MATEMATIKA, 2019, Volume 35, Number 1, 1–11

An Efficient and Authentication Signcryption Scheme Based on Elliptic Curves

[1]Manoj Kumar and [2]Pratik Gupta*

[1]Department of Mathematics and Statistics
Gurukula Kangri Vishwavidyalaya Haridwar (Uttrakhand) 249404, India

[2]School of Basic Science,
Jaipur National University, Jaipur 302017, India

*Corresponding author: pratikgupta1810@gmail.com

Article history
Received: 28 November 2017
Received in revised form: 19 April 2018
Accepted: 29 April 2018
Published on line: 1 April 2019

Abstract Signcryption schemes are compact and specially suited for efficiency-critical applications such as smart card dependent systems. Several researchers have performed a large number of significant applications of signcryption such as authenticated key recovery and key establishment in one small data packet, secure ATM networks as well as light weight electronic transaction protocols and multi-casting over the internet. In this paper we propose an efficient and authentication scheme of signcryption symmetric key solutions, using elliptic curves by reducing senders computational cost. It needs two elliptic curve point multiplication for sender and comparative study of computational cost for sender and recipient as well as there is no any inverse computation for sender and recipient. This makes it more crucial than others.

Keywords Elliptic curve; signcryption; digital signature; authentication; cryptographic nonce.

Mathematics Subject Classification 94A60, 14G50

1 Introduction

Two essential components of cryptography that can provide secure and authenticated communications, are encryption and digital signature. Based on the above terminology, the conventional schemes that prevent forgery and ensure confidentially of a message in public key cryptography, can be classified into following classes:

(i) Signature -and- encryption (SAE)
(ii) Encryption -then- signature (ETS)
(iii) Signature -then- encryption (STE)

The first two approaches are insecure in some situations. Although last one method is suitable composition, but it consumes high communication and high computational cost in implementation. Signcryption is an alternative approach for STE method to reduce the computation and communication costs. In 1997, Zheng [1] was introduced the concept of signcryption which is more secure and efficient than conventional method. Signcryption is function of encryption and digital signature in a single logical step. In brief, a STE approach can be explained as:

(i) Sender of message, uses DSA to sign the message.

(ii) Using symmetric encryption algorithm sender encrypts the message and signature with a randomly chosen message encryption key.

(iii) Using asymmetric encryption algorithm, sender encrypts the randomly chosen message encryption key.

(iv) Finally sender, sends the encrypted digitally signed message and encrypted randomly chosen message encryption key to the reciever.

A converse process is run at the receiver. This scheme can be presented in Figure 1. (S,U) is

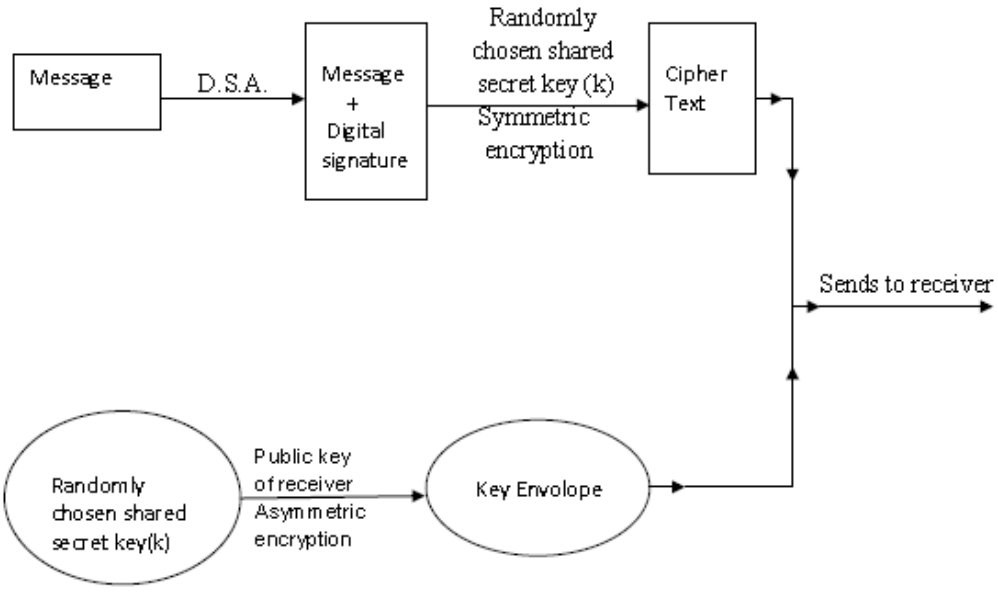


Figure 1: Signature-then-encryption Scheme.

