J. Appl. Environ. Biol. Sci., 6(5S)28-33, 2016

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

An Efficient Multi Receiver Signcryption with Forward Secrecy Based on Elliptic Curves

Nizamuddin[1], Arif Iqbal Umar[2], Abdul Waheed[2], Noor Ul Amin[2]

[1]Iqra National University Peshawar
[2]Department of Information Technology, Hazara University Mansehra, Pakistan

Received: February 3, 2016
Accepted: April 12, 2016

ABSTRACT

Multi receiver signcryption scheme achive the task digital signature and multi receiver encryption functions, cost effectively. We present a novel multi receiver signcryption having forward secrecy using elliptic curves in the public key infrastructure, ensures: message confidentiality, sender authenticity, message integrity, sender unforgeability, sender non-repudiation, sender private key forward secrecy and message public verification. Its low computation cost and communication overhead could make this construction a better option for use in resource constrained secure Multicast communication.
KEYWORDS:Cryptography;Signcryption; Forward Secrecy; Multicast

1. INTRODUCTION

Multicasting [1] is promising enabling technology for Next Generation Networks (NGN) to support several groups of users with flexible quality of service (QoS) requirements [2].

Forward secrecy coined by [3] is the security property that: if long-term keys compromised should not result in compromise of session keys. It is one of the important security properties for key agreement, confidentiality and implicit authentication [4].

Kurosawa [5] proposed first multi-recipient encryption scheme (MRES). Bellare et al. [4, 5] systematically studied the technique of randomness reuse and provided several generic and efficient constructions for MRES.

Since the first signcryption presented by Zheng [4] a set of Multi Receiver signcryption schemes [8, 9, 11, 12, 13, 14, 15, 16] and signcryption schemes with forward secrecy [17, 18, 19, 20, 21, 22] were proposed in the Public Key Infrastructure.

Existing schemes either lack multi receiver functionality or Forward Secrecy. Second the scheme proposed in [10] is based on expensive DLP which requires modular exponentiation as compare ECDLP.

We proposed an efficient Multi Receiver Signcryption with forward secrecy on elliptic curves. The detailed security analysis is presented and proved that our scheme ensures message confidentiality, sender authenticity, message integrity, signer unforgeability, sender non-repudiation, forward secrecy and message public verifiability. It is computational and communication efficient than existing multi receiver signcryption schemes.

2. Preliminaries

This section, briefly describe the basic notation, and definitions that will be used throughout the paper.

Let $q \geq 2^{160}$ be large prime number $\mathrm{F_q}$ is a finite field of order q.

An Elliptic Curve $E(F_q)$ over F_q be defined by an equation of the form:

$$E: y^2 = (x^3 + ax + b) \bmod q$$
$$(4a^3 + 27b^2) \bmod q \neq 0$$

A base point G on E with order $n \geq 2^{160}$, symmetric cipher(E_k) with secret key(k), message (m), session key(v), ciphertext(c) and encrypted session key(c_i), number of group member (t) and symmetric cipher (D_k) with session key (k) is used to decrypt.

Definition 1: ECDLP.

Let G and Q be two given points of an EC E, Find an integer k, such that $Q = k.G \bmod n$.

Corresponding Author: Nizamuddin, Iqra National University Peshawar, Pakistan. sahibzadanizam@yahoo.com

Definition 2: ECDLP Assumption.
Let k is an integer, P and Q be two given points of an EC E, such that $Q = k.P \bmod n$.
Finding an integer k is hard for sufficient large value of q and n.

3. Proposed Multi Receiver Signcryption Scheme

Proposed multi receiver signcryption scheme with forward secrecy consists of four phases: Setup, Key Generation, Multi Receiver Signcryption and Unsigncryption.

3.1. Setup

In this phase the common security parameters defined in preliminary section are published in group members.

3.2. Key Generation

In this phase each member of the multicast group randomly selects an integer $d_i \in \{1, 2, \dots, n-1\}$ as his private key and computes public key P_i as $P_i = d_i.G$ where $i \in \{1, 2, \dots, t\}$.
Each member get certificates from authority and distribute in the group.

