J. Appl. Environ. Biol. Sci., 7(12)194-200, 2017

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

Multi-Receiver Signcryption Based on Hyper Elliptic Curve Crypto System

Anwar Sadat[1], Rashid Ahmad[2], Insaf Ullah[3], Hizbullah Khattak[4], Sultan Ullah[5]

[1] Institute of Information Technology, Kohat University of Science and Technology, Pakistan
[2] Department of Physics, Kohat University of Science and Technology, Pakistan
[3,4] Department of Information Technology, Hazara University Mansehra, Pakistan.
[5]Department of Information Technology University of Haripur, K-P, Pakistan

Received: June 23, 2017
Accepted: September 15, 2017

ABSTRACT

Multicast signcryption enable the originator of a message to generate a signcryp text and sends it to the multiple receivers. The existing schemes available in the literature usually have high computational cost and communication overheads. This is because all the existing schemes are based on RSA and Elliptic Curve having large key sizes. In this work, we have considered a multicast signcryption scheme based on hyper elliptic curve cryptosystem. The designed scheme is lightweight in nature because of hyper elliptic curve small parameters size. This hyper-elliptic curve cryptosystem (HECC) with 80 bits provide equal level of security as compared with other cryptosystems like RSA with 1024 bit, elliptic curve with 160 bit. Moreover, the designed scheme is efficient in terms of security e.g. it meets up confidentiality, authenticity, integrity, public verifiability, unforgeability, nonrepudiation's and forward security.
KEY WORDS: Signcryption, multicast signcryption, hyper elliptic curve.

1. INTRODUCTION

Data communication through unsafe networks puts the security of the data on high risk, furthermore, data communication always needs secrecy and authenticity. In old days, messages were encrypted before their transmission by generating a digital signature called signature-then-encryption mechanism. The mechanism used confidentiality and authentication in two different steps, which required more computation. Hence, to decrease computation Zheng [1] was the first who introduced the new mechanism called signcryption. It is a cryptographic mechanism that combines both digital signature and encryption in a single logical step. After this lot of signcryption mechanism were introduced [2, 3, 4, 5, 6, 7, 8, 9]. The main drawback of all these signcryption schemes is lack of a multicast communication. The concept of multi-receiver signcryption was first introduced by Zheng [10] in 1998. The multi-receiver signcryption scheme enables the sender of a message to generate signcryptext, and then send the same copy of signcryptext to a group of receivers. Multicasting is an efficient way to send a same message to multiple recipients with reduced cost of communication and computation. These characteristics make multicasts an idyllic technology for communication where a cluster of people get combined on the same task. Secure multicasting has applications for secure data transmission from a single source to multiple receivers (military command and control, distance education, real-time video conference). In 2000, Bellare for the first time formalized the concept of Public-key Encryption in a Multi-User Setting [11]. In 2004, Yiliang Han [3] proposed two multi-recipient signcryption schemes. There are now numbers of multi-receiver signcryption schemes available in the literature [12-23]. All these schemes have more computational cost and communication overhead which is always a major concern. On the other hand, the inherent distributing secret key problem can be solving by RSA algorithm but again the main disadvantage of RSA is its higher computational overhead and communication cast. Neal Koblitz [24] and Victor Miller in 1985 invented a new scheme to overcome this drawback of existing scheme called Elliptic Curve (EC). Elliptic curve provides new arithmetic field for cryptography to enhance security level. The Hyper-elliptic Curve Cryptosystem (HECC) with 80 bits provide an equal level of security as compared with other cryptosystems like RSA with 1024 bit, elliptic curve with 160 bit and other public key cryptosystems by using low resources. Therefore, to reduce computational and communication overhead recently Din et al [25] proposed a multi-receiver signcryption scheme based on an elliptic curve. However, the scheme still suffered from high computational cost and communication overhead. Thus to decrease costs (computational and communication) we designed and analyzed a multi-receiver signcryption scheme based on a hyper elliptic curve. The designed scheme provides all the security services of previous schemes and reduced in computational cost and communication overhead. Therefore, we explain the basics of hyper elliptic curve in the sub section 1.1.

Corresponding Author: Anwar Sadat, Institute of Information Technology, Kohat University of Science and Technology, Pakistan.

