Convertible multi-authenticated encryption scheme with verifiable based on elliptic curve discrete logarithm problem

Nedal Tahat

Department of Mathematics,
Faculty of Sciences,
Hashemite University,
P.O. 150459, Zarqa 13115, Jordan
Email: nedal@hu.edu.jo

Abstract: The work presents a Convertible Multi-Authenticated Encryption (CMAE) scheme based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). The proposed scheme intended to develop the CMAE scheme to improve performance as compared to the other existing schemes. Most of CMAE scheme are very high at computational overhead and memory usage problem. This scheme desired to reduce time-consuming problem by using Elliptic Curve Cryptography (ECC). In addition, the proposed scheme provides good resistance to the chosen plain-text attacks and which is proven to be secure. As for efficiency, the computation cost of the proposed scheme is smaller than the existing schemes, such as Lu et al.’s scheme.

Keywords: multi-authenticated encryption; elliptic curve discrete logarithm problem; chosen plain-text attacks; encryption.


Biographical notes: Nedal Tahat is currently a Lecturer at the Hashemite University, Jordan, and has taught various undergraduate courses. He received his BSc degree in Mathematics from Yarmouk University, Jordan, in 1994, MS in Mathematics from Al al-Bayt University, Jordan, in 1998 and PhD in Mathematics from Universiti Kebangsaan Malaysia in 2010. His research area is in cryptography, with a focus on both classical and function-based digital signatures. He is now working on developing function-based signatures systems using hybrid mode problems. In addition, his current work is in the field of fixed point theory for mappings.

1 Introduction

A digital signature is a mathematical scheme used for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transition (integrity). Authenticated Encryption (AE) is a block cipher mode of operation which simultaneously provides confidentiality, integrity, and authenticity assurances on the data; decryption is combined in a single step with integrity validation. These attributes are provided under a single and easy-to-use programming interface. An AE scheme allows one signer to generate an authenticated ciphertext such that only a designated recipient has the ability to decrypt the signed message and verify its corresponding signature.

To send a message by a secure approach through a broadcast channel, the authenticated encryption scheme was proposed by Horster et al. (1994) in which only the specific recipient can recover the original message from an authenticated ciphertext signature produced by a signer and verify its integrity. Unfortunately, a later dispute over repudiation occurred because of the loss of public verification. To address this problem, Araki et al. (1998) proposed a convertible limited verifier signature scheme without revealing the designated verifier’s private key or performing the zero-knowledge protocol. Their scheme can be recognised as a new type of AE scheme and called the Convertible Authenticated Encryption (CAE) scheme. Many AE schemes and variation have been proposed in Wu and Hsu (2002), Chien (2003), Zhang and Wang (2005), and Sudha and Bhavani (2014). Wu et al. (2008) elaborated encryption on the merits of the CAE and the multi-signature schemes to propose a Convertible Multi-Authenticated Encryption
(CMAE), in which only the designated recipient can easily derive the original message from the ciphertext that has been produced by a multi-signer and verify its validity. Moreover, the converted ciphertext signature can be released in case of later dispute over repudiation to convince any verifier of the dishonesty of the signing group.

Based on Wu et al.’s (2008) CMAE scheme, Tsai (2009) proposed an improved CMAE scheme with One-Way Hash Function (OWHF). His scheme outperforms Wu et al.’s, one in terms of computational efficiency. Recently, Lu et al.’s (2014) proposed a secure CMAE based on discrete logarithm problem, in which they enhanced the semantics security of the message to overcome the defect in Tasi’s scheme.

The operations associated with the Elliptic Curve Cryptography (ECC) are more efficient than those associated with other cryptosystems, like the RSA and the DSA security solutions. Owing to the fact that the ECC has a smaller key size with other cryptosystems, like the RSA and the DSA security solutions, the ECC is more efficient than those associated with other cryptosystems. Moreover, the motivation to design a new CMAE scheme based on Elliptic Curve Discrete Logarithm Problem (ECDLP). Moreover, the proposed scheme provides the semantic security and it can be used in various cryptographic protocols where the anonymity of the requestor is required.

The rest of this paper is organised as follows. In Section 2, we propose our new CMAE scheme. In Section 3, we analyse the security and performance of the new scheme. Next, we present a small example of our scheme and this can be found in Section 4. Finally, Section 7 concludes the paper.

