J. Appl. Environ. Biol. Sci., 6(2S)144-150, 2016

© 2016, TextRoad Publication

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

A Novel Multi Receiver Signcryption Scheme Based on Elliptic Curves for Firewalls

Nizamuddin, Arif Iqbal Umar, Noor Ul Amin, Abdul Waheed

Department of Information Technology, Hazara University Mansehra, Pakistan

Received: January7, 2016
Accepted: March 2, 2016

ABSTRACT

We presenta Multi Receiver Signcryption Scheme based on elliptic curves for firewalls. It provides encrypted traffic authentication by Firewalls and ensures efficient and secure multicast communication.It enables firewall to verify encrypted message without obtaining any secret parameter from the participants. It has security attributes of message confidentiality, sender authentication, message integrity, signature unforgeability, sender non-repudiation, encrypted message authenticity and public verifiability. Its security attributes and cost effectivenes make it a suitable choice for efficient and secure multicast firewalls applications.

KEYWORDS: Public key Cryptography; Elliptic Curves; Signcryption; Multicast; Firewall

1. INTRODUCTION

Signcryption is a cryptographic primitives. It was proposed by Zheng [1] to reduce the computational and communication costs of authenticated encryption.It is a hot research area and many Signcryption Schemes are proposed in the litecture [1, 2, 3, 4, 5, 6, 7, 8].

Multicast is an efficient mean totransmit information from a source to multiple destinations. It reduces transmission overheads of the sender, network bandwidth consumption and latency. These characteristics make multicast an ideal technology for communication among group of people. Many Multi Receiver Signcryption schemes [9, 10, 11, 12, 13, 14, 15] are proposed to ensure efficient and secure multicast.

Firewalls are installed either as hardware devices or software applications to enforce security policies within a network or between networks. It operates at different layers and protects private local area networks from hostile intrusion.The application layer firewalls provides the most comprehensive filtering of end-user level message authentication.

The literature reflects that out of the proposed schemes, tenschemes [2, 3, 5, 9, 10, 11, 12, 13, 14,15] could not be implemented in firewalls applications due to lack of encrypted message authentication characteristic.Fourschemes [4, 6, 7, 8] are suitable for firewalls but have limitations.All these schemes do not provide multi receiver functionality. The scheme proposed in [4] is based on expensive Discrete Logarithm Problem (DLP) which requires modular exponentiation as compare to Elliptic Curve Discrete Logarithm Problem(ECDLP).The schemes proposed in [6, 7] are based on elliptic curves discrete logarithm problem but do not provide message confidentiality.

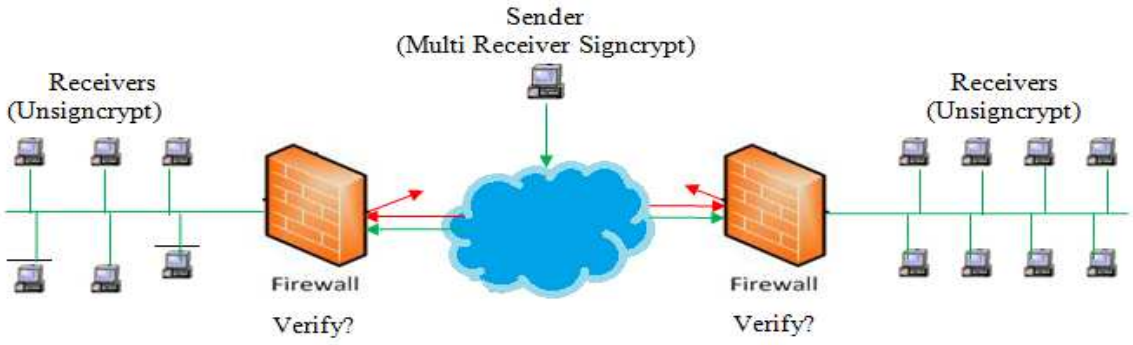

Figure 1.Application-Level Firewalls for Incoming Message Authentication in LAN

* **Corresponding Author:** Nizamuddin, Department of Information Technology, Hazara University Mansehra, Pakistan
sahibzadanizam@yahoo.com

2. Contribution. The objective of this research is to identify and implement the security requirements of firewalls for multicast Signcrypted messages. To achieve this objective, we designed an efficient multi receiver signcryption scheme based on elliptic curves that enables firewalls to verify the authenticity of the network traffic without disclosing the contents of the encrypted messages.
The proposed scheme has the security attributes for multicast message namely: confidentiality, integrity, origin non-repudiation, unforgeability, originator and encrypted message authentication and public verifiability. Encrypted message authentication attribute enable firewalls, to check the authenticity of incoming encrypted traffic. It is efficient in terms of computationalcost and communication overheads.It could be used for efficient and secure multicast communications.