1.1. Preliminaries

Let q be a prime number, where $q \geq 2^{80}$ and F_q is a finite field of order q. Hyper Elliptic Curve C(Fq) of genus g ≥ 2 over finite field F_q be defined the following equation

$$C: y^2 + h(x)y = f(x) \bmod q$$

Where $h(x) \in F[x]$ is a polynomial and degree $h(x) \leq g$ where $g \geq 2$. $f(x) \in F[x]$ is a monic polynomial and *the* degree of $f(x) \leq 2g + 1$. Unlike points on the elliptic curve, the points on the hyper elliptic curve do not form a group. Divisor D is a finite formal sum of points on the hyper elliptic curve and represented in Mumford form as:

$$D = \big(u(x), v(x)\big) = \big(\sum_{i=0}^{g} u_i\, x^i\,, \sum_{i=0}^{g-1} v_i\, x^i\big)$$

Divisor form an Abelian group called Jacobian group $J_c(F_q)$ and the order of Jacobian group $o(J_c(F_q))$ is defined as

$$\left|\left(\sqrt{q} - 1\right)^{2g}\right| \leq o(J_c(F_q)) \leq \left|\left(\sqrt{q} + 1\right)^{2g}\right|$$

Definition: HECDLP

Let D be the divisor of order n in the Jacobian group$J_c(F_q)$, find an integerx $\in F_q$, such that:

$$D_1 = x.\, D$$

This paper is organized in the following way. In section 2, we define the proposed scheme, in section 3 the security analysis are performed, in section 4 computational cost analysis is done, and in section 5 communication overhead analysis is carried out. In second last, we have to light a paper in discussion part 6 and Conclusions are present in the last section 7.

2. Proposed Scheme

This section contains the mechanism for key generations of proposed scheme and the basic notations used in proposed scheme and signcryption and un-signcryption algorithm.

2.1. Key Generation

The signcrypter pick a random number $d_s, where\ 0 < d_s < n$ is a private key and compute there public key like $P_s = d_s.D$. In addition, the signcrypter pick a random number $d_{rT}, where\ 0 < d_{rT} < n$ is a private key and compute their public key like$P_{rT} = d_{rT}.D$.

2.2. Basic Notations

The following are the basic notations, which are used, in our proposed algorithm

- D is the Divisor of hyper elliptic curve
- m is the plaintext (message)
- S signifies signature for the plaintext (message)
- K_1, K_2 represents the secret keys
- $\mathcal{X}$, $\hbar$ shows the randomly selected numbers
- d_s is the private key of signcrypter
- $P_s = d_s.D$ is the public key of signcrypter
- d_{rT} is the private key of un-signcrypter
- $P_{rT} = d_{rT}.D$ is the public key of un-signcrypter
- T represents the receiver group
- $\mathcal{H}$ indicates the one-way hash function
- C_T represents a secret key for each receiver

2.3. Signcryption Phase

Algorithm

In this first step, multicast signcrypted text $(c,\ \hbar,\ S, c_1, \ldots c_t)$ will be generated by verifying each recipient public key by using their certificates.

1. Confirms P_{rT}
2. Select $\mathcal{X}$, where $0 < \mathcal{X} < n$

3. Split $\mathcal{X}= K_1 \& K_2$
4. Compute$\mathfrak{f} = \mathcal{H}(m)$.
5. Calculate $\mathcal{C} = \mathcal{E}_{\mathrm{K}_1}(m)$
6. Computing secrete key for receiver group T
   - Pick randomly $\mathfrak{k}$
   - Computes $\mathrm{K_T} = \mathfrak{k}.P_{rT}$
   - Generate $\mathrm{K_{eT}} = \mathcal{H}(\mathrm{K_T})$
   - Compute $\mathcal{C}_\mathrm{T} = \mathrm{E}_{\mathrm{K_{eT}}}(\mathcal{X})$
7. Computes $\mathcal{S} = d_s + \mathfrak{f}.\mathfrak{k}$
8. Computes $\mathcal{U} = \mathfrak{k}.\mathcal{D}$
9. Send $(\mathcal{C}, \mathcal{U}, \mathcal{S}, \mathcal{C}_1, \ldots \mathcal{C}_\mathrm{t})$ to the group

2.4. Unsigncryption Phase

Algorithm

In the second step, each recipient will receive the signcrypted text $(c, r, \mathrm{s}, \mathrm{c}_1, \ldots \mathrm{c}_\mathrm{t})$ through a multicast channel; and will get the plain text and will verify the sender public key P_s by using his certificate.

