PLOS ONE

RESEARCH ARTICLE

# Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls

**Malik Zia*, Rashid Ali**

Department of Mathematics, Capital University of Science and Technology, Islamabad, Pakistan

* ziamalik199@gmail.com

## Abstract

In network security, firewall is a security system that observes and controls the network traffic based on some predefined rules. A firewall sets up a barrier between internal network and another outside unsecured network, such as the Internet. A number of signcryption schemes for firewall are proposed over the years, many of them are proved to have security flaws. In this paper, an elliptic curve based signcryption scheme for firewalls is analyzed. It is observed that the scheme is not secure and has many security flaws. Anyone who knows the public parameters, can modify the message without the knowledge of sender and receiver. The claimed security attributes of non-repudiation, unforgeability, integrity and authentication are compromised. After successful cryptanalysis of this scheme, we proposed a modified version of the scheme.





**Citation:** Zia M, Ali R (2018) Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls. PLoS ONE 13 (12): e0208857. https://doi.org/10.1371/journal.pone.0208857

**Editor:** Muhammad Khurram Khan, King Saud University, SAUDI ARABIA

**Received:** September 21, 2018

**Accepted:** November 24, 2018

**Published:** December 13, 2018



**Data Availability Statement:** All relevant data are within the paper.

**Funding:** The authors received no specific funding for this work.

**Competing interests:** The authors have declared that no competing interests exist.

## Introduction

In 1997 *Zheng* [1] introduced a new cryptographic scheme named Signcryption, which fulfills the functionalities of digital signature and encryption in a single logical step as shown in Fig 1. In traditional public key cryptography the process of both data encryption and authentication is achieved by first digitally signing the document and then encrypting the signed document for transmission over a public network (i.e, signature-then- encryption). It has two drawbacks of low efficiency and high computational cost. A Signcryption scheme reduces the computational cost as compared to signature-then- encryption scheme.

Encryption and digital signature are two basic security properties of any singcryption scheme. Such properties include integrity, non-repudiation, unforgeability and confidentiality. Forward secrecy and public verifiability are additional features that are provided depending upon the requirements.

Various signcryption schemes were introduced over the years, each scheme having its own benefits and drawbacks. In *Zheng's* signcryption scheme [1], the sender drives the secret key for symmetric encryption by using receivers public key. After receiving the signcrypted text, receiver gets the same secret key by using his private key. *Jung et al* [2] analysis shows that *Zheng* signcryption scheme [1] does not provide message confidentiality when the private key of sender is comporomised. He proposed a new signcryption scheme to overcome the drawbacks of *Zheng* [1] scheme with additional forward secrecy properity.