3. Proposed Multi Receiver Signcryption Scheme. The proposed Multi Receiver Signcryption scheme consists of five phases namely: Initialization, Key Generation, Multi Receiver Signcryption, Firewall Verification and Unsigncryption

3.1. Initialization. In this phase domain security parameters are defined and published by a trusted authority.

Table 1. Domain Security Parameters and Notation

Notation	Interpretation
$\mathbf{p}$	a large prime number, where p $\geq 2^{1024}$
$\mathbf{C}$	an elliptic curve : $y^2 = x^3 + ax + b$ over finite field of order q $\geq 2^{160}$
$\boldsymbol{G}$	a base point of elliptic curve with order n, where n $\geq 2^{160}$
$\boldsymbol{h}$	one-way hash function
$\boldsymbol{E_k/D_k}$	symmetric encryption /decryption algorithm using key k
$\boldsymbol{t}$	number of receiver
$\boldsymbol{m}$ / $\boldsymbol{c}$	message / cipher text
$\boldsymbol{c_i}$	encrypted session key

3.2. Key Generation. In this phase each member in the group randomly selectsaprivate key$P_{ri}$and generates public key P_{ui}as:

$$P_{ri} \in_R \{1, \ldots, n-1\}$$
$$P_{ui} = P_{ri}.G \bmod n$$

Each member of the group obtains certificate for public key from certificate authority and distribute the public key along with certificate.

3.3. Multi Receiver Signcryption. To multicast a message m in confidential and authenticated way to a group of t receivers having identities $\{ID_1, ID_2, \ldots, ID_t\}$, the sender runs *Multi Receiver Signcryption*algorithm. It input parameters are: Sender private/publickeyP_{rs} /P_{us}, and each receiver public keys $\{P_{u1}, P_{u2}, \ldots, P_{ut}\}$. It returns Signcrypted text(c, ω, r, s).
IF the sender having identityID_s wants to multicast message m to t receivers having identities$\{ID_1, ID_2, \ldots, ID_t\}$ in a confidential and authenticated way then the Sender performs the following steps:

Multi Receiver Signcryption $(\boldsymbol{m, P_{rs}, P_{u1}, P_{u2}, \ldots, P_{ut}})$

Step 1. Verifies each recipient public key P_{ui} by using their certificates
Step 2. Randomly selects an integer $w \in_R \{1, \ldots, n-1\}$
Step 3. Generates cipher textc, where$c = E_w(m)$
Step 4. Randomly selects an integer$x \in_R \{1, \ldots, n-1\}$
Step 5. Computes the encrypted session keys $c_i$for each recipient
a) Computes $sk = h(x.P_{ui})$
b) Computes $c_i = E_{sk}(w)$
c) Computes $\omega = \{c_1, c_2, \ldots, c_t\}$
Step 6. Computes $Y = x.G$
Step 7. Computes $r = h(c||\omega||Y)$ using one-way hash function
Step 8. Computes $s = x/(r + P_{rs}) \bmod n$
Returns(c, ω, r, s)
Multicast the Signcrypted text $(c, \omega, r, s)$to each group member

3.4 Signature Verification by Firewalls. Firewalls verify the authenticity of received Signcrypted text (c, ω, r, s)as follow:

Firewalls Verify$(\boldsymbol{c}, \boldsymbol{c_1}, \boldsymbol{c_2}, \ldots, \boldsymbol{c_t}, \boldsymbol{r}, \boldsymbol{s})$

Step 1. Verifies sender public key P_{us} using their certificate.
Step 2. Computes $Z = s.(P_{us} + r.G)$
Step 3. Computes $r' = h(c||\omega||Z)$
Step 4. Accept and forwards Signcrypted text if $r' = r$ otherwise reject.

Theorem1. Multi Receiver Signcryption verification is considered valid if the sender and verifier conform to the applied protocols $Z = s.(P_{us} + r.G)$.

Proof

$$Z = s.(P_{us} + r.G)$$
$$= \frac{x}{(r+P_{rs})}(P_{rs}.G + r.G)$$
$$= \frac{x.G}{(r + P_{rs})}(P_{rs}.+r)$$
$$= x.G = Y$$

Clearly, the equation $h(c||\omega||Y) = h(c||\omega||Z)$ is established.