1. Confirms P_s
2. Calculates $\mathrm{K_T} = \mathcal{U}.d_{rT}$
3. Generate $\mathrm{K_{eT}} = \mathcal{H}(\mathrm{K_T})$
4. Compute $\mathcal{X} = \mathrm{D}_{\mathrm{K_{eT}}}(\mathcal{C}_\mathrm{T})$
5. Split $\mathcal{X}= K_1 \& K_2$
6. Calculate $m = D_{\mathrm{K}_1}(\mathcal{C})$
7. Compute$\mathfrak{f} = \mathcal{H}(m)$.
8. Computes $P_s = \mathcal{S}.\mathcal{D} + \mathfrak{f}.\mathcal{U}$

Theorem 1

The proposed scheme signcryption and Unsigncryption are supposed to be valid if sender party and the receiver party compute the following equation.

$\mathrm{K_T} = \mathcal{U}.d_{rT}$

Proof:

$\mathrm{K_T} = \mathcal{U}.d_{rT}$

$= \mathcal{U}.d_{rT} = \mathfrak{k}.\mathcal{D}\ .d_{rT}$

$= \mathfrak{k}.d_{rT}.\mathcal{D} = \mathfrak{k}.P_{rT}$=$\mathrm{K_T}$

hence proved

3. Security Analysis

In this section, we briefly discuss security analysis of the improved scheme. Our proposed scheme satisfies all the security services, which are discussed in [25].

3.1. Confidentiality

Our designed multi receiver signcryption scheme uses a secrete key for encryption of message m before sending to the multicast group. Suppose the adversary Д wants to gets the plain text m from cipher text $\mathcal{C}$ then Д needs a secret key $\mathcal{X}$. Therefore, Д calculates $\mathcal{C}_\mathrm{T}$ from equation (1), hence computing $\mathcal{C}_\mathrm{T}$ the adversary Д required $\mathrm{K_{eT}}$ from equation (2) and $\mathrm{K_T}$ from equation (3). Thus computing $\mathrm{K_T}$ is infeasible for the adversary Д and equals to solve the elliptic discrete logarithm hard problem. Hence, our designed scheme ensures the security requirement of confidentiality.

$$\mathcal{C}_\mathrm{T} = \mathrm{E}_{\mathrm{K_{eT}}}(\mathcal{X}) \quad (1)$$

$$\mathrm{K_{eT}} = \mathcal{H}(\mathrm{K_T}) \quad (2)$$

$$\mathrm{K_T} = \mathfrak{k}.P_{rT} \quad (3)$$

3.2. Integrity of Message

For the integrity property, our proposed scheme uses hash function of a message like equation (4) before sending. Suppose an adversary Д modifies in cipher text like as $\mathcal{C}'$ then the message is changed to m', Therefore $m \neq m'$ $\& \mathfrak{f} \neq \mathfrak{f}'$. Thus in our designed scheme, it is hard for Д to change as $\mathcal{C}'$ and $\mathfrak{f}$ as $\mathfrak{f}'$ because of one-way hash function collision resistance property. Moreover, the receivers group confirms the originality of plain text by using equation (5).

$$\mathfrak{f} = \mathcal{H}(m) \quad (4)$$
$$P_s = \mathcal{S}.\mathcal{D} + \mathfrak{f}.\mathcal{U} \quad (5)$$

3.3. Unforgeability

The designed multi-receiver signcryption scheme provides the security service of unforgeability. In our designed scheme, the adversary Д cannot compute a forged signature for message. Hence, if an adversary Д generates a forged signature like (6). Therefore, the adversary required d_s from equation (7) and $\mathfrak{k}$ from equation (8). Thus computing d_s and $\mathfrak{k}$ are equaling to solve a two-time elliptic curve discrete logarithm hard problem, which is computationally hard for Д.

$$\mathcal{S}' = d_s + \mathfrak{f}.\mathfrak{k} \quad (6)$$
$$P_s = d_s * \boldsymbol{\mathcal{D}} \quad (7)$$
$$\mathcal{U} = \mathfrak{k}.\mathcal{D} \quad (8)$$

3.4. Authenticity

Furthermore, our proposed scheme assures the security requirements of authentication. Therefore, in our designed scheme, the senders used their own private key by generating the signature. Hence, the receivers used equation (5) for authentication because of the sender private key associated with their public key.

3.5. Non-Repudiation

Moreover, in our designed scheme the sender cannot deny from the transmitted message to the receiver. Hence in the proposed scheme when dispute occur between sender and receivers group. Thus, the third party can easily prove its authenticity by using equation (5). Therefore, our proposed scheme provides non-repudiations property because the sender public and private keys are associated with each other.