3.3. Multi Receiver Signcryption

To securely multicast a message to a group of receivers, the sender should run probabilistic polynomial-time algorithm *Multi Receiver Signcrypt*. It takes inputs: security parameters, message m, the sender's private keys d_s and receiver's public keys $\{P_1, P_2, \dots, P_t\}$, and returns a signcrypted text (c, ω, s, R).

Multi Receiver Signcrypt $(m, d_s, P_1, P_2, \dots, P_t)$

1. Verifies each receiver public key d_i by using their certificates.
2. Randomly selects an integer $v \in \{0, 1, \dots, n-1\}$ as message-encryption key
3. Compute $r = h(m)$
4. Generate ciphertext c as $c = E_v(m)$
5. Randomly selects an integer $k \in_R \{0, 1, \dots, n-1\}$
6. Computes the encrypted session keys c_i for each recipient
    a. Computes $K_i = k.P_i$
    b. Computes $S_k = h(K_i)$
    c. Computes c_i as $c_i = E_{S_k}(v)$
    d. Generate $\omega = \{c_1, c_2, \dots, c_t\}$
7. Computes $s = (d_s + r.k) \bmod n$
8. Computes $R = k.G$

    Multicast the Signcrypted text (c, ω, s, R)

3.4. Unsigncryption Phase

In the Unsigncryption phase, each receiver in the multicast group having identity ID_i select his relevant information (c, c_i, R, s) from multicast signcrypted text (c, ω, s, R) according to his position, gets the message and verify using deterministic polynomial-time *Unsigncryption* algorithm.

Unsigncryption $(c, c_i, R, s, P_s, d_{ri})$

1. Verifies sender public key $P_s$by using his certificate.
2. Computes $K_i = d_{ri}.R$
3. Computes $S_k = h(K_i)$
4. Generate $v = D_{S_k}(c_i)$
5. Generate message m as $m = E_v(c)$
6. Compute $r = h(m)$
7. Verifies $(s.G - r.R) = P_s$ If true then accept m else reject

---

Theorem 1: Multi Receiver Signcryption and Unsigncryption are considered to be valid if sender and receiver conform to the equation: $d_{ri}.R = k.P_i$

Proof :

$d_{ri}.R = d_{ri}.k.G$
$= k.d_{ri}.G$
$= k.P_i$

Clearly, the equation $d_{ri}.R = k.P_i$ is established.

4. Security Analysis

The proposed scheme provides seven securities attribute as: multicast message confidentiality, sender authentication, multicast message integrity, multicast message unforgeability, sender non-repudiation, forward secrecy and multicast message public verifiability. The proofs are based on the will known assumptions defined: that ECDLP and ECDHP are hard [10] and hash function is collision resistive and one way properties. The security attributes of the proposed scheme is compared with existing schemes in *Table 1.*

4.1. **Confidentiality**

In our scheme, if the attacker need to derive the original message, he must obtained K_{ei}. There are three scenarios that the attacker can try to compute K_{ei}. However, the possible ways to generate K_{ei} is equivalent to solve the ECDLP.

Case 1: An attacker can compute S_k from equation (3) and K_i from equation (2) if he computes d_{ri} from equation (1). The attacker gets P_{ri} easily but if tries to generate d_{ri} from equation (2), and then he has to solve ECDLP.

$$P_{ri} = d_{ri}.G \qquad (1)$$
$$K_i = d_{ri}.R \qquad (2)$$
$$S_k = h(K_i) \qquad (3)$$

Case 2: An attacker can compute S_k from equation (6) and K_i from equation (5) if he computes k from equation (4). The attacker gets R easily, but if tries to generate k from equation (4), and then he has to solve ECDLP.

$$R = k.G \qquad (4)$$
$$K_i = k.P_i \qquad (5)$$
$$S_k = h(K_i) \qquad (6)$$

Case 3: An attacker can compute S_k from equation (9) and K_i from equation (8) if he gets d_{ri} from equation (7). The attacker gets P_{ri} easily but if he tries to generate d_{ri} from equation (7), then he has to solve ECDLP.

$$P_{ri} = d_{ri}.G \qquad (7)$$
$$K_i = d_{ri}.R \qquad (8)$$
$$S_k = h(K_i) \qquad (9)$$

