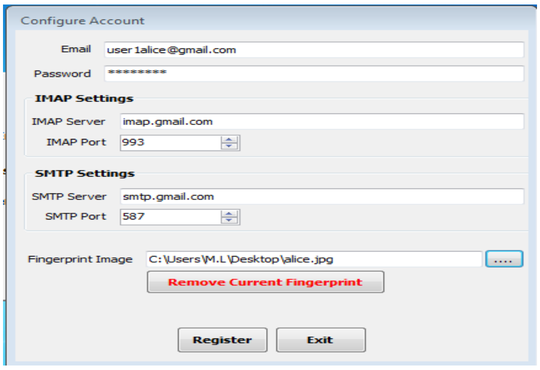

Send Signcrypted Emails

Email

Password

Fingerprint Image

Figure 4: Snapshot of send receive program.


Configure Account

Email: user1alice@gmail.com

Password: ********

IMAP Settings

IMAP Server: imap.gmail.com

IMAP Port: 993

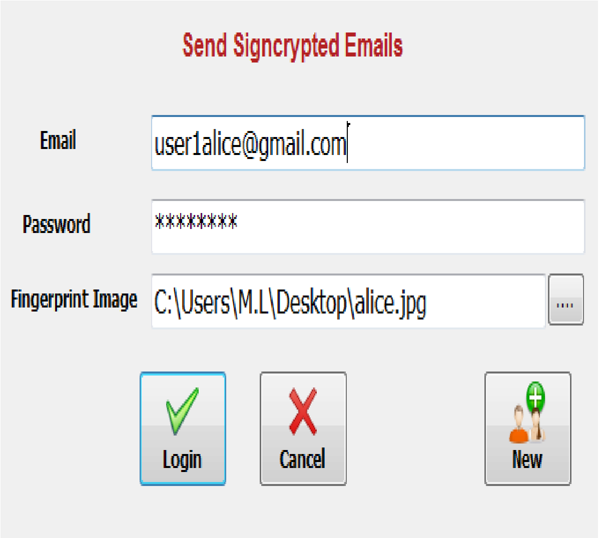
SMTP Settings

SMTP Server: smtp.gmail.com

SMTP Port: 587

Fingerprint Image: C:\Users\M.L\Desktop\alice.jpg

Figure 5: The first join of the user to the system press New button , enters his data then press Register to join to KGC.


Send Signcrypted Emails

Email: user1alice@gmail.com

Password: ********

Fingerprint Image: C:\Users\M.L\Desktop\alice.jpg

Figure 6: The user that already registers on the KGC enters his Email ID, password, and his finger print image, then press log in button.

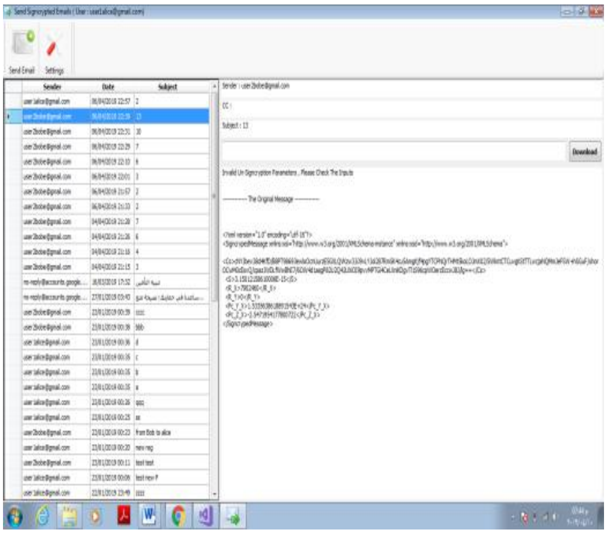
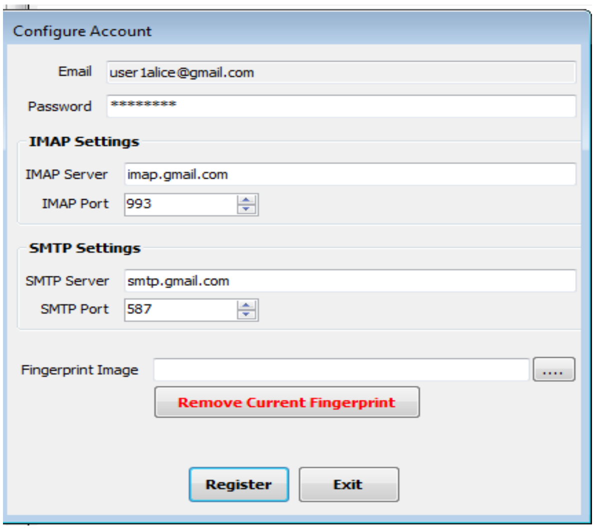