3.6. Public Verifiability

Additionally, the designed scheme ensures a public verifiability property. Thus, in our designed scheme when the sender repudiates from the communicated message to the receiver then anyone can verify the message from the sender by using the following steps.

- Verify the public key of signcrypter P_s
- Compute $\ddot{Y} = \mathcal{S}.\mathcal{D} + \mathfrak{f}.\mathcal{U}$
- Compute $P_s = \ddot{Y}$

If the last step is holds then the message is from sender otherwise the message is not sent by the sender.

3.7. Forward Secrecy

Our designed scheme also provides forward secrecy property. This means that one of the sender private key is compromised; hence, the adversary Д still cannot recover the backward and forward messages.

4. Computational Cost Analysis

We compare our proposed scheme with Din [25] & Yang [21] and Han [16] schemes in terms of major operations. It is observed from [26] that the single modular exponential (MEX) take 220 ms and single elliptic curve multiplication take 83 ms. Therefore The generalized formula for reduction of computational cost is [27]:

$$\frac{\text{existing scheme} - \text{proposed scheme}}{\text{existing scheme}}$$

From this, we assume that if elliptic curve multiplication (ECDLP) consume 83 ms for single divisor multiplication, then hyper elliptic curve (HEDPM) consumes the half of elliptic curve such as 41.5 ms.

Table 1: Comparative computational cost analysis for T receiver

Participants	Din [25]	Yang [21]	Han [16]	Our scheme
Sender	T+1ECDLP	T +1 MEX	T +2 MEX	T+1 HEDPM
Receive	3 ECPM	3 MEX	2 MEX	3 HEDPM

Table 2: % Computational Time Reduction in term of ms

No of receivers	Din[25]	Yang [21]	Han [16]	Our scheme	Total reduction in % from Yang & Han	Total reduction in % from Nizam
5	747 ms	1980 ms	1980 ms	373.5 ms	81.13 %	50%
15	1569 ms	4180 ms	4180 ms	788.5 ms	81.13%	49.74%
25	2407 ms	6380 ms	6380ms	1203.5 ms	81.13%	50%

5. Communication overhead

Communication overhead analysis is based on the NIST recommended security parameters size such that: for RSA $|p| \geq 2^{1024}$ for ECC $|q| \geq 2^{160}, |\mathcal{C}_T'|$ *and* for HECC $|n| \geq 2^{80}$ $280, |h| = 160, |\mathcal{C}_T'| = 128$. The communication cost for proposed scheme is $|C| + T|\mathcal{C}_T'| + |h| + |n|$, Han [16] is $|C| + T|\mathcal{C}_T'| + |h| + T|p|$, yang [21] is $T|C| + T|h| + T|q|$*and Din et al* [25] *is* $|C| + T|\mathcal{C}_T'| + |h| + |q|$.

The generalized formula for reduction of communication cost is [27]:

$$\frac{\text{existing scheme} - \text{proposed scheme}}{\text{existing scheme}}$$

The communication overhead of proposed scheme is analyzed and compared with existing schemes in Table 3,4, while up to 72 % communication overhead decrease from Yang [21], Han[16] schemes and up to 8 % from Din et al [25] scheme.

Table 3: communication overhead

Multi receivers schemes	Communication overhead
Ours	$\|C\| + T\|\mathcal{C}_T'\| + \|h\| + \|n\|$
Din [25]	$\|C\| + T\|\mathcal{C}_T'\| + \|h\| + \|q\|$
Yang [21]	$T\|C\| + T\|h\| + T\|q\|$
Han [16]	$\|C\| + T\|\mathcal{C}_T'\| + \|h\| + T\|p\|$

Table 4: reduction in communication overhead

No of receivers	Din [25]	Yang [21]	Han [16]	Our scheme	Total reduction in % from yang	Total reduction in % from Han	Total reduction in % from Din
5	1024 +640 +160 +160 =1984 kb	5120 +800 +800 =6720 kb	1024 +640 +160 +5120 =6944 kb	1024 +640+80+80=1 824kb	72.85kb	73.73kb	8.06kb
15	1024 +1920 +160 +160 =3268 kb	15360 +2400+2 400=201 60kb	1024 +1920+1 60 +15360 =18464 kb	1024+1920+80 +80=3104kb	84.60kb	83.18kb	5.01kb