a polynomial time algorithm consist in signcryption scheme [2] where S stand for signcryption algorithm which is probabilistic and U is unsigncryption algorithm which is deterministic. A signcryption scheme satisfy the following condition:

(i) Unique unsigncryptabilty - Given a message m of arbitrary length, the algorithm S signcrypts m and outputs a signcrypted text c. On input c, the algorithm U unisgncrypts c and recovers the original message un-ambiguously.

(ii) Security - (S,U) security is another quality of secure digital signature scheme that keeps confidentiality of message contents, unforgeability and non-repudiation.

(**iii**) **Efficiency** - The computational cost includes the computational time (that contain signcryption and unsigncryption) and the communication overhead, the scheme is comparability smaller than STE schemes parameters.

Diagrammatically a signcryption scheme can be described by Figure 2. Signcryption schemes

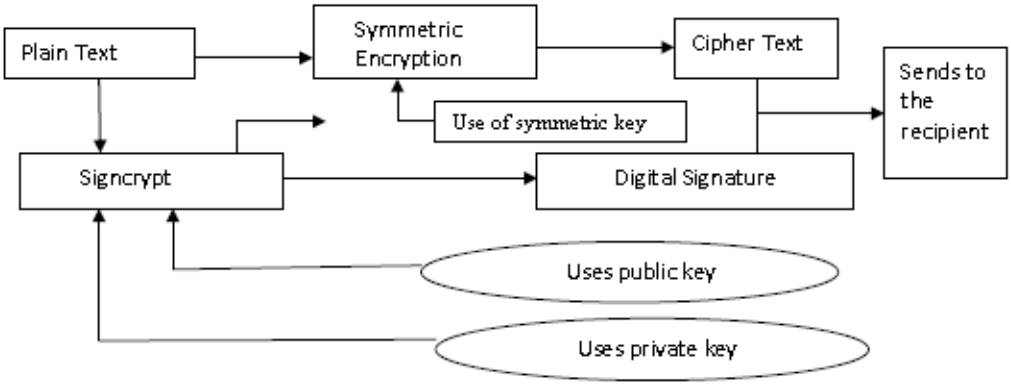


Figure 2: Signcryption Scheme

are compact and specially suited for efficiency-critical applications such as smart card dependent systems. Several researchers have performed a large number of significant applications of signcryption such as authenticated key recovery and key establishment in one small data packet [3], secure ATM networks [4] as well as light weight electronic transaction protocols [5] and multi-casting over the internet [6]. In the present paper we proposed an efficient signcryption scheme for symmetric key solutions, using elliptic curves. Organization of rest of the present paper is as follows: section two surveys the parallel work related to signcryption. Section three describes a brief mathematical background of ECC. Section four describes signcryption scheme using a nonce based on elliptic curves. In section five we use our signcryption scheme for key establishment. Section six analyses security of the proposed scheme. The paper is closed by section seven where we compared our proposed scheme with existing STE schemes.

2 Parallel Work

The history of cryptography defines the level of developments on it. But it is not for the use of common purpose. Now a days it developed in many terms like signcryption which is the most authentic one in the world of security. Some signcrption researches are based on modular exponential while others are based on elliptic curves. [7–10]. The first signcryption cryptography technique was proposed in 1997 by Zheng [1]. To get the authenticity and confidentiality features of cryptography he combines the features of digital signature and encryption algorithm which is based on discrete logarithmic problem. The drawback of Zheng signcryption scheme was that the judge can verify signature without the recipient privte key but the process of verification need key exchange protocol that was modified by Bao and Deng [11]. Zheng signcryption scheme can not be verified publically and Jung et al. [12] shows that it does not provide forward secrecy of message confidentiality when the sender's private key disclosed rather Gamage et al. [13] enhanced it can be verify the signcryption of cipher text publically.

