# CHAPTER 4

# PROPOSED SCHEME : MODIFIED ELLIPTIC CURVE SIGNCRYPTION

## 4.1. Introduction

As discussed in the previous chapter Zheng's Signcryption Scheme, is a cryptographic primitive which combines signature and encryption in a logically single step based on DLP [17,18]. Zheng's scheme succeeded to achieve the unforgeability, integrity and confidentiality of message but lacked forward security, public verifiability.

In 1998, Zheng and Iami proposed another signcryption scheme [19] based on ECDLP that achieved similar functionality but also it lacked forward security and public variability. Bao and Deng Proposed another modified signcryption scheme [21] that enabled a third party have $(m, r, s)$ to verify the signature without need to the recipient's private key or engaging a zero – knowledge interactive protocol . But this modified scheme also lacked forward security and public verifiability or encrypted message authentication. Gamage, Leiwo and Zheng proposed a scheme [22] that enabled encrypted message authenticated but also lacked to the forward security. Han and Hang [23,24], Hwang, Lai and Su proposed two schemes [25] depended on DHP but also they lacked the forward security and public verifiability plus to, the DHP scheme could be attacked.

This chapter introduces a new proposed scheme " *Modified Elliptic Curve Signcryption* " based on ECDLP and in addition to achieve the functionality of the signcryption schemes, *unforgeability*, *confidentiality, integrity* and *non – repudiation* it achieves *forward security and encrypted message authentication or public verifiability* which enable the third party to verify the signature or authenticate the encrypted message without need to recipient's private key or decrypt the message so this property can be used in the firewalls on the computer networks to forward the encrypted messages from certain users without decrypt them. Also, using a strong session key encryption depends on using a random chosen value plus to the private key of the sender and it is used to encrypt the message twice to increase the confidentiality and integrity of the message.

The proposed scheme is depending on using ECDSS followed by ElGamal encryption algorithm. It is slower than the Zheng's signcryption scheme but achieves saving in communication overhead reach to 50% with respect to the traditional approach signature – then – encryption and higher than Zheng saving which is 40%.

## 4.2. Proposed Scheme

The proposed scheme based on ECDLP and employs a strong session key encryption . The encryption key depends on a random chosen value $v\ \varepsilon_R\ [1, .., q-1]$ but also depends on Alice's private key $v_a$. The proposed scheme is described in the following three stages *key generation, signcryption* and *unsigncryption*.

## Key generation

Using the same EC parameters and the same keys for Alice and Bob of Zheng's signcryption scheme ( mentioned in chapter 3, table 3.7).

## Signcryption

When Alice needed to send a message to Bob, Alice generates the signcrypted text by following the below steps:

1. Alice picks a random value $v\ \varepsilon_R\ [1, \ldots., q-1]$
2. Compute $R = (vG) = (x_R, y_R)$
3. Compute session key encryption $k = (v + x_R.v_a)P_b = (x_k, y_k)$
4. Implement the message as a point on elliptic curve M ( see Appendix A)
5. Encrypt the message ( point M ) twice using $k$ as $c = E_{y_k}[E_{x_k}(M)]$
6. Compute $r = hash\ (c, x_R)$
7. Compute $s = (v_a.r\ - v)\ mod\ q$