6. DISCUSSION

In literature a lot of public key infrastructure based multireciever signcryption schemes are available. All these schemes have more computational cost and communication overhead which is always a major concern. On the other hand, the inherent distributing secret key problem can be solving by RSA algorithm but again the main disadvantage of RSA is its higher computational overhead and communication cast. Neal Koblitz and Victor Miller in 1985 invented a new scheme to overcome this drawback of existing scheme called Elliptic Curve (EC). Elliptic curve provides new arithmetic field for cryptography to enhance security level. This paper proposed multi-receiver signcryption scheme based on the hyper elliptic curve. The Hyper-elliptic Curve Cryptosystem (HECC) with 80 bits provide an equal level of security as compared with other cryptosystems like RSA with 1024 bit, elliptic curve with 160 bit and other public key cryptosystems by using low resources.

We compare our proposed scheme with existing scheme [16, 21,25] in term of cost. The cost is further categorized to computational cost and communication overhead. The computational cost can be computed in term of major operations like modular exponentiation, elliptic curve point multiplication and hyper elliptic curve point multiplication. Table 1 shows Comparative computational cost analysis for T receiver in terms of major operation. As MEX represents modular exponential, ECDLP means elliptic curve multiplication and HEDPM represent hyper elliptic curve divisor multiplication. Table 2 shows Comparative computational cost analysis for 5, 15 and 25 receiver in terms of milli seconds. We investigate that MEX, ECDLP and HEDPM is high consuming operations in proposed and schemes in [16,21,25]. In average computational time, ECPM takes 83 ms and MEX take 220 ms under Infineon's SLE66CUX640P security controller [26]. For single divisor multiplication hyper elliptic curve (HEDPM) consumes the half of elliptic curve such as 41.5 Ms. Thus from table 2 we conclude that our proposed scheme decreases in computational cost from [16,21] is about 81.13 % and from [25] about 50%.

Communication overhead represents the extra bits transmitted during communication excluding original message. NIST recommended security parameters size such that: for RSA $|p| \geq 2^{1024}$ for ECC $|q| \geq 2^{160}, |\mathcal{C}_T'|$ *and* for HECC $|n| \geq 2^{80}$ $280, |h| = 160,$ $|\mathcal{C}_T'|$= 128. Table 3,4 shows the comparisons in terms of signcryptext size of [16, 21, 25] and proposed scheme for 5 and 15 receiver. The communication cost for proposed scheme is$|C| + T|\mathcal{C}_T'| + |h| + |n|$, Han [16] is$|C| + T\,|\mathcal{C}_T'| + |h| + T\,|p|$, yang [21] is $T|C| + T\,|h| + T|q|$ and Din et al [25] is $|C| + T\,|\mathcal{C}_T'| + |h| + |q|$. The generalized formula for reduction of communication cost is(existing scheme − proposed scheme)/(existing scheme). To be very clear the generalized formula of communication cost reduction from [21] of proposed scheme is$T|C| + T\,|h| + T|q| - |C| + T|\mathcal{C}_T'| + |h| + |n|)/(T|C| + T\,|h| + T|q|$, from[16] $|C| + T\,|\mathcal{C}_T'| + |h| + T\,|p| - |C| + T|\mathcal{C}_T'| + |h| + |n|)/|C| + T\,|\mathcal{C}_T'| + |h| + T\,|p|$ and from [25] $|C| + T\,|\mathcal{C}_T'| + |h| + |q| - |C| + T|\mathcal{C}_T'| + |h| + |n|)/|C| + T\,|\mathcal{C}_T'| + |h| + |q|$.
Thus the communication overhead comparisons is concluding from Table 3, 4, while up to 72 % communication overhead decrease from Yang [21], Han [16] schemes and up to 8 % from Din et al [25] scheme.

7. Conclusion

In this paper, we have proposed a new scheme namely multi-receiver signcryption scheme based on the hyper elliptic curve. The proposed scheme provides a scheme for the small resource devices e.g. mobile phone, PDA, Pager and sensors etc. because of the hyper elliptic curve small parameters size. Furthermore, the proposed scheme meets all the security requirements. Moreover, it reduces computational cost about 81.13 % from Yang [21], Han [16] and up to 50 % from Din [25]. It also decreases up to 72 % communication overhead from Yang [21], Han [16] schemes and up to 8 % from Din [25] scheme.