4.2. **Integrity**

Recipient can insure taht received message is origenl using equation (10) and equation (11). If an attacker changes $c \ as \ c'$ the message is changed to m' such that $m \neq m'$ and $r' \neq r$. It is computationally infeasible for an attacker to modify c as c' such that $r' = r$ by the collision resistant property of h. This insure that if the c altered, the recipient can detect.

$$r = h(m) \qquad (10)$$
$$s.G - r.R = P_s \qquad (11)$$

4.3. **Unforgeability**

The attacker/ recipient cannot can't forge valid (m, s, R) without $d_s \, and \, k$. Assume that the attacker/recipient wants to forge a valid (m', s', R') from a previous one, he/she eavesdropped/received. He must generate s' from equation (14) For the message m' . But to compute s', attacker must compute d_s from equation (12) and k from equation (13) that is equivalent to solve two ECDLP, and receiver should compute k from equation (13) that is equivalent to solve one ECDLP. Therefore, our proposed scheme is unforgeable.

$$P_s = d_s.G \qquad (12)$$
$$R = k.G \qquad (13)$$
$$s' = (d_s + r.k) mod \, n \qquad (14)$$

4.4. **Authentication:**

The sender public key P_s is associated to his private key d_s and authenticated by its certificate. Only legitimate sender can generate valid signature s as proved in *Section 4.6*. Each receiver can verify the authenticity of the message received by using equation (15).

$$(s.G - r.R) = P_s \qquad (15)$$

4.5. **Non-repudiation**

The sender public key P_s is linked with private key d_s. The recipients / judge can use P_s certificate to authenticate the validity of the sender. In case of dispute the judge can settle it using the steps in ***Section 4.6***, without obtaing d_s.

4.6. **Judge Verification Phase**
In case of dispute the judge/ third party can decide that original sender sent m to the recipients. Any one of the receiver only provides (m, s, R) to judge. They decides obut the originator of the message, by using deterministic polynomial time algorithm *Judge Verify*.

Judge Verify (m, s, R)

1. Verifies sender's public key P_s
2. Computes $r = h(m)$
3. Computes $s.G - r.R$
4. The message is sent by original sender if
   $s.G - r.R = P_s$

Theorem 2: Receiver and Judge Verification Phase is considered valid if sender and receiver/judge conform to the equation: $s.G - r.R = P_s$
Proof:

$$s.G - r.R$$
$$= (d_s + r.k).G - r.R = P_s + r.k.G - r.R$$
$$= P_s + r.R - r.R$$
$$= P_s$$

Clearly, the equation $u.(P_s + R) = k.P_i$ is established.

4.7. **Forward secrecy**
If the sender's long-term private key d_s compromised, the attacker still cannot recover any previous message m from Signcrypted text (c, ω, s, R) . Let an attacker gets the sender private key $\mathrm{d_s}$, he can compute k from equation (16) if he computes r from equation (17). But he cannot derive the correct r without knowing original message m because the hash function is one-way and collision resistant

$$r = h(m) \qquad (17)$$
$$k = (r + d_s)^{-1} s \qquad (16)$$

Table 1: Comparative security analysis of our proposed schemes with existing schemes

Schemes	Security Features							Multi Receiver
	Confidentiality	Integrity	Authenticity	Unforgeability	Non Repudiation	Direct Public Verifiability	Forward Secrecy	
Proposed	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
[6]	Y	Y	Y	Y	Y	N	N	Y
[11]	Y	Y	Y	Y	Y	N	N	Y
[12]	Y	Y	Y	Y	Y	Y	N	Y
[13]	Y	Y	Y	Y	Y	N	N	Y
[14]	Y	Y	Y	Y	Y	N	Y	N
[15]	Y	Y	Y	Y	Y	Y	Y	N

5. Efficiency

The efficiency of public key cryptographic scheme can be measured on the base of computational cost of the major expensive operation Modular Exponentiation (M-Exp) and Elliptic Curve Point Scalar Multiplication (ECPM) and communication overhead on the base of *Extra bits appended* for security functions.

5.1. **Computation Cost**
The computational efficiency of proposed scheme is analyzed and compared with existing schemes on the base of major operations as shown in *Table 2.* The % computational cost reduction of proposed scheme compare to existing schemes is shown in *Table 3*. The execution time of $One\ \mathrm{M-Exp}(1024)$ is $220ms$ while level$One\ ECPM(160\ \mathrm{bits})$ is $83ms$ based on Infineon's SLE 66CUX640P (@ 15 MHz), a security controller [19] implementation.