Zheng and Imai [2] suggested an ECC based signcryption scheme thus providing all the basic security features, with cost less than as required by STE. ECC has smaller key size with respect to other scheme which is an advantage over the difficulty of ECDLP but still it needs forward secrecy. Toorani et al. [14] comes with new feature of signcryption scheme based on ECC which provide all the security attributes but this scheme comparability takes more computational time. Now our aim is to provide a new efficient scheme that will have low communication cost and less computational time as well as gives message authentication, forward secrecy and public verification. That is lacking in signcryption scheme stated above.

3 Mathematical Background of ECC

In this section first we discuss some essential arithmetic of elliptic curves (which are necessary to understand the proposed scheme). Although a lot of literature exist on arithmetic of elliptic curves [15], a simple and easier arithmetic of elliptic curves is given by the following [16]:
An elliptic curve $E(F_p)$ over a finite field F_p is defined by the parameters $a, b \in F_p$ (a and b satisfy the relation $4a^3 + 27b^2 \neq 0$), consists of the set of points $(x, y) \in F_p$, satisfying the equation $y^2 = x^3 + ax + b$. The set of points on $E(F_p)$ also include a point O, which is the point at infinity serve as the identity element under addition. Actually elliptic curve are not ellipse. They are so called because they are described by cubic equations similar to those are used for calculating the circumference of an ellipse. The Addition operation is defined over $E(F_p)$ and it can be seen that $E(F_p)$ forms an abelian group under addition [operation] and Geometrically, the addition of two distinct points and doubling of a point on an elliptic curve is described by Figure 3 and Figure 4.

- $P + O = O + P$ for all $P \in E(F_p)$.
- If $P = (x, y) \in E(F_p)$, then $(x, y) + (x, -y) = O$. (The point $(x, -y) \in E(F_p)$ and is called the negative of P and is denoted $-P$).
- If $P = (x_1, y_1) \in E(F_p)$ and $Q = (x_2, y_2) \in E(F_p)$ and $P \neq Q$, then $R = P + Q = (x_3, y_3) \in E(F_p)$, where $x_3 = \lambda - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$, and $\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)}$.

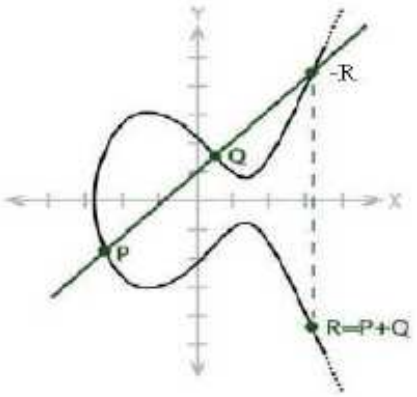


Figure 3: Addition of Two Points P and Q.

- Let $P = (x, y) \in E(F_p)$. Then the point $Q = P + P = 2P = (x_1, y_1) \in E(F_p)$, where $x_1 = \lambda^2 - 2x, y_1 = \lambda(x - x_1) - y$, and $\lambda = \frac{(3x^2+a)}{2y}$.

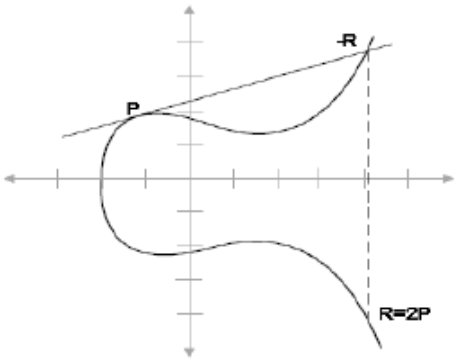


Figure 4: Doubling of a Point P, $R = 2P$.

4 Signcryption Schemes Using a Nonce Based on Elliptic Curve Cryptography

Before describing our proposed scheme, we first mention some important notations which are very helpful to understand our scheme.

q - a large prime number $> 2^{160}$.

a, b - two integer elements which are samaller than q and satisfy $4a^3 + 27b^2 mod q \neq 0$

F - the selected elliptic curve over finite field q *i.e.* $F = \{(x, y) : y^2 = (x^3 + ax + b) mod q\} \cup \{O\}$

O - a point of F at infinity.

G - a base point of order n, on elliptic curve F.

n - a prime number greater than 2^{160} satisfying $n \times G = O$.