2 The proposed CMAE scheme

In this section, a CMAE scheme with verifiable based on ECDLP is proposed. The proposed scheme is divided into four phases: initialisation phase, signature encryption phase, message recovery and signature conversion phases; these phases are designed as follows:

2.1 System initialisation phase

For the convenience of describing of the proposed technique, they are defined as the parameters follows:

- \( \oplus \): The bit-wise exclusive or operation.
- \( U_i \): Denote the user.
- Each \( U_i \) has private key \( x_i \in \mathbb{Z}_n^* \) and corresponding public key \( y_i = x_i G \). \( U_i \) is randomly chosen in the signing group determined as the client in advance.

2.2 The signature encryption phase

A chosen message \( M \in E(\mathbb{F}_p) \) is attempted to be sent to the designated recipient \( U_r \) by the signing group. Each \( U_i \in SG \) is performed as follows:

- \( U_i \) selects a random number \( \gamma_i \in \mathbb{Z}_n^* \), to compute the following:
  \[
  \xi_i = \gamma_i G = (\alpha_i, \beta_i), \quad \text{where} \quad c_i = \alpha_i (mod n) \quad (1)
  \]
  \[
  t_i = c_i y_i (mod n) \quad (2)
  \]
  \[
  F_i = (x_i + y_i) y_i (mod n) \quad (3)
  \]
  where \( y_v = x_v G (mod n) \) is the public key of specified recipient \( U_v \) and then broadcasts \( (\xi, t_i, F_i) \) to \( U_j \in SG \setminus U_i \).
- After receiving \( (\xi, t_i, F_i) \) from \( U_j \in SG \setminus U_i \), \( U_i \) computes the following:
  \[
  A = \sum_{U_j \in SG} \xi_j (mod n) \quad (4)
  \]
  \[
  T = \sum_{U_j \in SG} t_j (mod n) \quad (5)
  \]
  \[
  F = \sum_{U_j \in SG} F_j (mod n) \quad (6)
  \]
  \[
  L = (M + A)(mod n) \quad (7)
  \]
  \[
  W = h(L, M, F)(mod n) \quad (8)
  \]
  \[
  \sigma_i = (xW + y_i)(mod n) \quad (9)
  \]
  and then sends \( \sigma_i \) to \( U_j \in SG \setminus U_i \).
- After receiving \( (\xi, \sigma_j) \) from \( U_j \in SG \setminus U_i \), \( U_i \) verifies:
  \[
  \sigma_i G = (Wy_j + \xi_j)(mod n) \quad (10)
  \]
  If equation (10) holds, \( U_i \) executes the next step. Otherwise \( U_i \) requests \( U_j \in SG \setminus U_i \) to resend \( \sigma_i \).
- When all \( (\xi, \sigma_j) \) are collected and verified, the client \( U_k \), who can be any signer in SG, chooses a random number \( d \in \mathbb{Z}_n^* \) and computes:
  \[
  \sigma = \sum_{U_j \in SG} \sigma_j (mod n) \quad (11)
  \]
Convertible multi-authenticated encryption scheme

\begin{align}
C_i &= dG \pmod{n} \\
C_2 &= (L \oplus d_y_i)(\pmod{n})
\end{align}

Then client \( U_h \) sends \( (C_1, C_2, T, \sigma, W) \) to the specific recipient \( U_v \).

2.3 The message recovery phase

Upon receiving \( (C_1, C_2, T, \sigma, W) \) from the client \( U_h \), the designated recipient \( U_v \) performs the following three steps:

- Computes
  \[ F = x_i T \pmod{n} \]
  \[ L = (C_2 \oplus x_i C_i) \pmod{n} \]
- Recover the chosen message \( M \) by computing
  \[ M = L - \sigma G + W \sum_{U_j \in SG} y_j \]
- Verify \( W = h(L, M, F) \) by using the above recovered \( W, M \) and \( F \).

2.4 The signature conversion phase

In case of a later dispute regarding repudiation, \( U_v \) can release the converted multi-signature \( \sigma, W \) for the message \( M \).

With this converted signature, anyone can easily verify:

\[ W = h \left( M + \sigma G - W \sigma G + W \sum_{U_j \in SG} y_j, M, F \right) \]

2.5 Correctness of the proposed scheme

The correctness of the proposed scheme is shown in the following theorems.

Theorem 1: In the signature generation phase, \( U_h \) can verify the individual signature \( (\xi, \sigma_i) \) for \( W \) using equation (10).

Proof: The left-hand side of equation (10) can be rewritten as:
\[ \sigma_i G = (x_i W + y_i) G \pmod{n}, \text{by equation (9)} \]
\[ = (x_i G W + y_i G) \pmod{n} \]
\[ = (Wy_i + \xi_i) \pmod{n}, \text{by equation (11)} \]

Theorem 2: In the message recovery and verification phase, \( U_v \)'s can cooperatively recover \( M \) using equation (16).

