An Efficient Multi-Message Multi-Receiver Signcryption Scheme with Forward Secrecy on Elliptic Curves

Nizamud Din, Arif Iqbal Umar, Abdul Waheed, Noor Ul Amin
Department of Information Technology, Hazara University Mansehra
sahibzadanizam@yahoo.com, arifiqbalumar@yahoo.com,
abdulwaheed@hu.edu.pk, namin@hu.edu.pk

July 1, 2015

Abstract

Secure multicast communication has application in growing number of applications. Forward secrecy is of prime importance and insures message confidentiality even long-term private key compromised. We present an efficient construction of multi message multi receiver signcryption with forward secrecy on elliptic curves. It provides confidentiality, integrity, authenticity, non-repudiation, public verifiability, unforgeability and forward secrecy of multi message multicast. It is efficient in computation cost and communication overhead and suitable for resource constrained IP-based secure multi message multicast systems.

1 INTRODUCTION

To support several groups of users with flexible quality of service (QoS) requirements [1], multicasting [2]is promising enabling technology for Next Generation Networks (NGN). Compare to unicast communication its security concerns are considerably more complex.

Message security attribute forward secrecy coined by [3]is defined as compromised of sender long-term private key should not result in compromise of session keys. It is one of the important security properties for key agreement, confidentiality and implicit authentication [4].

Since the first signcryption presented by Zheng[5] and its multi receiver construction [6]in the public key infrastructure a set of multi receiver signcryption schemes[7][8][9][10], and signcryption schemes with forward secrecy[11][12]–[14].

Existing schemes lack either multi receiver functionality or forward secrecy.

We proposed an efficient multi message multi receiver signcryption with forward secrecy in the public key infrastructure using elliptic curves. The proposed scheme provides security attribute of message confidentiality, message

integrity, message verifiability, sender authenticity, signer unforgeability, sender non-repudiation and forward secrecy. It is computational and communication efficient and attractive for scarce multi message multicast communication.

2 PRELIMINARIES

The notations used in the rest of the paper are briefly described.

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

An Elliptic curve E over finite field F_q is defined by equation of the form:

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

Table1. Notation Guide

Notation	Explanation
G	A base point on elliptic curve E with order $n \geq 2^{160}$
d_i	Private key
P_i	Public key $P_i = d_i.G$
h/h_k	Hash/Keyed Hash Function
$E_k(.)/D_k(.)$	Symmetric Encryption/Decryption Algorithm using key k
m_i/c_i	Message/Ciphertext
$\perp$	Reject

Definition 1 *ECDLP:*

Let P and Q be two given points of an elliptic curve E , Find an integer k , such that $Q = k.P$ mod n. Computing an integer k is hard for sufficient large value of sufficient security parameters.

Definition 2 *ECDHP:*

Let $\{d, e\} \epsilon F_q$ and G,P,Q are points on E and $P = x\bullet G$ and $Q = y\bullet G$. Without knowing x and y , find another point $Z = x.y.G$

Computing point $Z = x.y.G$ is hard for sufficient security parameters.

3 PROPOSED MULTI RECEIVER SIGNCRYPTION SCHEME

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

- **Setup**

In setup phase, the security parameters such as finite field, elliptic curve, and base point are defined and published in-group members.

- **Key Generation**

In key generation phase member $i \epsilon \{1, 2, \ldots, t\}$ of the multicast group randomly generate private key $d_i \epsilon \{1, 2, \ldots, n-1\}$ and computes public key $P_i = d_i.G$ where $i \epsilon \{1, 2, \ldots, t\}$.

Each member of the multicast group gets certificate of his public key from the certificate authority and publish to the group member.

- **Multi-Message Multi Receiver Signcryption**

Let a group member wants to securely multicast a vector of distinct messages $m_i \epsilon M$ to distinct receivers having identity ID_i, the sender should run probabilistic polynomial time (PPT) algorithm $MM - MRSC$, takes inputs: vector of distinct messages $m_i \epsilon M$, the sender's private keys d_s and all receiver's public keys $\{P_1, P_2, \ldots, P_t\}$, and returns a signcrypted text $\Psi = (\Omega, \omega, s, R)$.