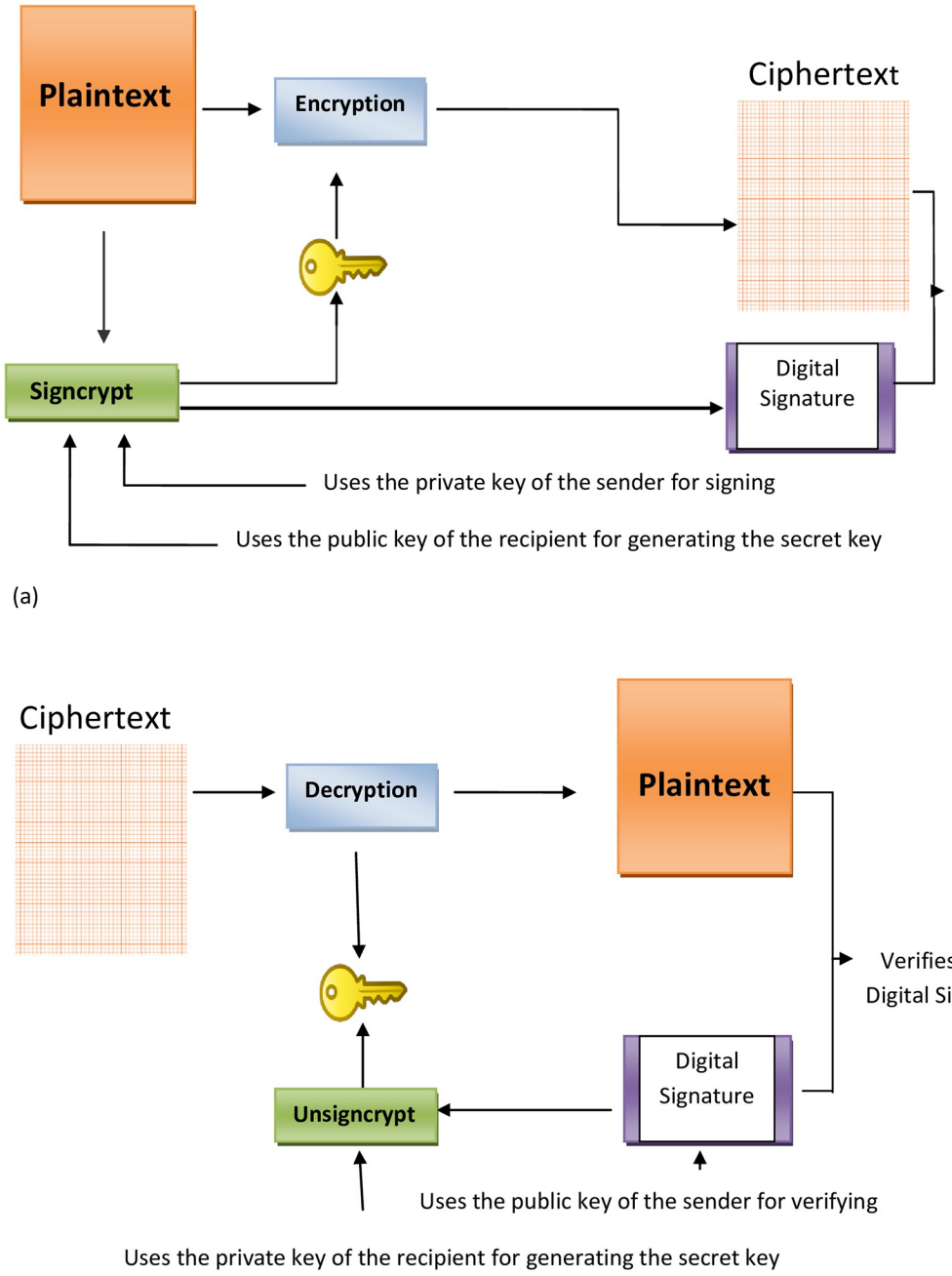


**Fig 1. Signcryption model.**

https://doi.org/10.1371/journal.pone.0208857.g001

Later on, *Bao and Dang* [3] modified *Zheng's* [1] scheme such that the judge can authenticate the signature without any use of recipient's private key. Gamage et al [4] modified *Zheng* [1] scheme so that anyone can authenticate the signature of the corresponding ciphertext. The proposed is based upon discrete logarithm problem (DLP) for firewalls authentications but does not provide multi-reciever functionality. *Boneh et al* [5] proposed a new aggregate signature scheme which reduces the size of certificate chains. If there are $n$ distinct messages and $n$ distinct users then aggregating all distinct $n$ signatures to a single short signature in such a way

that each user assures the authenticity of received message. The proposed scheme reduces the computational and communication cost as compared to single signature schemes. *Horng et al* [6] proposed an efficient certificate less aggregate signature scheme for vehicular sensor networks. The proposed scheme achieves the conditional privacy preservation and it is secure against existential forgery on adaptively chosen plaintext attack. Their scheme has less computational overhead as compared to existing aggregate signature scheme. *Toorani* and *Shirazi* [7] introduced a signcryption scheme based on elliptic curve with additional forward secrecy property. *Selvi* [8] introduced an identity based signcryption technique for multiple receivers by using bilinear pairing. For some recent authentication protocols and their applications, we refer to the work presented in [9]–[12].