Proof: Firstly, the value \( L \) can be recovered using equation (15):
\[ C_2 \oplus x_i C_i = (L \oplus d_y_i) \oplus x_i C_i, \text{by equation (13)} \]
\[ = (L \oplus d_y_i) \oplus x_i dG, \text{by equation (12)} \]
\[ = (L \oplus d_y_i) \oplus dx_i G \]
\[ = L \]

Then, the message \( M \) can be recovered using equation (16).
\[ L - \sigma G + W \sum_{U_j \in SG} y_j \]
\[ = (M + A) - \sigma G + W \sum_{U_j \in SG} y_j G, \text{by equation (7)} \]
\[ = (M + A) - \sum_{U_j \in SG} \sigma G + W \sum_{U_j \in SG} x_j G, \text{by equation (11)} \]
\[ = (M + A) - \sum_{U_j \in SG} \sigma G + W \sum_{U_j \in SG} x_j G \]
\[ = \left( M + \sum_{U_j \in SG} \xi_j \right) - \sum_{U_j \in SG} \left( x_j W + y_j \right) G \]
\[ + W \sum_{U_j \in SG} x_j G, \text{by equations (4), (9)} \]
\[ = \left( M + \sum_{U_j \in SG} \gamma_j G \right) - \sum_{U_j \in SG} \left( x_j W + y_j \right) G \]
\[ + W \sum_{U_j \in SG} x_j G, \text{by equation (1)} \]
\[ = M + \sum_{U_j \in SG} \gamma_j G - W \sum_{U_j \in SG} x_j G - \sum_{U_j \in SG} \gamma_j G + W \sum_{U_j \in SG} x_j G \]
\[ = M \]

3 Security analysis and performance evaluation

Security analysis and computational complexity of the proposed scheme are given below.

3.1 Security analysis

The security of the proposed scheme is based on the well-known cryptographic assumptions which are: solving the ECDLP and the intractability of reversing the OWHF (Diffie and Hellman, 1976). In the following we discuss some possible attacks against the proposed scheme and show that the proposed scheme is secure under the protection of the ECDLP and OWHF assumption.

1 The attacker tries to reveal the secret key \( x_i \) of the signer \( U_i \in SG \) or the secret key \( y_j \) of the designated recipient \( U_v \) from all public information. With the authentication encryption \( (C_1, C_2, T, \sigma, W) \), \( \xi_i \) and \( \sigma_i \), the attacker cannot derive the signer’s secret key \( x_i \) from equation (9), since the equation contains two unknown variables \( x_i \) and \( y_i \) protected under the ECDLP assumption. Similarly, the
attacker cannot reveal verifier’s key $x_v$ from equations (14) and (15), since $x_v$ is protected under the ECDLP assumption.

2 The attacker tries to forge an authenticated encryption signature.

To forge a signature for satisfying equation (16), the attacker must know all random $y'_i$, $s$ and $U'_i$'s private key $x_i$. However, this attack is not worked since all $y'_i$, $s$ and $x_i$ are protected under the ECDLP assumption, and the attacker cannot get them, because $x_i$ and $y'_i$ are only hold by the signer’s $U_i \in SG$. Thus, it is impossible for any attacker to forge the digital multi-signature of the message $M$.

3 The attacker tries to forge a converted signature by three methods:

a. to keep the chosen message $M$ secret, the converted signature

$$\left( \sum_{U'_i \in SG} x_i h(L, M, F) + y'_i \right) \pmod{n}, W$$

is able to protect the secret message using signer’s two parameters, $\xi$ and $y'_i$, such that it is impossible for any attacker to obtain the chosen message $M$ from $\sigma$. As for the signature $W$, it is computationally infeasible to drive the original message $M$ from $h(L, M, F)$ due to the difficulty of reserving an OWHF. After all, it is impossible to derive the chosen message from the signature.

b. An attacker cannot derive the transmitted message $L$ from $(C_1, C_2)$ since it is based on ECDLP. Thus, the attacker can’t recover the message by equation (16).

c. If an attacker tries to break the indistinguishability for two candidate messages $(M_1, M_2)$, he must check an ordinary signature converted from the signature:

$$W = h \left( M_1 + \sigma - \sum_{U'_i \in SG} y'_i, M_1, x, T \right)$$

or

$$W = h \left( M_2 + \sigma - \sum_{U'_i \in SG} y'_i, M_2, x, T \right)$$

In general,

$$W = h \left( M + \sigma - \sum_{U'_i \in SG} y'_i, M, F \right)$$

and

$$\sigma = H(L, M, F) + \sum_{U'_i \in SG} \xi_i \pmod{n}$$

which lead to:

$$W = h \left( M_1 + \sigma - \sum_{U'_i \in SG} y'_i, M_1, x, T \right)$$

or

$$W = h \left( M_2 + \sigma - \sum_{U'_i \in SG} y'_i, M_2, x, T \right)$$

and each signer’s public key $y_i$ has no idea about the specific recipient’s private key $x_i$ and individual private key $x_i$ plus random number $y'_i$. Hence, it is infeasible to output the original message $M$ such that the proposed scheme can satisfy the indistinguishability of the confidentiality.