Table 2: Comparative computational cost analysis

Schemes	Multi Receiver Signcryption Cost Signcryption Cost for t Receiver	Unsigncryption Cost
Proposed	$t+1\ ECPM$	$3\ ECPM$
[6, 10]	$t\ \ M-Exp$	$2\ M-Exp$
[13]	$t+1\ M-Exp$	$3\ \ M-Exp$
[15]	$t+2\ M-Exp$	$2\ \ M-Exp$

Table 3: % Computational Time Reduction

Number of Receiver	Multi Receiver Signcryption Schemes			%Saving in Computation Cost at each Recipient	
	[6, 10]	**[13]**	**[15]**	**[6, 10, 15]**	**[13]**
5	54.7	62.2	67.6	43.4	62.2
10	58.5	62.2	65.4	43.4	62.2
50	61.5	62.2	62.9	43.4	62.2
100	61.8	62.2	62.6	43.4	62.2

5.2. **Communication overhead**

Communication overhead analysis is based on the NIST recommended security parameters size such that:
$|p| \geq 2^{1024}, |q| \geq 2^{160}, |n| \geq 2^{160}, |h| = 160\ bits\ \ and\ |c_i| = 128\ bits.$

The communication overhead of proposed scheme is analyzed and compared with existing schemes in *Table 4*, while % communication overhead reduction of proposed scheme compared to existing schemes is shown in *Table 5*.

Table 4: Comparative Communication Overhead analysis

Multi Receiver Signcryption Schemes	Communication Overhead
[13]	$t|c| + t|\ h| + t|q|$
[6, 10]	$|c| + t|\ c_i| + t|\ h| + t|q|$
[15]	$|c| + t|\ c_i| + |\ h| + t|p|$
[16]	$|c| + t|\ c_i| + t|\ h| + |q|$
[9]	$|c| + t|\ c_i| + t|\ h| + |q|$
Proposed	$|c| + t|\ c_i| + |\ h| + |q|$

Table 5: % saving in Communication Overhead

Number of Recipients	Multi Receiver Signcryption Schemes		
	[9, 16]	**[6, 10]**	**[15]**
5	50	64.285	86.486
10	52.631	67.857	87.671
50	54.945	70.714	88.642
100	55.248	71.071	88.765

6. Conclusion

This paper present an efficient elliptic curves based construction of Multi Receiver Signcryption in the Public key infrastructure. It provides confidentiality, sender authentication, message integrity, sender unforgeability, sender non-repudiation, key forward secrecy and message public verifiability. Proposed scheme have additional properties of forward secrecy preserving message confidentiality, if private key of the sender compromised. Analysis shows that proposed scheme is efficient 43 to 62 % in term of computation cost and 50 to 88 % in term of communication overhead compared to existing schemes. Therefore it can be concluded that the proposed scheme is a lightweight security system and is more suitable for secure multicast environments having scarce resources.

REFERENCES

[1] A. K. Haddad, R. H. Riedi. (2014). Bounds on the Benefit of Network Coding for Wireless Multicast and Unicast, IEEE Transactions on Mobile Computing, 13(1) 102-115.

[2] R. O. Afolabi, A. Dadlani, K. Kim. (2013). Multicast Scheduling and Resource Allocation Algorithms for OFDMA-Based Systems: A Survey, IEEE Communications Surveys & Tutorials, Vol. 15(1) 240-254.

[3] W. Diffie, P. C. van Oorschot, M. J. Wiener. (1992). Authentication and authenticated key exchange, Designs Codes and Cryptography 2, 107-125

[4] B. Colin, G. Nieto, Juan M. (2011). On forward secrecy in one round key exchange, In LNCS: Cryptography and Coding, 451-468.

[5] Kurosawa, K. (2002). Multi-recipient public-key encryption with shortened ciphertext. In: PKC 2002. LNCS, vol. 2274, 48–63.

[6] Bellare, M., Boldyreva, A., Staddon, J. (2002). Multi-recipient encryption schemes: Security notions and randomness re-use, In PKC 2003. LNCS, vol. 2567, 85–99.