Firewall is a security system that monitors the network traffic based on some rules. Some schemes are suitable for firewalls but each has its own drawbacks and limitations.

Recently, Iqbal et al [13] introduced a new efficient signcryption scheme based on elleptic curve for firewalls. They claim that their scheme is secure and no one can duplicate the original message. In this paper, our analylsis shows that the scheme proposed in [13] is not secure and has many security flaws.

This paper is organized as: First we present the signcryption scheme introduced by Iqbal et al [13], followed by the cryptanalysis section. The improvement and modification of the scheme of the scheme is described in the next section. Later, the security analysis of the modified scheme is discussed, followed by the conclusion section.

## Signcryption scheme of Iqbal et al

Recently, Iqbal et al [13] proposed a new signcryption scheme for firewalls. The proposed scheme is based on elliptic curve cryptography. An elliptic curve over a finite field $\mathbb{F}_p$ consists of the points satisfying the equation $y^2 = x^3 + ax + b \bmod p$, where $a$, $b$ belongs to $\mathbb{F}_p$ (the multiplicative group of integers mod $p$) along with a point $O$ at infinity. The entire security of elliptic curve cryptography is based upon elliptic curve discrete logarithm problem that is, given points $A$ and $B = nA$ on an elliptic curve, it is computationally hard to find the integer $n$. For details on elliptic curve cryptography we refer to [14].

The basic aim of their proposed scheme is to present a new signcryption scheme for firewalls. The authors claim that proposed scheme provides security attributes of integrity, message confidentiality, signature unforgeability, public verifiability, non-repudiation, and forward secrecy properity. Their analysis shows that proposed scheme is computationally efficient as compared to alraedy existing signcryption schemes. The scheme proposed by Iqbal et al [13] is described below.

**Global parameters** Both Alice and Bob agreed on the following parameters (Table 1).

**Algorithm 1**. The Iqbal et al [13] scheme is described in four phases given below:

**Table 1. Global parameters.**

| Variables | Description |
|---|---|
| $p^*$ | A large prime number, where $p^* > 2^{1024}$. |
| $E_{p^*}(a, b)$ | An elliptic curve over $GF(p^*)$. |
| $G$ | A base point $G$ of a group of a very large order $q$. |
| $H$ | A one way hash function. |
| $E$ and $D$ | Symmetric encryption and decryption algorithms. |
| $ID_i$ | Identifiers of sender and receiver from CA. |

https://doi.org/10.1371/journal.pone.0208857.t001

## 1. Key generation

- User A (Sender)
  - Selects an integer $n_A$ randomly as a private key such that $n_A < q$
  - Calculates public key as elliptic curve point $P_A = n_A G$
- User B (Receiver)
  - Selects an integer $n_B$ randomly as a private key such that $n_B < q$
  - Calculate his Public key as elliptic curve point $P_B = n_B G$

## 2. Signcryption

Suppose that Alice(sender) wants to transmit a message $m$ over a public network to Bob (receiver). First Alice checks the Bob,s certificate and verifies his public key $P_B$. She performs the following steps to send a signcrypted text.

1. Choose a random number $v$ from $[1, 2, 3. . ..q - 1]$.
2. Calculate $R = vG = (x_R, y_R)$.
3. Calculate $r = (v + n_A) \bmod q$.
4. Calculate $Q = rP_B = (x_Q, y_Q)$.
5. Calculate $k = H(x_Q||ID_A||y_Q||ID_B)$.
6. Calculate ciphertext $C = E_k(m)$ by using symmetric encryption $E_k$ with the secret key $k$.
7. Calculate $t = H(C||x_R||ID_A||y_R||ID_B)$.
8. Calculate $s = rt^{-1} \bmod q$.
9. Sends $(C, R, s)$ to reciever.