Hash - a one-way hash function.

$E_{k_1}(.)/D_{k_1}$ - symmetric encryption/decryption algorithm with private key k_1 such as DES or AES.

N_B - cryptographic nonce

$\{0, 1\}^{l_n}$ - size of bits

l_n - Length of bits

The user A randomly selects an integer $d_A < n$ as his/her private key and computes public key $e_A = d_A \times G$. The user B also selects private key d_B and computes public key $e_B = d_B \times G$.

Assume that Alice wants to send a message m to Bob. Alice generates digital signature (R, s) of message m and uses the symmetric encryption algorithm and secret key k_1 to encrypt m. Let c be cipher text. Alice generates the signcrypted text (R, s, c) as in the following Figure 5.

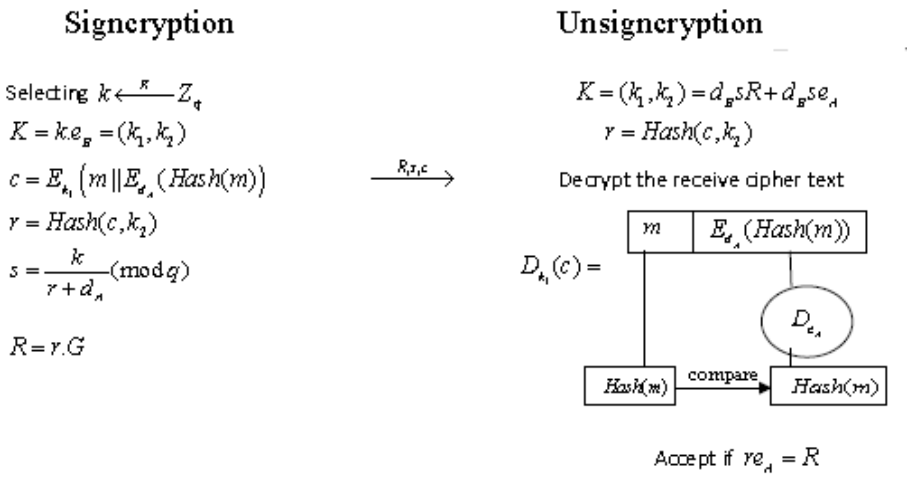


Figure 5: The Proposed Scheme

5 Key Establishment Using Signcryption Based on Elliptic Curve Cryptography

In this phase, some public parameters (discussed in previous section) are generated. Now, key exchange between user A and user B can be described as follows:

(i) User B chooses a randomly cryptography nonce N_B and sends to User A.

(ii) User A chooses randomly K_A and t.

(iii) User A generates digital signature (r, s) of message m and uses the symmetric encryption algorithm and secret key k_1 to encrypt m. Let c be the cipher text. User A generates the signcrypted text (c, r, s) as in the following Figure 6:

6 Security Analysis of the Proposed Scheme

The security analysis is studied with respect to the security components which the proposed algorithm should satisfy. Boneh and Lipton [17] describes that two problems(ECDLP and ECDHP) are equivalent when best algorithm for ECDLP is fully exponential computational time complexity. These two problems can be explained as follows:

The Elliptic Curve Discrete Logarithm Problem (ECDLD): Suppose F is an elliptic curve over q and $P, Q \in F$. Given a multiple Q of P,the elliptic curve discrete log problem is to find $t \in Z$ such that $tP = Q$. It is computationally infeasible to generate t from P and Q [18].

The Elliptic Curve Diffie-Hellman Problem (ECDHP): Suppose F is an elliptic curve over q. Given $P, Q \in F$ such that $P = c.G$ and $Q = d.G$ where G is base point of F, the elliptic curve diffie-Hellman problem is to find $t \in Z$ such that $t = c.d \times G$. It is assumed computationally infeasible problem [19].