Figure 7: Send- receive program contents of two menus.


Configure Account

Email: user1alice@gmail.com

Password: ********

IMAP Settings

IMAP Server: imap.gmail.com

IMAP Port: 993

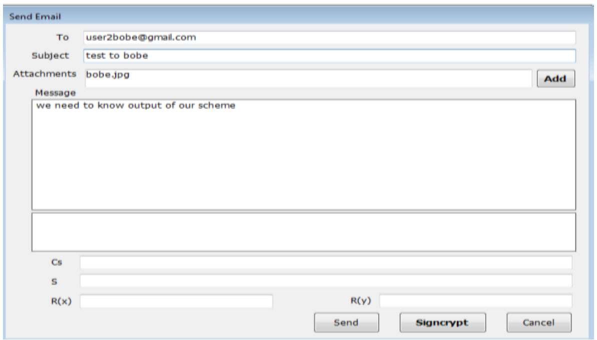
SMTP Settings

SMTP Server: smtp.gmail.com

SMTP Port: 587

Fingerprint Image

Figure 8: Settings menu



Send Email

To: user2bobe@gmail.com

Subject: test to bobe

Attachments: bobe.jpg [Add]

Message: we need to know output of our scheme

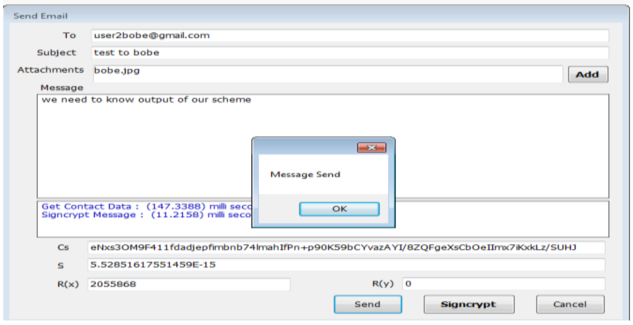
Cs

S

R(x) R(y)

[Send] [Signcrypt] [Cancel]

Figure 9: Send email that used for sending the desired email without signcryption.



Send Email

To: user2bobe@gmail.com

Subject: test to bobe

Attachments: bobe.jpg [Add]

Message: we need to know output of our scheme

Get Contact Data : (147.3388) milli seco
Signcrypt Message : (11.2158) milli seco

Message Send [OK]

Cs: eNxs3OM9F411fdadjepfimbnb74lmahIfPn+p90K59bCYvazAYI/8ZQFgeXsCbOeIImx7iKxkLz/SUHJ

S: 5.52851617551459E-15

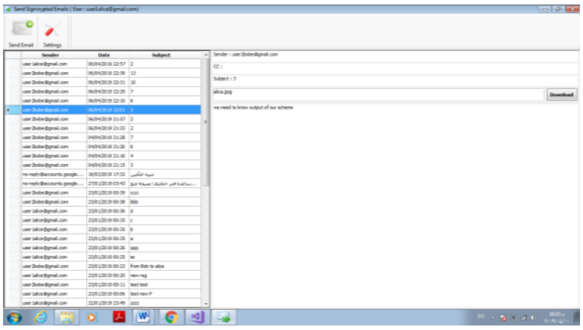
R(x): 2055868 R(y): 0

[Send] [Signcrypt] [Cancel]

Figure 10: After signcryption of the message, press on "Send" button to send the signcrypted message to the receiver that is already register on the web site of key generation center.