## 3. Signature verification by firewalls

This scheme enables firewalls to authenticate the signcrypted text $(C, R, s)$ without reading the contents of the original message. Firewalls verify the signature of Alice by using signcrypted text $(C, R, s)$. Only the ciphertext and public parameters are required to verify the signature unforgeability. Firewalls authentication consists of the following steps:

1. Receive $(C, R, s)$ from the sender.
2. Calculate the elliptic curve point as $P^* = (R + P_A)$.
3. Calculate $t = H(C||x_R||ID_A||y_R||ID_B)$.
4. Firewalls authenticate the message $m$ only if $stG = P^*$.

## 4. Unsigncryption

1. Recieve $(C, R, s)$ from sender.
2. Calculate the elleptic curve point $P^* = (R + P_A)$.

3. Calculate $Q = (n_B)P^* = (x_Q, y_Q)$.
4. Calculate $k = H(x_Q||ID_A||y_Q||ID_B)$.
5. Find the plaintext $m = D_k(C)$ by using symmetric encryption scheme with shared key $k$.
6. Calculate $t = H(C||x_R||ID_A||y_R||ID_B)$.
7. Accept the message $m$ only if $stG = P^*$.

## Cryptanalysis

In this section, Iqbal et al scheme [13] is cryptanalyzed. It is proved that the scheme has many security issues and weaknesses. Their scheme does not provide the message authenticity, unforgeability and non-repudiation. Mallory (an attacker) builds a new signcryption algorithm which generates the signcrypted text that is acceptable by unsigncryption algorithm. Suppose Mallory can intercept the network traffic between Alice and Bob and wants to generate a valid signcrypted text as described in Fig 2.

Mallory performs the following operations to transmit a message $m'$ of his choice.

### 1. Signcryption

1. Choose a random number $v'$ from $[1, 2, 3. . ..q - 1]$.
2. Calculate the elliptic curve point as $R' = v'G - P_A = (x'_R, y'_R)$.
3. Calculate the elliptic curve point as $Q' = v'P_B = (x'_Q, y'_Q)$.
4. Calculate the secret key as $k' = H(x'_Q||ID_A||y'_Q||ID_B)$.
5. Calculate the ciphertext $C' = E_k{}'(m')$ by using symmetric encryption scheme $E_k{}'$ with secret key $k'$.
6. Calculate the hash value as $t' = H(C'||x'_R||ID_A||y'_R||ID_B)$.
7. The signature parameter $s'$ is calculated as $s' = t'^{-1}v' \mod q$.
8. Mallory sends $(C', R', s')$ to Bob.

### 2. Signature verification by firewalls

1. Receive $(C', R', s')$ from sender.
2. Calculate the elliptic curve point as $P^* = (R' + P_A)$.
3. Calculate $t' = H(C'||x'_R||ID_A||y'_R||ID_B)$.
4. Firewalls authenticate the message $m'$ by verifying the relation $s't'G = P^*$.

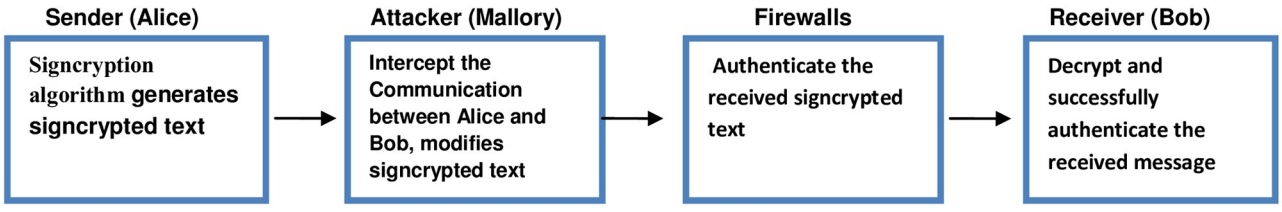


**Fig 2. Our cryptoanalysis model.**

https://doi.org/10.1371/journal.pone.0208857.g002

### 3. Unsigncryption

1. Bob receives the text $(C', R', s')$.
2. Calculate the elliptic curve point as $P^* = (R' + P_A)$
3. Calculate the elliptic curve point as $Q' = (n_B)P^* = (x'_Q, y'_Q)$
4. Calculate the secret key as $k' = H(x'_Q||ID_A||y'_Q||ID_B)$.
5. Find the plaintext $m' = D_{k'}(C')$ by using symmetric encryption scheme with secret key $k'$.
6. Calculate the hash value as $t' = H(C'||x'_R||ID_A||y'_R||ID_B)$.
7. Accept the message $m'$ by verifying $s't'G = P^*$.