4 In order to protect the interests of designated recipient, the proposed scheme sets a message conversion phase to ensure that anyone can verify the validity of the converted ciphertext signature and message in case that the signing group repudiates on it. Furthermore, the converted verification equation provides an adversary with no chance of setting up the chosen plain-text attacks such that the proposed scheme can satisfy the non-repudiation.

3.2 Performance evaluation

This section discusses the computational complexity performance of the proposed CMAE scheme. For facilitating the computational complexity, the following notations are defined (Nehru and Shanmugam, 2014; Contini et al., 2006):

- $T_{\text{mul}}$: Time complexity for executing the modular multiplication,
- $T_{\text{exp}}$: Time complexity for executing the modular exponentiation,
- $T_{\text{add}}$: Time complexity for executing the modular addition,
- $T_{\text{ec-mul}}$: Time complexity for executing the elliptic curve multiplication,
- $T_{\text{ec-add}}$: Time complexity for executing the elliptic curve addition,
- $T_h$: Time complexity for executing the hash function.
Convertible multi-authenticated encryption scheme

Table 1  The comparison among our scheme and Lu et al.’s scheme

<table>
<thead>
<tr>
<th>Phases</th>
<th>The proposed scheme</th>
<th>Lu et al.’s scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature encryption phase</td>
<td>Time complexity: $\left(\frac{n+2}{2}\right)T_{enc-add}$</td>
<td>$\left(\frac{n^2+3n-1}{2}\right)T_{enc-add} + nT_r$</td>
</tr>
<tr>
<td></td>
<td>$+(3n+2)T_{enc-add} + nT_b$</td>
<td>$n^2 + 725n - 1)T_{enc-add}$</td>
</tr>
<tr>
<td></td>
<td>Complexity in $T_{mul}$</td>
<td>$\left(\frac{n^2+725n}{2}\right)T_{enc-add}$</td>
</tr>
<tr>
<td>Message recovery and verification phase</td>
<td>Time complexity: $(n+2)T_{enc-add} + 4T_{enc-msg} + T_k$</td>
<td>$(n+1)T_{enc-add} + T_{msg} + 3T_{exp} + T_h$</td>
</tr>
<tr>
<td></td>
<td>Complexity in $T_{mul}$</td>
<td>$\left(\frac{n^2+730n}{2}\right)T_{enc-add}$</td>
</tr>
<tr>
<td>Signature conversion phase</td>
<td>Time complexity: 0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Complexity in $T_{mul}$</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>Time complexity: $(4n+4)T_{enc-add}$</td>
<td>$(n^2 +2n)T_{enc-add} + (3n + 3)T_{exp}$</td>
</tr>
<tr>
<td></td>
<td>$+(5n+6)T_{enc-msg} + (n+1)T_k$</td>
<td>$(n+1)T_k$</td>
</tr>
<tr>
<td></td>
<td>Complexity in $T_{mul}$</td>
<td>$\left(\frac{n^2+733n}{2}\right)T_{enc-add}$</td>
</tr>
</tbody>
</table>

The equivalence of the time complexity for various operation units in terms of $T_{mul}$ is given in Table 2 according to what is given in Koblitz et al. (2002), Tahat et al. (2008), Servos et al. (2013), and Henock et al. (2015).

Table 2  Time complexity for various operation units in terms of $T_{mul}$

<table>
<thead>
<tr>
<th>$T_{exp}$</th>
<th>$T_{enc-add}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\approx 240T_{mul}$</td>
<td>$\approx 10T_{mul}$</td>
</tr>
<tr>
<td>$\approx 47T_{mul}$</td>
<td>$\approx 0.12T_{mul}$</td>
</tr>
</tbody>
</table>

4 Numerical simulation

Assume that $p = 1091, n = 1051$, $x^3 = (x^3 - 3x + 33)(\text{mod}1091)$ $G = (299, 62)$ is a base with order $n$.