Note that in the snapshot of signcryption time is about 11 mill seconds, while the same signcrypted message in [30] takes 197 mills second which proves that proposed scheme is very efficient.

If the signature is correctly verified, the receiver will decrypt the ciphertext to recover the original message. While if the signature isnt verified, a warning message will appear and so the ciphertext will not be decrypted.



Send Signcrypted Emails (User : user1alice@gmail.com)

Sender : user2bobe@gmail.com

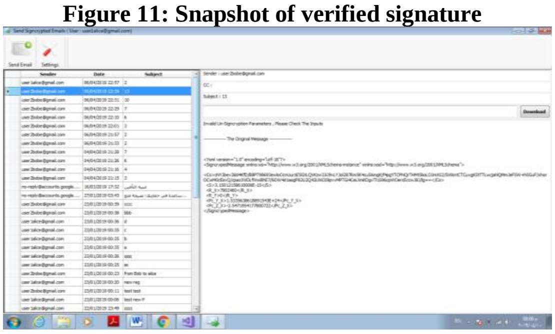
CC :

Subject : 3

alice.jpg [Download]

we need to know output of our scheme

Figure 11: Snapshot of verified signature



Send Signcrypted Emails (User : user1alice@gmail.com)

Sender : user2bobe@gmail.com

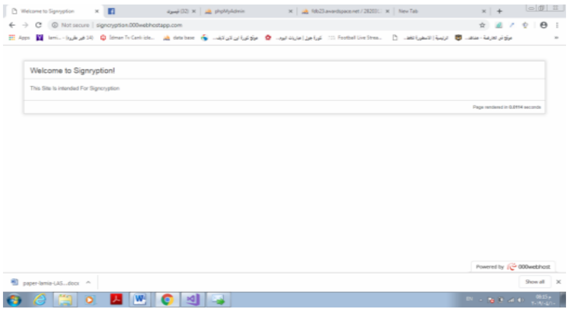
CC :

Subject : 13

Invalid Un-Signcryption Parameters , Please Check The Inputs

———— The Original Message ————

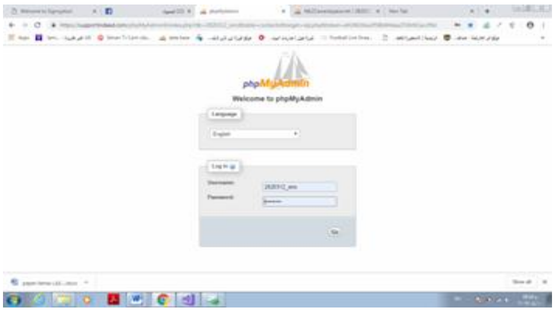
Figure 12: Snapshot of unverified signature with changing only one byte of S



Welcome to Signryption!

This Site Is intended For Signcryption

Figure 13: Snapshot of web site of KGC



Welcome to phpMyAdmin

Figure 14: Snapshot of database of KGC

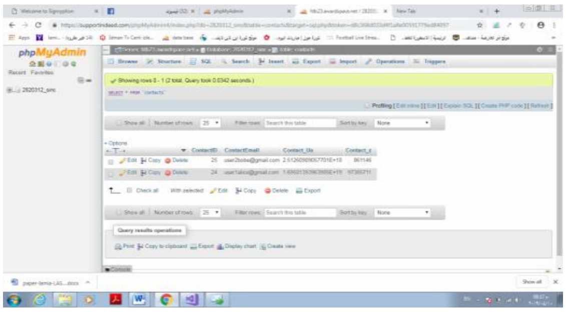


Figure 15: Snapshot of data base of key generation center

5. SECURITY ANALYSIS

The proposed scheme is an EC-DLP based scheme. For an entity m whose public key is