[7] Bellare, M., Boldyreva, A., Kurosawa, K., Staddon. (2007). Multi recipient encryption schemes: How to save on bandwidth and computation without sacrificing security, IEEE Transactions on Information Theory 53(11), 3927–3943.

[8] Y. Zheng. (1998). Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption), Advances in Cryptology-CRYPTO 97, LNCS 1294, Springer-Verlag. 165-79 (1997).

[9] Y. Zheng, Signcryption and Its Applications in Efficient Public Key Solutions, Information Security Workshop, LNCS1397, 291-312

[10] Y. Han, X. Yang, Y. Hu. (2004). Signcryption based on elliptic Curves and its multi-party schemes"3rd international conference on Information security, 216 – 217

[11] H. M. Elkamchouchi, A. M. Emarah, E. A. A. Hagras. (2007). A new public key multi-message signcryption (PK-MMS) scheme for secure Communication Systems, 5th Annual Conference on Communication Networks and Services Research, 387-392.

[12] H. M. Elkamchouchi, A. M. Emarah, E. A. A. Hagras. (2007). A New Efficient Public Key Multi-Message Multi-Recipient Signcryption (PK-MM-MRS) Scheme For Provable Secure Communications, International Conference on Computer Engineering & Systems,

[13] X. Yang, M. L. Lixian, W. Y. Han. (2008). New ECDSA-verifiable multi-receiver generalization signcryption, 10th IEEE International Conference on High Performance Computing and Communications, 1042-1047

[14] H. M. Elkamchouchi, M. E. Nasr, R. Ismail. (2009). A New Efficient Publicly Verifiable Signcryption Scheme and Its Multiple Recipients Variant for Firewalls Implementation, 26th National Radio Science Conference,

[15] Y. Han, X. Gui. (2009). Multi-recipient signcryption for secure group communication, 4th IEEE Conference on Industrial Electronics and Applications, 161-165

[16] H. M. Elkamchouchi, M. E. Nasr, R. Ismail. (2009). A new efficient publicly verifiable signcryption scheme and its multiple recipients variant for firewalls implementation, IEEE National Radio Science Conference, 1-9.

[17] H. M. Elkamchouchi, M. Nasr, R. Ismail. (2009). A New Efficient Multiple Broadcasters Signcryption Scheme (MBSS) for Secure Distributed Networks. IEEE 5th International Conference on Networking and Services, 204-209

[18] F. Ahmed, A. Masood, F. Kausar. (2010). An efficient multi recipient signcryption scheme offering non repudiation, 10th IEEE International Conference on Computer and Information Technology.

[19] Y. Zheng, H. Imai. (1998). How to construct efficient signcryption schemes on elliptic Curves" Information Processing Letters 68, 227-233.

[20] H. Y. Jung, K. S. Chang, D.H. Lee, J.I. Lim. (2001). Signcryption schemes with forward secrecy, Proceeding of WISA, 403–475.

[21] R. J. Hwang, C. H. Lai, and F. F. Su. (2005). An efficient signcryption scheme with forward secrecy based on elliptic Curves, Applied Mathematics and Computation 167, 870–881.

[22] M. Toorani, A. A. B. Shirazi. (2009). An Elliptic Curves-based Signcryption Scheme with Forward Secrecy, Journal of Applied Sciences, 9(6), 1025-1035.

[23] E. Mohamed, H. Elkamchouchi. (2009). Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy, International Journal of Computer Science and Network Security 9(1).

[24] Nizamuddin, S. A. Ch, Amin, N. (2011). Signcryption Schemes with Forward Secrecy Based on Hyperelliptic Curve Cryptosystem, High Capacity Optical Networks and Enabling Technologies, 244-247.

[25] S.A. Ch, Nizamuddin, M. Sher. (2012). Public Verifiable Signcryption Schemes with Forward Secrecy Based on Hyperelliptic Curve Cryptosystem, Information Systems, Technology and Management Communications in Computer and Information Science, 285, 135-142

[26] L. Batina, S.B. O¨ rs, B. Preneel, J. Vandewalle. (2003). Hardware architectures for public key cryptography, Integration the VLSI Journal 34 (1–2) 1–64.