Algorithm 3 *$MM - MRSC$ (m_i,d_s,P_1,P_2,...,P_t)*

- *1. Verifies each receiver public key d_i*
  2. Randomly selects an integer $k \epsilon_R \{1, \ldots, n-1\}$
  3. Computes for each recipient
    - *Computes $K_{h_i} || S_{k_i} = h(k.P_i)$*
    - *Computes $r_i = h(m_i || K_{h_i})$*
    - *Computes $c_i = E_{S_{k_i}}(m_i || K_{h_i})$*
    - *Generates $\Omega = \{c_1, c_2, \ldots, c_t\}$*
  4. Computes $s_i = (d_s + r_i.k) mod n$
  5. Generate $\omega = \{s_1, s_2, \ldots, s_t\}$
  6. Computes $R = k.G$
  7. Return $\Psi = (\Omega, \omega, R)$

  Multicast Ψ

- **Unsigncryption Phase**

  Each receiver in the multicast group having identity ID_i selects his relevant information (c_i, ω, s, R) from multicast signcrypted text $\Psi = (\Omega, \omega, s, R)$ and run deterministic polynomial-time Unsigncryption algorithm and output the verified message or $\perp$.

  Algorithm 4 *Unsigncryption (c_i, R, s, P_s, d_{ri})*

  1. Verifies sender public key P_s
  2. Computes$K_{h_i} || S_{k_i} = h(d_{ri}.R)$
  3. Compute $m_i || K_{h_i} = D_{S_{k_i}}(c_i)$
  4. Compute $r_i = h(m_i || K_{h_i})$

5. *Verifies* $(s.G - r_i.R) = P_s$ *If true then accept* m_i *else* $\perp$

Theorem 5 *multi-message multi-receiver signcryption and Unsigncryption valid, if sender and receiver confirm 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: multi message multi-receiver confidentiality, integrity, unforgeability, forward secrecy, public verifiability; sender authentication and non-repudiation based on the will known security assumptions that solving ECDLP and ECDHP are hard for sufficient security parameters[10] and hash function is one way and collision resistance.

4.1 Confidentiality

Let an eavesdropper wants to derive the original messages, he must get the secret keys K_{h_i} and S_{k_i} . However, we show that possible ways to generate K_{h_i} and S_{k_i} is equivalent to solve the $ECDLP$ and $ECDHP$.

Case 6 *An eavesdropper can compute* K_{h_i} *and* S_{k_i} *from equation (2), if he computes* d_{ri}*from equation (1). The attacker gets each recipient public key* P_{ri} *easily but if tries to generate* d_{ri} *from equation (2), and then he has to solve* $ECDLP$.

$$P_{ri} = d_{ri}.G \quad (1)$$

$$K_{h_i}||S_{k_i} = h(d_{ri}.R) \quad (2)$$

Case 7 *An eavesdropper can compute* K_{h_i} *and* S_{k_i} *from equation (6), if he computes* Z*. The attacker gets each recipient public key* P_{ri} *and* R *but computing* Z *as in equation (5) from equation (3)and (4), and then he has to solve* $ECDHP$.

$$R = k.G \quad (3)$$

$$P_{ri} = d_{ri}.G \quad (4)$$

$$Z = d_{ri}.k.G \quad (5)$$

$$K_{h_i}||S_{k_i} = h(Z) \quad (6)$$

4.2 Integrity

Each recipient in the multicast group can verify whether the received message is not corrupted one, and original as sent by the sender. Sender computes r_i=$h\,(m_i||K_{h_i})$, and $s_i = (d_s + r_i.k)\ mod\ n$. Receiver Computes $r^{'} =$

$h\,(m_i||K_{h_i})$and verify $(s.G - r^{'}.R) = P_s$. It is computationally infeasible for an attacker to modify c as $c^{'}$ such that $m \neq m^{'}$ and $r^{'} = r$ by the one-way and collision resistant property of hash function.