$P_m = S_m . G$, where S_m is his/her private key and G is the generator of the EC, then if both S_m and G are given, the public key $P_{m.}$ can be easily computed. But given the public key P_m and G, the computation of the private key S_m is computationally hard. This is known as the EC-DLP. The proposed scheme achieves all security services as follows:

5.1 Confidentiality

In the proposed scheme, there are two secret keys: the primary key w_x and the secondary key k_1. The secondary key k_1 is inserted in the ciphertext in positions depending on the ones in the binary sequence of the primary key. So proposed scheme security depends totally on the primary key w_x which is protected by the EC-DLP.

The attacker has access to only C_s ,R ,S and $P_{C.}$ To obtain w_x he has to know z or S_{Bob} which are protect by EC-DLP according to Eqns. 11,12,13, and 14.

5.2 Message integrity and non-repudiation

From the digital signature equation S= (v / S_{Alice} - T) mod p the sender Alice signs using his private key S_{Alice} and he/she cannot disown sending the email message. The receiver verifies if

P_{Alice} . (T +S) = R. If it is verified, then (C_s, R, S) is actually sent by the sender Alice. Else the sender did not send it.

5.3 Public verification

Proposed scheme achieves public verification for the signature. This means that anyone can be a judge and can verify that the sender actually sent the message. The receiver sends (Cs, R, S) to the judge who can do the following:

1) Calculate T = Hash(C_s // R_x).
2) If P_{Alice} . (T +S) = R, then the judge will be sure that sender actually sent (C_s, R ,S) to the receiver, other else the sender did not send it.

Here, all variables that are used in the judge verification are public.

5.4 Forward Secrecy

Forward secrecy means even though the attacker obtained the sender's private key, he cannot recover plaintext M. In the propose scheme, if the attacker tries to derive the plaintext M from (C_s, R, S), he must obtain the secondary key secret k_1 which is hidden in ciphertext according to the ones positions of the binary sequence of the primary key w_x. To obtain w_x he needs to know W = Y - U = Y - (z . P_{Bob}) =Y – (S_{Bob} . Z) = (w_x, w_y) where W is independent on sender's private key and protected by EC encryption. Therefore, the proposed scheme achieves forward secrecy.

5.5 Firewall effect

The proposed scheme provides a firewall effect which means that the signature is verified before decryption. Upon receiving the ciphertext (C_s, R, S), the receiver firstly verifies if (P_{Alice} . (T +S) = R). Then decrypt C_s to obtain the plaintext, else he rejects it without decryption.

6. COMPARISON

Here, a comparison of proposed scheme with similar existing schemes will be given. The schemes in [13, 31] use the pairing [32] and encryption-then -signature which is inefficient. The scheme in [33] uses certificate cryptography that has some problems and doesn't achieve public verification property. The scheme in [30] also uses pairing so it is inefficient. The scheme in [37] also uses pairing and depend on integer factorization problem which is inefficient .The comparison is shown in Table 1 and Fig. 16. Mul. means No. of point multiplication.

Table 1: Comparison between of the proposed system with other existing schemes

Scheme	Mul.	Firewall	Pairing	Public-key system	Public verification
Scheme1 in [33]	5	NO	NO	CA	NO
Scheme2 in [30]	8	NO	YES	CLC	NO
Scheme3 in [34]	9	NO	NO	CLC	NO
Scheme4 in [35]	6	YES	NO	CA	YES
Scheme5 in [36]	8	NO	NO	CLC	NO
Proposed Scheme	3	YES	NO	CLC	YES

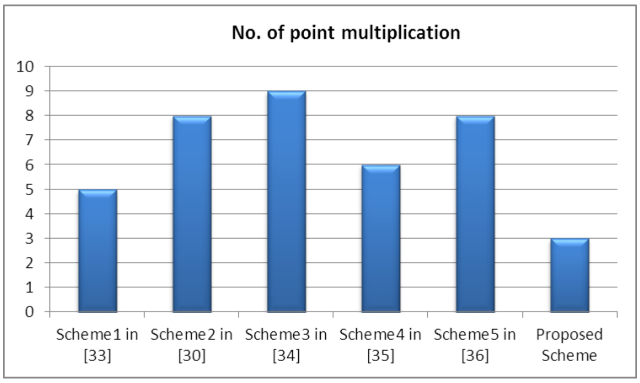


Figure 16: proposed scheme compared with other similar existing schemes.