3.5 Unsigncryption. Each receiver in multicast group having identity ID_i extracts his corresponding parameters (c, c_i, r, s) from Signcrypted text (c, ω, r, s), verifies and gets the message using *Unsigncryption*algorithm as follows:

Unsigncryption $(\boldsymbol{c, c_i, r, s, P_{us}, P_{ri}, P_{ui}})$

Step 1. Verifies sender public key $P_{us}$by using his certificate.
Step 2. Computes $Z = s.(P_{us} + r.G)$
Step 3. Computes $r' = h(c||\omega||Z)$
Step 4. Computes $sk = h(P_{ri}.Z)$
Step 5. Computes$w = D_{sk}(c_i)$using symmetric decryption algorithm and secret key sk
Step 6. Computes message as $m = D_w(c)$using symmetric decryption and key w
Step 7. Accept message if $r = r'$ else reject

Theorem2. Multi Receiver Signcryption decryption is considered valid if sender and receiver conform to the applied protocols.

Proof

$$P_{ri}.\mathrm{Z} = P_{ri}.s.(P_{us} + r.G)$$
$$= P_{ri}.\frac{x}{(r + P_{rs})}(P_{rs}.G + r.G)$$
$$= \frac{P_{ri}.x.G}{(r + P_{rs})}(P_{rs}.+r)$$
$$= x.P_{ri}.G$$
$$= x.P_{ui}$$

Clearly, the equation $P_{ri}.\mathrm{Z} = x.P_{ui}$ is established.

4 Security Analysis. The security analysis of the proposed scheme is presented. It is based on the assumption that solving Elliptic Curve Discrete Logarithm Problem (ECDLP) is hard for sufficient large numbers [16, 17]. The proposed scheme is compared with state of the art schemes. It is reflected in Table1.

Definition 1: (The Elliptic Curve Discrete Logarithm Problem). Let P and Q be two points of an elliptic curve C. Find an integer k, such that $Q = k.P$.

4.1 Confidentiality. The proposed scheme provides confidentiality, if an attacker wants to derive the original message, then attacker must obtain the secret key sk and further compute message session key w. The following are the possible **cases** to derive secret key sk :

Case 1: An attacker can compute sk from Equation (4) if attacker gets x from Equation (2) and P_{ri} from Equation (3).The attacker can compute Z from Equation (1) and get the receiver public key P_{ui}, however if attacker tries to compute x from Equation (2) and P_{ri} from Equation (3) and then attacker has to solve two $ECDLP$.

$$Z = s.(P_{us} + r.G) \quad (1)$$
$$Z = x.G \quad (2)$$
$$P_{ui} = P_{ri}.G \quad (3)$$
$$sk = h\,(x.P_{ri}.G) \quad (4)$$

Case 2: An attacker can compute sk from Equations (6) and (7) if attacker gets P_{rs} from Equation (5). The attacker can get the sender public key P_{us}, however if tries to compute P_{rs} from Equation (5) then attacker has to solve $ECDLP$.

$$P_{us} = P_{rs}.G \quad (5)$$
$$s = x/\,(r + P_{rs})\ mod\ n \quad (6)$$
$$sk = h\,(x.P_{ui}) \quad (7)$$

Case 3: An attacker can compute sk from Equations (9) and (10) if attacker gets P_{ri} from Equation (8). The attacker can get any receiver public key P_{ui}, however if attacker tries to compute P_{ri} from Equation (8) then attacker has to solve $ECDLP$.

$$P_{ui} = P_{ri}.G \quad (8)$$
$$\mathrm{Z} = s.(P_{us} + \mathrm{r.G}) \quad (9)$$
$$sk = h(P_{ri}.Z) \quad (10)$$

4.2 Integrity. Firewalls and each recipient can verify whether the received signcrypted text is the original, and sent by the legitimate sender. In Signcryption phase the sender computes r using one-way collision resistive hash function. If an attacker changes the original ciphertext c as c', r is changed to $r' = h_k(c'||\omega||Z)$. It is computationally infeasible for an attacker to modify c as c' such that $r' = r$ due to collision resistive property of one-way hash function.

4.3 Public Verifiability. Third party can verify the authenticity of the multi receiver signcrypted text(c, ω, r, s) message when dispute occurs. The verification procedure defined in *section 3.4,* requires public parameters; sender's public key P_{us} and(c, r, s).

4.4 Encrypted Message Authentication. Firewalls can verify whether received multi receiver signcrypted text is sent by legitimate sender or not without disclosing message contents using procedure defined in *section 3.4*.