4.3 Unforgeability

Without sender private key d_s and session key k eavesdropper can't forge valid (m_i, s_i, R), while the legitimate receiver cannot forge without d_s or session key k.

The stronger forgery legitimate receiver tries to forge a valid $\left(m_i^{'}, s_i^{'}, R_i^{'}\right)$ from a previous (m_i, s_i, R), that he received. He must generate $s_i^{'}$ from equation (9) for message $m_i^{'}$. To compute $s_i^{'}$; he must either compute d_s from equation (7) or k from equation (8), that is equivalent to solve $ECDLP$; hence proposed scheme is unforgeable.

$$P_s = d_s.G \tag{7}$$

$$R = k.G \tag{8}$$

$$s^{'} = (d_s + r.k) mod n \tag{9}$$

4.4 Authentication

Each receiver authenticates the sender by using his public key P_s certificate and verifies the authenticity of the message by using equation

$$(s.G - r.R) = P_s \tag{10}$$

4.5 Non-repudiation

In key distribution phase, sender obtain certificate associated with public key P_s that is associated with sender private key d_s. Sender cannot deny the message signcrypted by them as the third party/ judge can validate the sender public key using his/her certificate and settle dispute

4.6 Judge Verification Phase

In case of dispute, receiver only provides (m_i, K_{h_i}, s_i, R) to the third party/judge to decide that original sender sent m_i to the recipient or not. The judge run deterministic algorithm *Judge Verify* and decide whether the original sender sent message or not.

Algorithm 8 *Judge Verify (m_i, K_{h_i}, s_i, R)*

1. *Verifies sender's public key P_s by using his certificate.*

2. *Computes* $r_i = h(m_i||K_{h_i})$

3. *Computes* $s.G - r_i.R$

4. *The message is sent by original sender if* $s.G - r_i.R = P_s$

Theorem 9 *Receiver and judge verification phase is considered valid if sender and receiver/judge conform to the equation:* $s.G - r.R = P_s$
Proof.

$$\begin{aligned} & s.G - r_i.R \\ = \; & (d_s + r_i.k).G - r_i.R \\ = \; & (d_s + r_i.k).G - r_i.R \\ = \; & d_s.G + r_i.k.G - r_i.R \\ = \; & P_s + r_i.R - r_i.R \\ = \; & P_s \end{aligned}$$

Clearly,the equations.$G - r.R = P_s$ *is established.* ■

4.7 Forward secrecy

Let the sender's private key d_s compromised, the eavesdropper try to recover any previous message m_i from signcrypted text Ψ . They can computes k from equation (11) if computes r_i from equation (12) without knowing original message m_i which is infeasible because the hash function is one-way.

$$r_i = h\left(m_i||K_{h_i}\right) \tag{12}$$

$$k = (r_i + d_s)^{-1}s \tag{11}$$

The security attributes of the proposed scheme is compared with existing schemes in Table 2

Table 2 Security Analysis of Proposed Scheme with Existing Schemes

	Security features							
Schme	F_1	F_2	F_3	F_4	F_5	F_6	F_7	Multi Receiver
Proposed	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**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*

Confidentiality (F_1), Integrity (F_2), Authenticity(F_3), Unforgeability (F_4), Non-Repudiation(F_5), Direct Public Verifiability (F_6), Forward Secrecy (F_7)

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, while sending data from sender to receiver.

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 3.

Table 3 Comparative Computational Cost Analysis

Scheme	Signcryption Cost t Receiver	Unsigncryption Cost
Proposed	$\mathbf{t+1ECPM}$	**3ECPM**
[6, 10]	$t\ M-Exp$	$2M-Exp$
[13]	$t+1M-Exp$	$3M-Exp$
[15]	$t+2M-Exp$	$2M-Exp$

The execution time of One $M-Exp$ (1024) is $220ms$ while levelOne $ECPM$ ($160bits$) is $83ms$ based on Infineon's SLE $66CUX640P$ (@ $15MHz$), a security controller [15] implementation. The % computational cost reduction of proposed scheme compare to existing schemes is shown in Table 3.