Alice sends $c, r, s$ to Bob

*At Alice:*

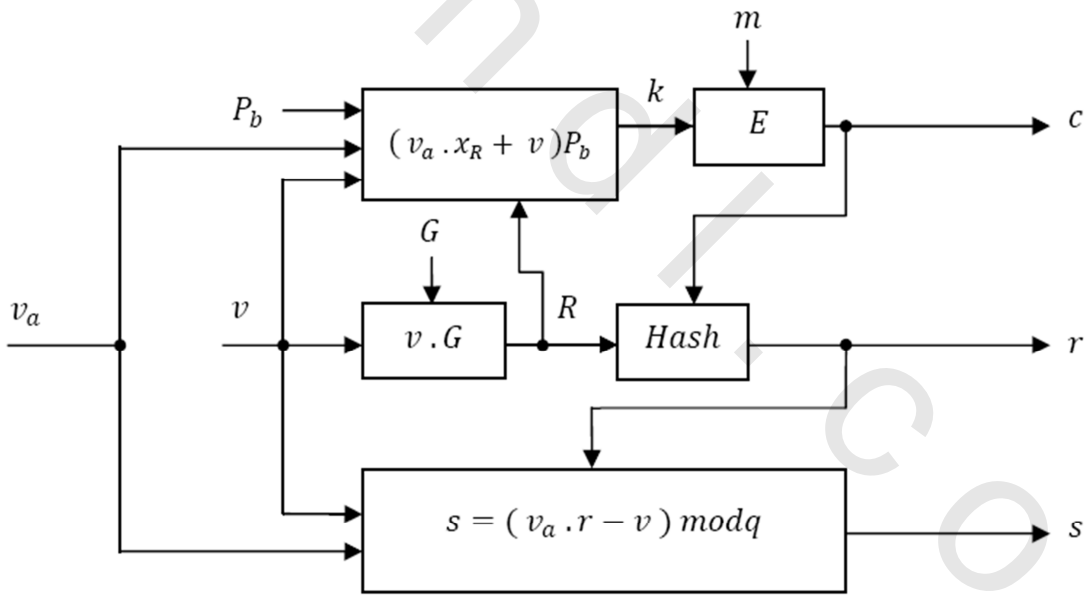


**Figure 4.1. Modified Elliptic Curve Signcryption Block Diagram**

Unsigncryption

When Bob receives the message first verify the signature to check the message came from Alice or not, if not he will reject the message.

1. Compute $R = rP_a - sG = (x_R, y_R)$
2. Compute $r' = hash\ (c, x_R)$

   if $\begin{cases} r' = r & \text{Accept } c \text{ and complete decryption process} \\ r' \neq r & \text{Reject } c \end{cases}$

3. Compute $k = v_b(R + x_R P_a) = (x_k, y_k)$
4. Decrypt the message $M = D_{y_k}[D_{x_k}(c)]$

*At Bob:*

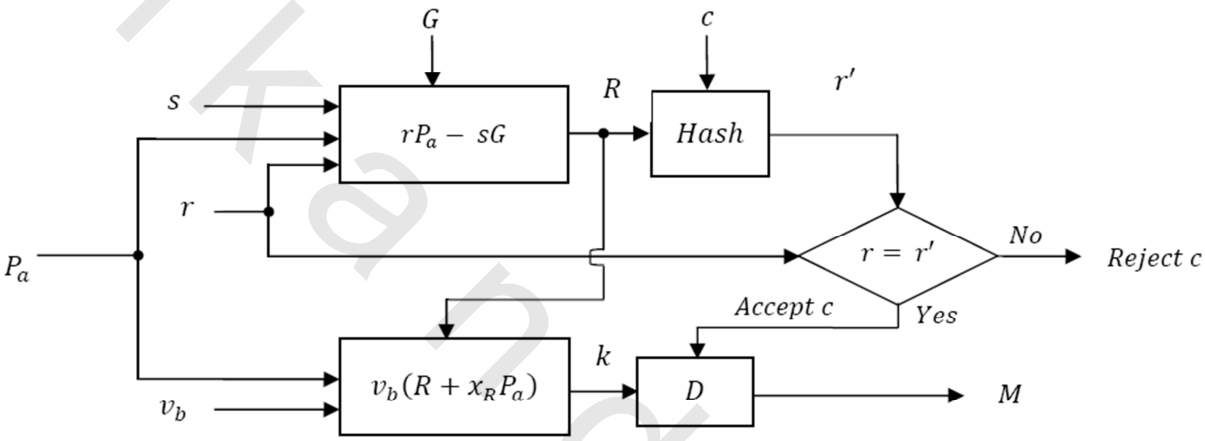


**Figure 4.2. Modified Elliptic Curve Unsigncryption Block Diagram**

## 4.2.1. System Analysis

To prove $R$

*Proof:* $R = rP_a - sG$

$= rP_a - (v_a.r - v)G$

$= rP_a - v_a.rG + vG$

$= vG$

To prove the session key encryption

*Proof:* $k = v_b(R + x_R P_a)$

$= v_b(vG + x_R.v_a G)$

$= v_b G(v + x_R.v_a)$

$= P_b(v + x_R.v_a)$

## 4.2.2. Security Analysis

The session key encryption establishment part of the proposed scheme has the following security attributes:

1. **Known session key security :** Each message is signcrypted with a unique session key since random value $v$ is used for session key establishment. The session key will also differ for different recipients since their public keys are involved in key derivation function [26].
2. **Resilience to Key Compromise Impersonation (KCI) attack :** Under intractability of ECDLP, the KCI attack [26] is thwarted in the proposed scheme. An adversary that could obtain $v_a$ should find the corresponding $v$ of $R$ in order to deduce the corresponding session key that is generally in deposit of solving the ECDLP.
3. **Partial Forward secrecy :** Session key derivation function of the proposed scheme provides partial forward secrecy since even if $v_a$ is revealed, finding the corresponding random number $v$ is still necessary that is generally in deposit of solving the ECDLP [26].

The security attributes of the proposed scheme are described as follows.

1. **Confidentiality :** Confidentiality is achieved by encryption. To decrypt the ciphertext, an adversary needs to have Bob's private key $v_b$ or have Alice's private key $v_a$ and the random value $v$ that in deposit of solving ECDLP to $R$.
2. **Unforgeability :** It is computationally infeasible to forge a valid signcrypted text $(c, r, s)$ and claim that it is coming from Alice without having Alice's private key $v_a$ .
3. **Integrity :** It is computationally infeasible where the integrity is guaranteed by security attributes and Confidentiality of the signcryption. So an adversary should also have the valid session key to decrypt the message and add his modifications.
4. **Non-repudiation :** If the sender Alice denies that she sent the signcrypted text $(c, r, s)$, any third party can run the verification procedure to check that the message came from Alice.
5. **Public verifiability :** Verification requires knowing only Alice's public key. All public keys are assumed to be available to all system users through a certification authority or a public directly. The receiver of the message does not need to engage in a zero-knowledge proof communication with a judge or to provide to prove [27].
6. **Forward secrecy :** An adversary that obtains $v_a$ will not be able to decrypt past messages [27]. Previously recorded values of $(c, r, s)$ that were obtained before the compromise cannot be decrypted because the adversary that has $v_a$ will need to $v$ to decrypt.

**Table 4.1. Comparison between Provided Attributes of Different Signcryption Schemes**

| Signcryption Schemes \ Attributes | Unforgeability | Confidentiality | Integrity | Non-repudiation | Direct Public Verifiability | Forward Secrecy |
|---|---|---|---|---|---|---|
| **Zheng and Imai [19]** | Yes | Yes | Yes | Using another protocol | No | No |
| **Bao and Deng [21]** | Yes | Yes | Yes | Directly | No | No |
| **Gamage - leiwo and Zheng [22]** | Yes | Yes | Yes | Directly | Yes | No |
| **Han, Yang and Hu [23]** | No | No | No | Directly | No | No |
| **Hwang, Lai and Su [25]** | No | No | No | Directly | No | No |
| **Proposed Scheme** | Yes | Yes | Yes | Directly | Yes | Yes |

### 4.2.3. Saving in Communication overhead

Communication overhead represents any associated data to the ciphertext, is used to recover the message of verify the signature (e.g. point 4). Communication overhead calculations are based on the following assumptions:

1. $|hash(.)| = |KH(.)| = |q|/2$ .
2. $|q| \approx |p^h|$ .
3. Elliptic curve digital signature standard outputs $(r, s)$ representing 2 points so its comm. overhead is $2|q|$ .
4. ElGamal elliptic curve encryption outputs 2 points on the curve ($c_1$ ciphertext, $c_2$ is called DHP to recover message ) [1,8]. So its communication overhead is $|q|$.