7. CONCLUSION

An efficient secure email scheme based on CL-EC signcryption is introduced in this paper. It achieves all the required security services in an efficient method. The scheme can be applied on the real network system without making remarkable modifications to the currently existing email system. The proposed signcryption is optional and it is implemented using C# programming language. Security analysis of the proposed scheme has been provided. According to the results, proposed scheme is more efficient than the existing email schemes due to its least number of EC point multiplications without bilinear pairings operation which is time consuming.

8. REFERENCES

[1]. J. B. Postel, "Simple mail transfer protocol", 1982. http://www.rfc-editor.org/info/rfc821.

[2]. Buchmann, Johannes A., Karatsiolis, Evangelos, Wiesmaier, Alexander, "Introduction to Public Key Infrastructures " © Springer-Verlag Berlin Heidelberg 2013.

[3]. https://en.wikipedia.org/wiki/ID-based_cryptography

[4]. A. Shamir, "Identity-based cryptosystems and signature schemes", in Advances in Cryptology-CRYPTO'84, 1984, pp. 47–53.

[5]. Ays¸e G¨ul Karatop and Erkay Savas¸ "An Identity-Based Key Infrastructure Suitable for Messaging Applications" Faculty of Engineering and Natural Sciences Sabanci University Istanbul, Turkey.

[6]. S. William, "Cryptography and Network Security", vol. 139, no. 3. Boston, USA. Prentice Hall, 2011.

[7]. Khalil Challita and Hikmat Farhat," Combining Steganography and Cryptography: New Directions " (IJNCAA) 1(1): 199-208, 2011 (ISSN 2220-9085).

[8]. Venkata Bhanu Chowdary Allada, Mallikarjun Susarla "Developing an Efficient Solution to Information Hiding through Text Steganography Along with Cryptography", IJCST Vol. 8, Issue 1, Jan - March 2017.

[9]. Amal Khalifa "LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography" Conference Paper · November 2013.

[10]. Magdy Saeb,"Encryption Key Distribution Applying Steganographic Techniques", (IJCSCS) August 2014.

[11]. S. Al-Riyami and K. Paterson, "Certificateless public key cryptography", In C. Laih, editor, Asiacrypt 2003, Lecture Notes in Computer Science, pages 452-473, 2003.

[12]. A. R. Sattam and P. Kenneth,"Certifcateless public key cryptography a full version," in Asiacrypt'03,LNCS 2894, Springer, pp. 452- 473, 2003.

[13]. Suresh Kumar Balakrishnan and V. P. Jagathy Raj "Practical Implementation of a Secure Email System Using Certifcateless Cryptography and Domain Name System", International Journal of Network Security, Vol.18, No.1, PP.99-107, Jan. 2016.

[14]. Sattam S. Al-Riyami and Kenneth G. Paterson ,"Certificateless Public Key Cryptography", Advances in Cryptology - ASIACRYPT 2003 pp 452-473 .

[15]. Alexander W. Dent,"A Brief Introduction to Certificateless Encryption Schemes and their Infrastructures", EuroPKI 2009: Public Key Infrastructures, Services and Applications pp 1-16.

[16]. Miller M.,"Uses of elliptic curves in cryptography". Advances in Cryptography Crypto '85.1986; 417-426.

[17]. Koblitiz N., "Elliptic curve cryptosystems". Mathematics of computation. Vol. 48; No. 177; 1987; 203-208.

[18]. D. Hankerson, A. J. Menezes, and S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag New York Inc, 2006.

