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 signcryption 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 introduced 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

\[ y^2 = x^3 + ax + b \]  

(1)

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

![Figure 1: Addition: R=P+Q](image)

- **EC point addition:**
  If \( P(x_1, y_1) \) and \( Q(x_2, y_2) \) are two points on an EC and \( P(x_1, y_1) \neq Q(x_2, y_2) \), by drawing line between \( P \) and \( Q \) it will intersect the EC at a third point \( R(x_3,y_3) \). The addition of \( P \) and \( Q \) is reflection of this point about \( x \)-axis. It is calculated using following equations:

\[ x_3 = \lambda^2 - x_1 - x_2 \]  

(2)

\[ y_3 = \lambda(x_1 - x_3) - y_1 \]  

(3)

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

(4)

**EC Discrete Logarithm Problem EC-DLP:**

For a point \( P \) \( \in \) \( E(F_q) \) of order \( n \), where \( E \) is an EC defined over a finite field \( F_q \), and another point \( Q = nP \), the EC-DLP is to find the integer \( k \in \{0, n - 1\} \) such that \( Q = kP \). The integer \( k \) is named the DL of \( Q \) to the base \( P \), denoted \( k = \log_P Q \).

\( Q = kP \) 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... etc) 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.

![Figure 2: Sending secure email](image)

![Figure 3: Receiving secure email](image)
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: \( 4a^2+27b^2 \mod p = 0 \),
- \( F \) : The EC over finite field \( (\gamma^2 = x^3+ax+b \mod p) \)
  where \( x \) and \( y \) both lie in \( [1, 2 \ldots p-1] \).
- \( \infty \) : 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.
- \( E_k(\cdot)/D_k(\cdot) \) : 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.
   \[ P_G=s.G \] (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:
   \[ X_m = x_m.G \] (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:
   \[ Q_m = H(ID_m||X_m) \] (7)
2. Calculate the partial private key:
   \[ D_m = s.Q_m \] (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:
   \[ S_m = x_m.D_m = x_m.s.Q_m \] (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 \( w_y \) is used as the primary secret key.
2. Convert \( w_y \) 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 \( w_y \) insert one byte of the secondary key in the ciphertext.
   To send the primary key \( w_y \) securely to the receiver, EC encryption will be used as following:

   Generate a random number \( z \) and compute:
   \[ Z = z.G \] (11)
   \[ U = z.P_{Bob} \] (12)
   \[ Y = W + U \] (13)
   \[ P_s = [Z, Y] \] 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 \( P_s = [Z, Y] \), Bob compute \( W = Y - (S_{Bob}.Z) = (w_x, w_y) \) (14)
Then convert \( w_y \) 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.
3. \( k_1 \) will be hidden in the ciphertext by using the primary \( w_x \) as follow: \( k_1 = 128 \text{ bit} = 16 \text{ byte} \), 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 \( C = C + k_1 \).

4. Select random number \( v < p \).

5. Compute:
   \[
   R = v \cdot G = (R_x, R_y)
   \]
   \[
   T = \text{Hash} (C_s//R_x)
   \]
   The symbol // means the concatenation.
   \[
   S = (v / S_{Alice} - T) \mod p
   \]
   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:
   \[
   T = \text{Hash} (C_s//R_x)
   \]

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

3. Extract \( k_1 \) from \((C_s)\) where \( C = C_s - k_1 \)

4. Decrypt \((C_s)\) to obtain the message as:
   \[
   M = E_{k_1}(C)
   \]

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.

**Figure 4**: Snapshot of send receive program.

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

**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.

**Figure 8**: Settings menu
5. SECURITY ANALYSIS

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

\[ P_m = S_m \cdot G, \text{ where } S_m \text{ is his/her private key and } G \text{ is the generator of the EC, then if both } S_m \text{ and } G \text{ are given, the public key } P_m \text{ can be easily computed. But given the public key } P_m \text{ and } G, \text{ the computation of the private key } S_m \text{ 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_a 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_a which is protected by the EC-DLP.

The attacker has access to only C, R, S and P_C. To obtain w_a 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} \cdot (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 $(C_s, R, S)$ to the judge who can do the following:

1) Calculate $T = \text{Hash}(C_s // R_s)$.

2) If $P_{Alice} \cdot (T + S) = R$, 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 $k_2$ which is hidden in ciphertext according to the ones positions of the binary sequence of the primary key $w_c$. To obtain $w_c$, he needs to know $W = Y - U = Y - (z \cdot P_{Bob} - S_{Bob} \cdot Z) = (w_c + w_s)$ where W is independent on sender’s primary 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 $P_{Alice} \cdot (T + S) = R$. 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 the proposed system with other existing schemes**

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Mul.</th>
<th>Firewall</th>
<th>Pairing</th>
<th>Public-key system</th>
<th>Public verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme1 in [33]</td>
<td>5</td>
<td>NO</td>
<td>NO</td>
<td>CA</td>
<td>NO</td>
</tr>
<tr>
<td>Scheme2 in [30]</td>
<td>8</td>
<td>NO</td>
<td>YES</td>
<td>CLC</td>
<td>NO</td>
</tr>
<tr>
<td>Scheme3 in [34]</td>
<td>9</td>
<td>NO</td>
<td>NO</td>
<td>CLC</td>
<td>NO</td>
</tr>
<tr>
<td>Scheme4 in [35]</td>
<td>6</td>
<td>YES</td>
<td>NO</td>
<td>CA</td>
<td>YES</td>
</tr>
<tr>
<td>Scheme5 in [36]</td>
<td>8</td>
<td>NO</td>
<td>NO</td>
<td>CLC</td>
<td>NO</td>
</tr>
<tr>
<td>Proposed Scheme</td>
<td>3</td>
<td>YES</td>
<td>NO</td>
<td>CLC</td>
<td>YES</td>
</tr>
</tbody>
</table>

**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
[5]. Aysê 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.