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.

Table 4 Comparative Communication Overhead Analysis

Scheme	Communication Overhead
[13]	$t\,\|c\| + t\,\|h\| + t\,\|q\|$
[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	$\mathbf{\|c\| + t\,\|c_i\| + \|h\| + \|q\|}$

6 CONCLUSION

In this paper, an efficient construction of multi-message multi-receiver signcryption based on elliptic curves is proposed. It provides message confidentiality, sender authentication, message integrity, message verifiability, sender unforgeability, sender non-repudiation and forward secrecy. Forward secrecy preserves message confidentiality even if sender long-term private key compromised. Cost Analysis shows that proposed scheme is efficient and provides lightweight multi-message multicast secure message dissemination.

References

[1] R. O. Afolabi, A. Dadlani, and K. Kim, "Multicast Scheduling and Resource Allocation Algorithms for OFDMA-Based Systems: A Survey," IEEE Commun. Surv. Tutorials, vol. 15, no. 1, pp. 240–254, 2013

[2] A. Keshavarz-Haddad and R. Riedi, "Bounds on the benefit of network coding for wireless multicast and unicast," Mob. Comput. IEEE . . . , 2014.

[3] W. Diffie, P. van Oorshot, and M. Wiener, "Authentication and Authenticated Key Exchange," Des. Codes Cryptogr., vol. 2, pp. 107–125, 1992.

[4] C. Boyd and J. G. Nieto, "On forward secrecy in one-round key exchange," Lect. Notes Comput. Sci., vol. 7089 LNCS, pp. 451–468, 2011.

[5] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption)," in Advances in Cryptology — Crypto '97, 1997, pp. 165–179.

[6] Y. Zheng, "Signcryption and its applications in efficient public key solutions," in Information Security, LNCS Volume 1396, 1998, pp. 291–312.

[7] H. M. Elkamchouchi, A. M. Emarah, and E. A. A. Hagras, "Public Key Multi-Message Signcryption (PK-MMS) scheme for secure communication systems," in Proceedings - CNSR 2007: Fifth Annual Conference on Communication Networks and Services Research, 2007, pp. 329–334.

[8] H. M. Elkamchouchi, A. A. M. Emarah, and E. a a Hagras, "A new efficient public key multi-message multi-recipient signcryption (PK-MM-MRS) scheme for provable secure communications," ICCES'07 - 2007 Int. Conf. Comput. Eng. Syst., pp. 89–94, 2007.

[9] H. Elkamchouchi, M. Nasr, and R. Ismail, "A new efficient multiple broadcasters signcryption scheme (MBSS) for secure distributed networks," Proc. 5th Int. Conf. Netw. Serv. ICNS 2009, pp. 204–209, 2009.

[10] F. Ahmed, A. Masood, and F. Kausar, "An efficient multi recipient signcryption scheme offering non repudiation," Proc. - 10th IEEE Int. Conf.

Comput. Inf. Technol. CIT-2010, 7th IEEE Int. Conf. Embed. Softw. Syst. ICESS-2010, ScalCom-2010, no. Cit, pp. 1577–1581, 2010.

[11] R. Hwang, C. Lai, and F. Su, "An efficient signcryption scheme with forward secrecy based on elliptic curve," vol. 167, pp. 870–881, 2005.

[12] M. Toorani and A. A. B. Shirazi, "Cryptanalysis of an elliptic curve-based signcryption scheme," Int. J. Netw. Secur., vol. 10, no. 6, pp. 51–56, 2010.

[13] M. Toorani and A. A. B. Shirazi, "Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve," in Proceedings of the 2008 International Conference on Computer and Electrical Engineering, ICCEE 2008, 2008, pp. 428–432.

[14] E. Mohamed and H. Elkamchouchi, "Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy," vol. 9, no. 1, pp. 395–398, 2009.

[15] L. Batina, S. Örs, B. Preneel, and J. Vandewalle, "Hardware architectures for public key cryptography," Integr. VLSI J., 2003.