The communication overhead of the traditional approach signature – then – encryption, using ECDSS followed by ElGamal elliptic curve encryption is $2|q| + |q| = 3|q|$ . The communication overhead of the proposed scheme represented in $(r, s)$ is $|hash(.)| + |q| = |q|/2 + |q| = 1.5|q|$ . Thus, bandwidth saving can be calculated as:

$$\text{Saving} = \frac{3|q| - 1.5|q|}{3|q|} = 50\%$$

This saving is higher than the calculated one in Zheng- Imai, which is 40%.

*Note*: refer. [28] saving in communication overhead equation is not correct because he assumed that the communication overhead of ElGamal elliptic curve encryption is $2|q|$ depending on ElGamal elliptic curve encryption outputs 2 points on the curve $(c_1, c_2)$, considered 2 points as overhead. But the communication overhead of ElGamal elliptic curve encryption is one $|q|$. Then the correct equation of bandwidth saving is

$$\text{Saving} = \frac{2.5|q| - 2|q|}{2.5|q|} = 20\ \%$$

Then the correct saving in comm. overhead is 20% not 43% as he mentioned. So, his proposed scheme "*Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy*" achieved public variability and forward security but with saving in communication overhead and computational costs lower than the traditional approach and higher than Zheng's signcryption scheme.

### 4.2.4. Saving in Computational Cost

The computational cost of the proposed scheme can be easily compared with those of other signcryption schemes presented in table 4.3, by calculating total required number of operations, as shows that the proposed scheme is slower than Zheng and Imai signcryption scheme, But it provides the highest number of security attributes, as it is described in table 4.2.

**Table 4.2. Comparison between Required Operations for Different Signcryption Schemes**

| Operation / Signcryption Schemes | Participant | EXP | DIV | ECPM | ECPA | MUL | ADD | HASH |
|---|---|---|---|---|---|---|---|---|
| **ECDSS Signature – ELGamal Encryption** | Alice | – | 1 | 3 | 1 | 1 | 1 | 1 |
| | Bob | – | 1 | 3 | 2 | – | – | 1 |
| **Zheng and Imai [19]** | Alice | – | 1 | 1 | – | 1 | 1 | 2 |
| | Bob | – | – | 2 | 1 | 2 | – | 2 |
| **Bao and Deng [21]** | Alice | 2 | 1 | – | – | – | 1 | 3 |
| | Bob | 3 | – | – | – | 1 | – | 3 |
| **Gamage - leiwo and Zheng [22]** | Alice | 2 | 1 | – | – | – | 1 | 2 |
| | Bob | 3 | – | – | – | 1 | – | 2 |
| **Han, Yang and Hu [23]** | Alice | – | 1 | 2 | – | 2 | 1 | 2 |
| | Bob | – | 1 | 3 | 1 | 2 | – | 2 |
| **Hwang, Lai and Su [25]** | Alice | – | – | 2 | – | 1 | 1 | 1 |
| | Bob | – | – | 3 | 1 | – | – | 1 |
| **The proposed scheme** | Alice | – | – | 2 | – | 2 | 2 | 1 |
| | Bob | – | – | 4 | 2 | – | – | 1 |

Where

EXP : Modular Exponentiation
DIV : Modular Division/inverse
ECPM : Elliptic Curve Point Multiplication
ECPA : Elliptic Curve Point Addition
MUL : Modular Multiplication
ADD : Modular Addition
HASH : One-way Hash function

## 4.3. Conclusions

The proposed scheme achieves the functionality of signcryption schemes, in addition to achieve forward security and public variability or authenticated encrypted message which employed in the firewalls on computer networks to filter network traffics. Also, using a strong session key encryption depends on using a random chosen value plus to the private key of the sender and it is used to encrypt the message twice to increase the confidentiality and integrity of the message.

Although, the proposed scheme is slower than Zheng's signcryption scheme it achieves saving in communication overhead reach to 50 % higher than Zheng's scheme saving which is 40% and achieves security attributes higher than Zheng's scheme and the others modified signcryption schemes.