REFERENCES

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

[2] Y. Zheng, H.Imai, 1998. How to construct efficient signcryption schemes on elliptic Curves: Intl. J. Information Processing Letters 68(5): 227-233.

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

[4] R. J. Hwang, C.-H. Lai, and F.-F. Su, 2005. An efficient signcryption scheme with forward secrecy based on elliptic Curves, Journal of Applied Mathematics and Computation, 167(2): 870-881.

[5] Y. Han, X. Yang, P. Wei, Y. Wang, and Y. Hu, 2006. ECGSC: Elliptic Curves Based Generalized Signcryption Third International Conference on Ubiquitous Intelligence and Computing, Lecture Notes in Computer Science 4159 Springer, pp: 956-965.

[6] R. Tso, T. Okamoto, and E. Okamoto, 2008. ECDSA-Verifiable Signcryption Scheme with Signature Verification on the Signcrypted Message, Inscrypt 2007, LNCS 4990, pp: 11–24.

[7] M. Toorani, Ali Asghar Beheshti Shirazi, 2008. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic Curves, Proceedings of 2008 International Conference on Computer and Electrical Engineering (ICCEE'08), pp: 428-432.

[8] X. Wang, X. Yang and J. Zhang, 2010. Provable Secure Generalized Signcryption, Journal of Computers, 5(5): 807-814.

[9] Mohsen Toorani, Ali Asghar Beheshti Shirazi, 2010. Cryptanalysis of an Elliptic Curves-based Signcryption Scheme, International Journal of Network Security, 10(1): 51-56.

[10] . Zheng, 1998. Signcryption and its applications in efficient public key solutions, International workshop on Information Security, pp: 291-312.

[11] M. Bellare, A. Boldyreva, S. Micali, 2000. Public-key Encryption in a Multi-User Setting: Security Proofs and Improvements, Advances in Cryptology-Eurocrypt 2000, LNCS Vol. 1807, Springer-Verlag, pp: 259-274.

[12] Zheng, Shanyu, Manz, David, A. Foss, Jim, 2007. A communication-computation efficient group key algorithm for large and dynamic groups, International Journal on Computer Networks, 51(1): 69-93.

[13] Elkamchouchi, H. M., Emarah, A. A., & Hagras, 2007. A new efficient public key multi-message multi-recipient signcryption (PK-MM-MRS) scheme for provable secure Communications, IEEE International Conference on Computer Engineering & Systems, pp: 89-94.

[14] F. Li, X. Xin, and Y. Hu, 2008. Identity-based broadcast signcryption, Journal of Computer Standards & Interfaces, 30: 89-94.

[15] Elkamchouchi, H. M., Nasr, M. E., & Ismail, R., 2009. A new efficient publicly verifiable signcryption scheme and its multiple recipient's variant for firewalls implementation. IEEE Radio Science Conference, pp: 1-9.

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

[17] Pang, L. Jun, Cui and J. Jing, 2011. A new multi-receiver ID-based anonymous signcryption, Chinese journal of computer, 11: 2104-2113.

[18] Sanjeev, Agnihotri and U. Kumari, 2012. A multicasting scheme based on signcryption for dynamic groups, International Journal of Advancements in Technology, 3(3): 127-136.

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

[20] M. Jul, R. Sh, M. Sha, M. Ra, 2014. Secure group communication based on elliptic curve cryptography, International Journal of Transactions on Networks and Communication, 2(1): 1-26.

[21] 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, pp: 1042-1047.

[22] Waheed et al., 2016. Cryptanalysis and Improvement of Multi Recipient Signcryption Scheme. J. Appl. Environ. Biol. Sci., 6(4S): 157-161.

[23] Nizamuddin et al., 2016. A Novel Multi Receiver Signcryption Scheme Based on Elliptic Curves for Firewalls. J. Appl. Environ. Biol. Sci., 6(2S): 144-15.

[24] V. S. Miller, 2000. Use of Elliptic Curves in Cryptography, Advances in Cryptology: Proceedings of Crypto '85 Conference, 218, pp: 417-426.

[25] Din et al., 2016. An Efficient Multi Receiver Signcryption with Forward Secrecy Based on Elliptic Curves, J. Appl. Environ. Biol. Sci., 6(5): 28-33.

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

[27] Shehzad et al., 2012. Public Verifiable Signcryption Schemes with Forward Secrecy Based on Hyper elliptic Curve Cryptosystem. Intl. Conf. on information system, technology and management, pp: 135–142.