[19]. Jeffrey L. Vagle, "A Gentle Introduction to Elliptic Curve Cryptography", November 21, 2000.

[20]. Joseph H. Silverman,"An Introduction to the Theory of Elliptic Curves", 2006.

[21]. https://simple.wikipedia.org/wiki/RSA_algorithm.

[22]. Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)," in Seventeenth Annual International Cryptology Conference, 1997, pp. 165-179.

[23]. JM L., Mao W., " Two birds one stone: signcryption using RSA". In Topics in Cryptology (CT-RSA'03), Joye M (ed), LNCS 2612. Springer-Verlag: San Francisco, CA, USA, 2003; 211–225.

[24]. Malone-Lee J, "Identity based signcryption". Available from: http://eprint.iacr.org/2002/098.pdf [Accessed on 30 May 2011].

[25]. Libert B., Quisquator JJ., "A new identity based signcryption scheme from pairings". In Proceedings of IEEE Information Theory Workshop (ITW'03). Elsevier: Paris, France, 2003; 155–158.

[26]. Chow SSM, Yiu SM, Hui LCK, Chow KP," Efficient forward and provably secure ID based signcryption scheme with public verifiability and public ciphertext authenticity". In Proceedings of Information Security and Cryptology (ICISC'03), Lim JI, Lee DH (eds), LNCS 2971. Springer-Verlag: Seoul, Korea, 2004; 352–369. International Journal of Computer Applications (0975 – 8887) Volume 165 – No.2, May 2017 43.

[27]. Boyen X., "Multipurpose identity based signcryption: a Swiss army knife for identity based cryptography". In Advance in Cryptology (CRYPTO'03), Boneh D (ed), LNCS 2729. Springer-Verlag: Santa Barbara, California, USA, 2003; 383–399.

[28]. Chen L., Malone-Lee J. ,"Improved identity-based signcryption". In Public Key Cryptography (PKC'05), Vaudenay S (ed), LNCS 3386. Springer-Verlag: Les Diablerets, Switzerland, 2005; 362–379.

[29]. PSLM B., Libert B., McCullagh N., JJ. Quisquater JJ., "Efficient and provably-secure identity based signatures and signcryption from bilinear maps". In Advance in Cryptology (ASIACRYPT'05), Roy BK (ed), LNCS 3788. Springer-Verlag: Chennai, India, 2005; 515–532.

[30]. Abdul Wahid, Masahiro Mambo," Implementation of Certificateless Signcryption based on Elliptic Curve Using Java script" (IJCANDI) Vol 1, No 3, August 2016, pp. 90-100.

[31]. Mohammed Hassouna, Nashwa Abbas Farah, Bazara Barry ,and Eihab Bashier Mohammed Bashier , and Eihab Bashier Mohammed Bashier, "An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model",(IJCSI) Vol. 10, Issue 2, No 3, March 2013.

[32]. Zhengjun Cao, Lihua Liu,"On the Disadvantages of Pairing-based Cryptography".

[33]. A K Mohapatra,PhD, Jyoti Kushwaha,and Tanya Popli ,"Enhancing Email Security by Signcryption based on Elliptic Curve" , International Journal of Computer Applications (0975 – 8887) Volume 71– No.17, June 2013.

[34]. Hui-fang YU, Bo YANG,"Low-computation certificateless hybrid signcryption scheme", Yu and Yang / Front Inform Technol Electron Eng 2017 18(7):928-940.

[35]. Malik ZiaID, Rashid Ali ,"Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls", https://doi.org/10.1371/journal.pone.0208857 December 13, 2018 .

[36]. Bo Zhang , Zhongtian Jia, and Chuan Zhao,"An Efficient Certificateless Generalized Signcryption Scheme", https://doi.org/10.1155/2018/3578942, Volume 2018, Article ID 3578942, 11 pages.

[37]. Balasubramanian V and Mala T" Improved Certificateless Signcryption for IoT Smart Devices ", Appl. Math. Inf. Sci. 13, No. 1, 31-38 (2019) .