In this way Mallory makes a fake signcrypted text of his choice and sends it to Bob. After receiving the signcrypted message $(C', R', s')$, first the firewalls successfully verifies the signature. Then at the receiver's end unsigncryption algorithm verifies the signcrypted text and then decrypts the message. Bob now believes that the message is sending by authentic person Alice. In this way Mallory, defeats the cryptosystem and now able to send any signcrypted text of his own choice.

### 4. Correctness

The same secret key $k'$ is generated by Mallory and Bob. The elliptic curve point $Q'$, which is used for generation of secret key $k'$, is same.

$$\begin{aligned} Q' &= (n_B)P^* \\ &= (n_B)(R' + P_A) && \text{(Step (2) Unsigncryption algorithm)} \\ &= (n_B)(v'G - P_A + P_A) && \text{(Step (2) Signcryption algorithm)} \\ &= (n_B)(v'G) \\ &= v'P_B = Q' \end{aligned}$$

After receiving the signcrypted text, unsigncryption algorithm correctly verifies the authenticity of received message.

$$\begin{aligned} s't'G &= (t'^{-1}v')(t'G) && \text{(Step (7) Signcryption algorithm)} \\ &= v'G \\ &= P^* \end{aligned}$$

Moreover, this scheme has no protection against Man-At-The-End (MATE) attack. For details on MATE attack, we refer to the work of Akhunzada et al [15] and the references their in.

## Modification and improvement of Iqbal et al scheme

Our analysis shows that the claimed security properties of Iqbal et al [13] scheme are compromised. We modifies the scheme to ensure the basic properties of security. In proposed scheme, the method to generate common secret key is very weak. We modify the key generation process so that only authentic sender and receiver can generate valid common key. In step (5) of signcryption algorithm 1, we replace $(ID_A, ID_B)$ to $(x_S, y_S)$ in key generation phase. In our improved scheme, Only authentic sender can generate the signcrypted text that is verified by

unsigncryption algorithm. In our improved scheme, global parameters and firwalls authentication is same as proposed by Iqbal et al [13].

**Algorithm 2**. Our modified signcryption scheme is described as:

## 1. Signcryption

1. Choose a random number $v$ from $[1, 2, 3. . ..q - 1]$.
2. Calculate $R = vG = (x_R, y_R)$.
3. Calculate $r = (v + n_A) \bmod q$.
4. Calculate $Q = rP_B = (x_Q, y_Q)$
5. Calculate $S = (n_A)P_B = (x_S, y_S)$.
6. Calculate $k = H(x_Q||x_S||y_Q||y_S)$.
7. Calculate the ciphertext $C = E_k(m)$ by using symmetric encryption $E_k$ with secret key $k$.
8. Calculate $t = H(C||x_R||ID_A||y_R||ID_B)$.
9. Calculate $s = t^{-1}r \bmod q$.
10. Sends $(C, R, s)$ to reciever.

## 2. Unigncryption

1. Recieve $(C, R, s)$ from sender.
2. Calculate the elleptic curve point as $P^* = (R + P_A)$.
3. Calculate $Q = (n_B)P^* = (x_Q, y_Q)$.
4. Calculate $S = (n_B)P_A = (x_S, y_S)$.
5. Calculate $k = H(x_Q||x_S||y_Q||y_S)$.
6. Find the plaintext message $m = E_k(C)$ by using symmetric encryption with secret key $k$.
7. Calculate $t = H(C||x_R||ID_A||y_R||ID_B)$.
8. Accept the message $m$ only if $stG = P^*$.