4.5 Non-repudiation. Sender cannot deny from multi receiver signcrypted text. As the sender public key P_{us} is associated to his private key P_{rs}, using sender public key P_{us}. Third party can decide using procedure defined in *section 3.4*, whether the message is sent by the claimed sender or not.

4.6 Unforgeability. The attacker/recipient cannot forge valid (m, r, s) without private key of the sender. Assume they tries to forge a valid (m', r', s') from a previous (m, r, s) eavesdropped. They must generate s' from Equation (14) for message m'. For computing valid signature s', attacker has to compute sender private key P_{rs} from Equation (11) while recipient has to compute secret parameter x from Equations (12) and (13) which is equivalent to solve $ECDLP$.

$$P_{us} = P_{rs}.G \quad (11)$$
$$\mathrm{Z} = s.(P_{us} + \mathrm{r.G}) \quad (12)$$
$$P_{ri}.\mathrm{Z} = x.P_{ui} \quad (13)$$
$$s' = x/(r + P_{rs})\ mod\ n \quad (14)$$

Table 2. Comparsionof Security Features and Suitability of the Proposed and Existing Schemes for Implementation in Firewalls

Schemes	Security Features					Multi Receiver Functionality	Suitability for Firewalls Application
	Confidentiality	Authenticity	Integrity	Non Repudiation	Unforgeability		
Proposed	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Gamage [4]	Yes	Yes	Yes	Yes	Yes	No	Yes
Bao [5]	Yes	Yes	Yes	Yes	Yes	No	No
Mohamed [6]	No	Yes	Yes	Yes	Yes	No	Yes
Iqbal et al [7]	No	Yes	Yes	Yes	Yes	No	Yes
Toorani [8]	Yes	Yes	Yes	Yes	Yes	No	Yes
Zheng [9]	Yes	Yes	Yes	Yes	Yes	Yes	No
Han etal. [10]	Yes	Yes	Yes	Yes	Yes	No	No
Elkamchochi [11]	Yes	Yes	Yes	Yes	Yes	Yes	No
Han [14]	Yes	Yes	Yes	Yes	Yes	Yes	No
Li[15]	Yes	Yes	Yes	Yes	Yes	Yes	No

5. Efficiency. Efficiency of public key cryptographic scheme is usually evaluated on basis of the number of major expensive operation involved, like Modular Exponentiation (M-Exp) or Elliptic Curve Point Scalar Multiplication (ECPM) and communication overhead (Extra bits appended for security purposes) during sending data from sender to multi receivers.

5.1 Computational Cost Analysis. The computational efficiency of the proposed scheme is analyzed on the basis of two major operations namely M-Exp and ECPM. Table 3 illustrates the efficiency comparison of the proposed scheme and existing schemes. The proposed scheme is based on elliptic curve and is efficient than M-Exp based scheme.

In the same security level one ECPM(160 bits) has 83ms while one M-Exp (1024) has 220ms execution time in the Infineon's security controller SLE 66CUX640P (@ 15 MHz) [18]. Percent computation cost reduction in milli second of the proposed scheme on the basis of security controller [14] implementation is shown in Table 4:

Table 3. Computational Cost Comparison

Schemes	Signcryption	Firewalls Verification	Unsigncryption
Proposed	$t+1$ ECPM	2 ECPM	3 ECPM
[9]	t M − Exp	-	2 M − Exp
[11]	t M − Exp	-	2 M − Exp
[12]	t M − Exp	-	2 M − Exp
[13]	$t+2$ M − Exp	2 M − Exp	3 M − Exp

Table 4. % Saving in Computation Time

Number of Receiver	Signcryption		Unsigncryption
	[9] [11] [12]	[13]	[9] [11] [12] [13]
5	54.727	67.662	31.967
10	58.5	65.416	31.967
50	61.518	62.998	31.967
100	61.895	62.642	31.967

5.2. Communication Overhead Analysis. The proposed scheme is efficient than existing schemes as shown in Table 5.

Compared to existing schemes percent communication overhead reduction of the proposed scheme for

t receivers and NIST recommended security parameters size is shown in Table 6:

Table 5. Communication Overhead

Schemes	Communication Overhead	Classification
Proposed	$\|c\| + t\|c_i\| + \|h\| + \|n\|$	**Efficient**
[14]	$\|c\| + t\|c_i\| + \|h\| + t\|q\|$	Moderate Efficient
[13], [18]	$\|c\| + t\|c_i\| + t\|h\| + t\|q\|$	Moderate Inefficient
[15]	$\|c\| + t\|c_i\| + \|h\| + t\|p\|$	
[17]	$t\|c\| + \|h\| + \|q\|$	Inefficient