We will apply our example on three users signing group; each user choose $x_1 = 203, x_2 = 164, x_3 = 373 \in Z_n^*$ and compute:

$y_1 = 203G = (380, 720)$
$y_2 = 164G = (492, 661)$
$y_3 = 373G = (260, 426)$

4.1 Signature encryption phase

A chosen message $M = 3G = (538, 815) \in E(\mathbb{F}_p)$ is attempted to be sent to the designated recipient $U_v$ by the signing group. Each $U_i \in S G$ is performed as follows:

- $U_i$ selects a random number $y_i = 183, y_2 = 261, y_3 = 323 \in Z_n^*$, to compute the following:
  - $z_i = 183G = (337, 847)$, $z_2 = 261G = (250, 997)$,
  - $z_3 = 323G = (23, 292)$
  - $c_1 = 337(\text{mod}1051), c_2 = 250(\text{mod}1051), c_3 = 23(\text{mod}1051)$
  - $t_1 = 337y_1 = 9G, t_2 = 250y_2 = 11G$ and
  - $t_3 = 23y_3 = 171G$
  - $F_1 = (203+183)236G = 710G$,
  - $F_2 = (164+261)236G = 455G$
  - $F_3 = (373+323)236G = 300G$

where $y_v = x_iG(\text{mod}1051) = 236G$ is the public key of the specified recipient $U_v$ and then broadcasts $(z_i, t_i, F_i)$ to $U_j \in SG \setminus U_i$.

- After receiving $(z_i, t_i, F_i)$ from $U_j \in SG \setminus U_i$, $U_i$ computes the following:
If equation (10) holds, \( \sigma \) verifies:

\[
\begin{align*}
W &= h(L, M, F) = 543 \\
\sigma_i &= (203 \times 543 + 183)(mod1051) = 57(mod1051) \\
\sigma_j &= (164 \times 543 + 261)(mod1051) = 1029(mod1051) \\
\sigma_k &= (203 \times 543 + 183)(mod1051) = 19(mod1051)
\end{align*}
\]

and then sends \( \sigma_i \) to \( U_j \in SG \setminus U_i \).

After receiving \( (\tilde{\xi}_j, \sigma_j) \) from \( U_j \in SG \setminus U_i, U_i \) verifies:

\[
\begin{align*}
\sigma_j G &= (57G) = (W_{y_1} + \xi_i)(mod1051) \\
57G &= (543 \times 203G + 183G)(mod1051) = 54G \\
\sigma_j G &= (W_{y_2} + \xi_j)(mod1051) \\
1029G &= (543 \times 1064G + 261G)(mod1051) = 1029G \\
\sigma_j G &= (W_{y_1} + \xi_j)(mod1051) \\
19G &= (543 \times 373G + 323G)(mod1051) = 19G
\end{align*}
\]

If equation (10) holds, \( U_i \) executes the next step. Otherwise \( U_i \) requests \( U_j \in SG \setminus U_i \) to resend \( \sigma_j \). When all \( (\tilde{\xi}_j, \sigma_j) \) are collected and verified, the client \( U_i \) can be any signer in SG, chooses a random number \( 359 \in \mathbb{Z}_n \), and computes:

\[
\begin{align*}
\sigma &= (57 + 1029 + 19)G \mod(1051) = 45G \\
C_1 &= 359G \\
C_2 &= (800G + 359 \times 236G) \mod(1051) = 371G
\end{align*}
\]

Then client \( U_k \) sends \( (C_1, C_2, T, \sigma, W) \) to the specific recipient \( U_r \).

### 4.2 The message recovery phase

Upon receiving \( (C_1, C_2, T, \sigma, W) \) from the client \( U_i \), the designated recipient \( U_r \) performs the following three steps:

- Computes
  \[
  \begin{align*}
  F &= 236 \times 278G \mod(1051) = 446G \\
  L &= (371G + 236 \times 359G) \mod(1051) = 1015G
  \end{align*}
  \]

- Recover the chosen message \( M \) by computing
  \[
  \begin{align*}
  M &= (800G - 54G + 543(203 + 164 + 373)) \\
  G \mod(1051) &= 33G = M
  \end{align*}
  \]

- Verify \( W = h(L, M, F) = 543 \) by using the above recovered \( W, M \) and \( F \).

### 5 Conclusion

This paper suggested a secure and efficient CMAE scheme based on ECDLP. The schemes utilise the inherent advantage of elliptic curve cryptosystems in terms of smaller key size and lower computational overhead compared to its counterpart public key cryptosystems such as RSA and ElGamal so the proposed scheme outperforms Lu et al.’s scheme in all the aspects of the computation complexities, also the time complexity is lower than the existing CMAE. Furthermore, the proposed scheme is resistant against the chosen plain-text attacks for an adversary breaking the indistinguishability of confidentiality. Any adversary cannot derive the correct message from the candidate message.

### References