## 3. Correctness

The same secret key $k$ is generated by sender and receiver. The elliptic curve point $Q$ is used for key generation, which is same in Step(4) of signcryption and Step(3) in Unsigncryption algorithm.

$$\begin{aligned} Q &= n_B P^* = n_B(R + P_A) && \text{(Step (2) unsigncryption algorithm)} \\ &= n_B(vG + n_A G) && \text{(Step (2) Signcryption algorithm)} \\ &= (v + n_A)P_B && \text{(Key generation process)} \\ &= rP_B = Q && \text{(Step (4) Signcryption algorithm)} \end{aligned}$$

Receiver accept the message $m$ only if the following equation is verified by unsigncryption algorithm.

$$\begin{aligned} stG &= (t^{-1}r)tG && \text{(Step (9) Signcryption algorithm)} \\ &= rG = (v + n_A)G && \text{(Step (3) Signcryption algorithm)} \\ &= vG + P_A && \text{(Key generation process)} \\ &= R + P_A = P^* && \text{(Step (2) Unigncryption algorithm)} \end{aligned}$$

## Security analysis

The modified scheme provides the confidentiality of message. The common shared secret key $k$ is used for symmetric encryption and decryption which is only known to sender and receiver. The scheme ensures authentication, as it is certificate based. The validity of certificates is verified in signcryption and unsigncryption phases. Bob (receiver) can verify that the received message is not altered by Mallory (attacker). So our scheme provides message integrity. Without the knowledge of private key $k$ of Alice (sender), no one can generate the valid signcrypted text. Our scheme also provides signature unforgeability, non-repudiation, ciphertext-only authentication, public verification and forward secrecy of message confidentiality. The computational cost in signcryption, unsigncryption and signature verification phase is same as given in [13]. The communication cost of modified scheme is also same as in [13]. The comparison of modified scheme with the existing schemes is described in Table 2 below.

We now discuss some attack models for our improved signcryption scheme and give counter measures against these attacks.

### Man-At-The-End (MATE)attack

Previously Man-At-The-End (MATE) attack is neglected largely in security analysis by researchers because it is difficult to model, analyze and evaluate predominantly [15]. Since the attacker is human, therefore can utilize all the capabilities of a human mind. Beside the adversary has authorized and unlimited access to the device and this results in all security protections to stand up for an adversary for a specific period of time.

**Table 2. Comparision of our modified scheme with existing schemes.**

| Signcryption Scheme | C | I | U | N | P | A | F | F.S |
|---|---|---|---|---|---|---|---|---|
| Zheng [1] | yes | yes | yes | yes | no | no | no | no |
| Gamage [4] | yes | yes | yes | yes | yes | yes | no | yes |
| Bao and deng [3] | yes | yes | yes | yes | no | no | no | no |
| Jung et al [2] | yes | yes | yes | yes | no | no | yes | no |
| Elkamchochi [16] | yes | yes | yes | yes | no | no | no | no |
| Zheng and Imai [17] | yes | yes | yes | yes | no | no | no | no |
| Mohamed [18] | yes | yes | yes | yes | yes | yes | no | yes |
| Han et al [19] | yes | yes | yes | yes | no | yes | no | no |
| Hwang e t al [20] | yes | yes | yes | yes | no | yes | no | no |
| Zhou [21] | yes | yes | yes | yes | no | yes | no | no |
| Iqbal et al [13] | yes | no | no | no | yes | no | yes | yes |
| Our Modified Scheme | yes | yes | yes | yes | yes | yes | yes | yes |

C: Confidentiality, I: Integrity, U: Unforgebility, N: Non-repudiation, P: Public Verification, A: Authentication of ciphertext-only, F: Forward Secrecy, F.S: Firewall Suitability.

https://doi.org/10.1371/journal.pone.0208857.t002

The MATE attack has different forms depending upon the physical scenario of compromised device. At an individual level, altering attack is possible in which adversary altered the integrity of piece of software [22]. In reverse engineering attack, the adversary trace the intellectual property rights from the device software and then disrupts the privacy right of vendor [23]. Similarly, in cloning attack an adversary creates and issues the copies of software by vilating the copyright laws [24]. Sometime an adversary may attavk by crafting his own exploit code using the publicly available codes to make it hard to be reconised by an antivirus software [25].