Table 6. % Saving in Communication Overhead

Number of Receiver	% Communication Overhead Reduction		
	[14]	[13], [18]	[15]
5	33.333	57.142	83.783
10	44.444	64.285	86.301
50	53.333	70	88.365
100	54.444	70.714	88.626

6. Conclusions

We proposed a novel Multi Receiver Signcryption Scheme based on Elliptic Curves for firewalls. It satisfies mandatory security attributes for Multi Receiver Signcryption. The scheme has a benefit of encrypted traffic authentication.It allows firewalls to verify the encrypted message without obtaining any secret parameter from the corresponding participants. The proposed scheme reduced computation cost from 31% to 67% and communication overhead 33% to 88% as compare to existing schemesfor multicast group containing receivers (5-100) with sufficient security parameters.

REFERENCES

[1]. Zheng, Y. (1997). Digital signcryption or how to achieve cost (signature & encryption)□ cost (signature)+ cost (encryption). In *Advances in Cryptology—CRYPTO□97* (pp. 165-179). Springer Berlin Heidelberg.

[2]. Jung, H. Y., Lee, D. H., Lim, J. I., & Chang, K. S. (2001). Signcryption schemes with forward secrecy. *Proceedings of WISA2001, Springer-Verlag*.

[3]. Hwang, R. J., Lai, C. H., & Su, F. F. (2005). An efficient signcryption scheme with forward secrecy based on elliptic curve. *Applied Mathematics and computation*, *167*(2), 870-881.

[4]. Gamage, C., Leiwo, J., &Zheng, Y. (1999, January). Encrypted message authentication by firewalls. In *Public Key Cryptography* (pp. 69-81). Springer Berlin Heidelberg.

[5]. Bao, F., & Deng, R. H. (1998, January). A signcryption scheme with signature directly verifiable by public key. In *Public Key Cryptography* (pp. 55-59). Springer Berlin Heidelberg.

[6]. Mohamed, E., &Elkamchouchi, H. (2009). Elliptic curve signcryption with encrypted message authentication and forward secrecy. *IJCSNS*, *9*(1), 395.

[7]. Iqbal, W., Afzal, M., & Ahmad, F. (2013). An efficient elliptic curve based signcryption scheme for firewalls. In *2013 2nd National Conference on Information Assurance (NCIA)* (pp. 67–72). IEEE. doi:10.1109/NCIA.2013.6725326

[8]. Toorani, M., & Beheshti, A. (2009, July). A directly public verifiable signcryption scheme based on elliptic curves. In *Computers and Communications, 2009. ISCC 2009. IEEE Symposium on* (pp. 713-716). IEEE.

[9]. Zheng, Y. (1998). Signcryption and its applications in efficient public key solutions. In *Information Security* (pp. 291-312). Springer Berlin Heidelberg.

[10]. Han, Y., Yang, X., & Hu, Y. (2004, November). Signcryption based on elliptic curve and its multi-party schemes. In *Proceedings of the 3rd international conference on Information security* (pp. 216-217). ACM.

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

[12]. Elkamchouchi, H. M., Emarah, A. A., & Hagras, E. (2007, November). A new efficient public key multi-message multi-recipient signcryption (PK-MM-MRS) scheme for provable secure communications. In *Computer Engineering & Systems, 2007. ICCES'07. International Conference on* (pp. 89-94). IEEE.

[13]. Elkamchouchi, H., Nasr, M., & Ismail, R. (2009, April). A New Efficient Multiple Broadcasters Signcryption Scheme (MBSS) for Secure Distributed Networks. In *Networking and Services, 2009. ICNS'09. Fifth International Conference on* (pp. 204-209). IEEE.

[14]. Han, Y., & Gui, X. (2009, May). Multi-recipient signcryption for secure group communication. In *Industrial Electronics and Applications, 2009. ICIEA 2009. 4th IEEE Conference on* (pp. 161-165). IEEE.

[15]. Li, H., Chen, X., Pang, L., & Shi, W. (2013). Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme. *PloS one*, *8*(6), e49141.

[16]. Brown, D. (2009). Standards for efficient cryptography, SEC 1: elliptic curve cryptography. *Released Standard Version*, *1*.

[17]. Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, *1*(1), 36-63.

[18]. Batina, L., Örs, S. B., Preneel, B., & Vandewalle, J. (2003). Hardware architectures for public key cryptography. *Integration, the VLSI journal*, *34*(1), 1-64.