Although MATE attack is difficult to analyze and model but there are mechanism to protect your device. The techniques to protect against MATE attack are: digital asset protection, software protection, hardware protection and hardware -based software protection. For further details on core protection mechanism against this attack we refer to [15].

### Man-In-The middle-attack

In man-in-middle attack, an adversary intercepts the network traffic between two parties and alter the information in such a way that both parties believes they are communicating with each other. The proposed Signcryption scheme of Iqbal et al is not secure against man-in-middle attack and an active attacker modifies the signcrypted text that is verified by unsigncryption algorithm.

Our modified Signcryption scheme overcome this security issue and resist against man-in-middle attack. Adversary get the signcrypted text ($C$, $R$, $s$) from publicly transmitted message but unable to modify the signcrypted message of his choice. The private key of Alice is used for key generation process in Step(5) of signcryption algorithm and then used for signature generation in Step (9) of signcryption algorithm. If attacker generates a signcrypted text with any fake key then unsigncryption algorithm will not be able to verify the signature in Step (8) of unsigncryption algorithem and hence the message $M$ will not be accepted.

## Conclusion

In this paper, the security of Iqbal et al [13] scheme is analyzed and it is proved that that it has many security flaws. In their proposed scheme, one can easily generate the signcrypted text of his choice that is acceptable by unsigncryption algorithm. Their scheme does not provide message authentication, integrity, non-repudiation and unforgeability as claimed in [13] (Table 1). We modified their scheme to ensure the compromised security attributes. Our improved scheme provides the security attributes of authentication, message confidentiality, unforgeability, integrity, non-repudiation, Public Verification, authentication of ciphertext-only, forward Secrecy and firewall Suitability. The comparison of the modified signcryption scheme with the existing schemes in the literature is highlighted in Table 2.

## Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

## Author Contributions

**Conceptualization:** Malik Zia, Rashid Ali.

**Formal analysis:** Malik Zia.

**Investigation:** Malik Zia.

**Methodology:** Malik Zia.

**Supervision:** Rashid Ali.

**Writing – original draft:** Malik Zia.

**Writing – review & editing:** Rashid Ali.

## References


1. Zheng Y. Digital signcryption or how to achieve Cost (Signature and Encryption) Cost (Signature) + Cost (Encryption), Advances in Cryptology-crypto 97, lncs 1294, Springer-Verlag, 1997. pp.165–179.
2. Jung HY, Chang KS, Lee DH, Lim JI. Signcryption schemes with forward secrecy. Proceeding of Information Security Application WISA 2001, pp. 403-475.
3. Bao F, Deng R. A signcryption scheme with signature directly verifiable by public key. Advances in Cryptology PKC 98, LNCS 1431, Springer Verlag 1998, pp.55–59.
4. Gamage C, leiwo J, Zheng Y. Encrypted message authentication by firewalls. International Workshop on Practice and theory in Public Key Cryptography (PKC-99), LNCS 1560, springer-verlag,march" 1999, pp.69-81.
5. Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. International Conference on the Theory and Applications of Cryptographic Techniques, Springer 2003, pp. 416-432.
6. Horng SJ, Tzeng SF, Huang PH, Huang, Wanga X, Li T, Li, Khan MK. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. Information Sciences, Elsevier 2015, pp. 48–66.
7. Toorani M, Beheshti AS. Cryptanalysis of an Elliptic Curve-based Signcryption Scheme. International Journal of Network Security 2010, Vol.10, No.1, PP.51–56.
8. Selvi S, Vivek S, Srinivasan R. An efficient identity based signcryption scheme for multiple receivers. International Workshop on Security, Springer, Berlin, Heidelberg 2009. pp. 71-88
9. Li X, Ibrahim MH, Kumari S, Sangaiah AK, Gupta V, Choo KK. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Computer Networks. 2017, p.p. 429–43.
10. Grindrod K, Khan H, Hengartner U, Ong S, Logan AG, Vogel D, Gebotys R, Yang J. Evaluating authentication options for mobile health applications in younger and older adults. PloS one. 2018 Jan 4; 13(1): e0189048. https://doi.org/10.1371/journal.pone.0189048 PMID: 29300736
11. Li X, Niu J, Bhuiyan MZ, Wu F, Karuppiah M, Kumari S. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things. IEEE Transactions on Industrial Informatics. 2018, p.p. 3599–3609. https://doi.org/10.1109/TII.2017.2773666
12. Li X, Peng J, Niu J, Wu F, Liao J, Choo KKR, A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things. IEEE Internet of Things Journal 2018, Vol. 5: p.p 1606–1615 https://doi.org/10.1109/JIOT.2017.2787800
13. Iqbal W, Afzal M, Ahmad F. An Efficient Elliptic Curve Based Signcryption Scheme for Firewalls. 2nd National Conference on Information Assurance (NCIA) 2013, ISBN: 978-147991288-9, IEEE Computer Society.
14. Stallings W. Cryptography and Network Security. Prentice Hall 2000, 4th Edition.
15. Akhunzada A, Sookhak M, Anuar NB, Gani A, Ahmed E, Shiraz M, Furnell S, Hayat A, Khan MK. Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions. Journal of Network and Computer Applications, Elsevier 2015. Vol.48 pp. 44–57 https://doi.org/10.1016/j.jnca.2014.10.009
16. Elkamachouchi HM, Nasr ME, Ismail R. A New Efficient publicly Verifiable Signcryption Scheme and its Multiple Recipients Variant for Firewalls Implementation. IEEE 26th National Radio science conference 2009, pp.1-9.
17. Zheng Y, Imai H. How to construct efficient signcryption schemes on elliptic curves. Information processing letters (68) 1998, p.p 227–233.
18. Mohammad E, Elkamchouchi HM. Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy. International Journal of Computer Science and Network Security 2009, Vol 9 No 1 pp.395–398.

19. Han Y, Yang X, Yiliang H, Xiaoyuan Y, Ping W, Yuming W, Yupu H. Elliptic curve based generalized signcryption. International Conference on Ubiquitous Intelligence and Computing Springer 2006, pp. 956-965
20. Hwang RJ, Lai CH, Su F. An Efficient signcryption scheme with forward secrecy based on elliptic curve. Applied mathematics and computation 2005, 870–881. https://doi.org/10.1016/j.amc.2004.06.124
21. Zhou X. Improved Signcryption Scheme with public Verifiability. Knowledge Engineering and software Engineering, 2009, KESE 09, Pacific-Aisa Conference on, PP.178-181.
22. Falcarin P, Collberg C, Atallah M, Jakubowski. Guest editors:introduction software protection. IEEE Software 2011, Vol no 28,PP. 24–27. https://doi.org/10.1109/MS.2011.34
23. Tang M, Qiu Z, Li W, Sun W, Hu X, Zhang H. Power analysis based reverse engineering on the secret round function of block ciphers. Concurrency and Computation: Practice and Experience. 2014; Vol. 26 (8): pp. 1531–1545 https://doi.org/10.1002/cpe.3068
24. Shan Z, Cao H, Lv J, Yan C, Liu A. Enhancing and identifying cloning attacks in online social networks. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication 2013. ACM, ISBN: 978-1-4503-1958-4
25. Svensson G. Auditing the human factor as a part of setting up an information security management system. Dissertation: Master Thesis. Available from: http://urn.kb.se/resolve, 2013.