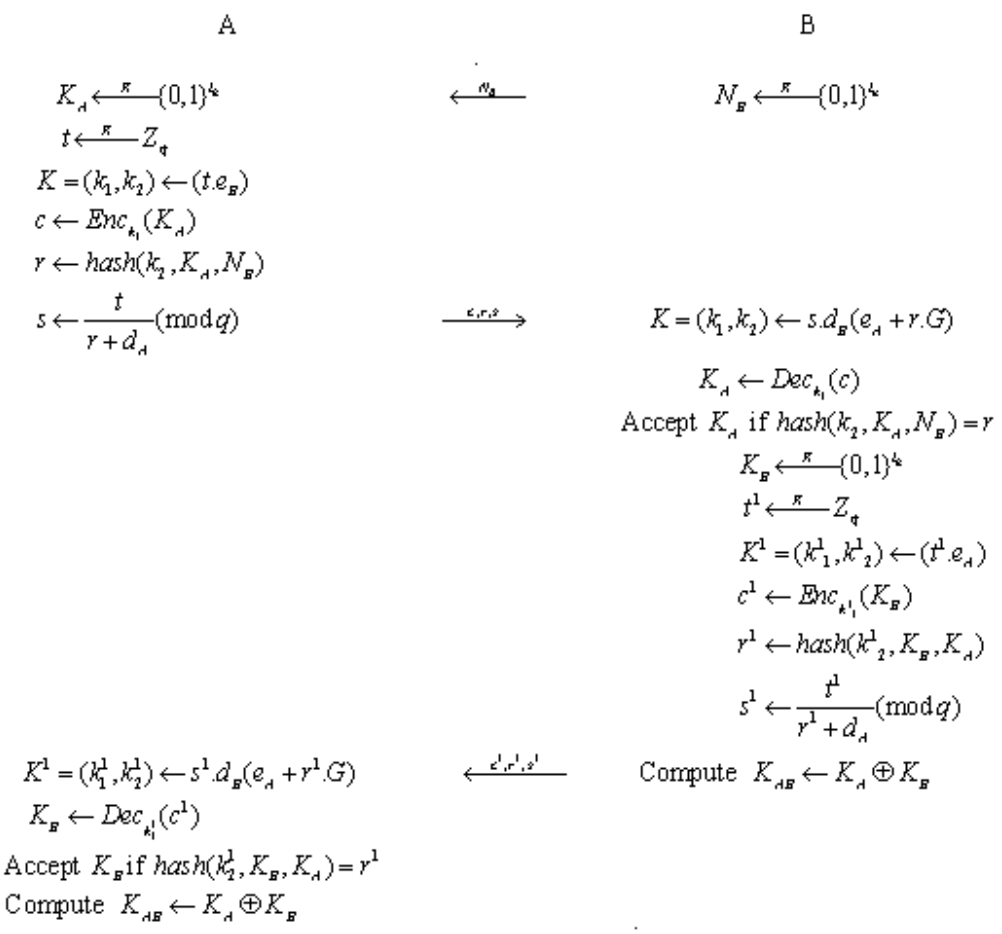
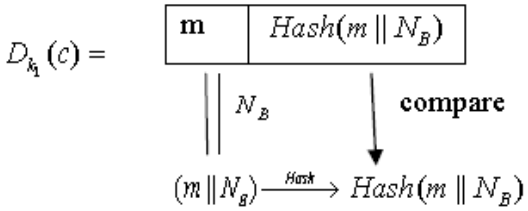


Figure 6: Key Exchange Protocol

The security components of the security analysis is to be studied as follows:

- **Confidentiality.** Confidentiality is a process of securing the message content from unauthorized parties. In our proposed scheme, if eavesdropper wants to derive the secret key k_1 which is the x-coordinate value of point K. It is quite infeasible for eavesdropper to solve it because possible ways to generate secret key k_1 is equal to solve the ECDLP or ECDHP problems.
- **Authentication.** Authentication is a process of verification which identify the authenticate user through certain verification method. The authentication property is made sure by the following compare of $Hash$ value



If the comparison evaluates to be true, the proposed scheme provides the authentication of the sender identity and the transmitted message.

- **Integrity.** Integrity is a process of maintaining the data that must not be changed by unauthorized person during in transit. In our scheme, getting $r = Hash(c, k_2), s = rd_Ae_B + K$ of the signcryption phase. If the message content is changed the ciphertext C is changed to C^1, the related message changed to M^1. By the property of one-way hash function, it is computationally infeasible. This changed is detected at time of verification and the message gets rejected. So the integrity of the other message is confirmed.
- **Unforgeability.** In our scheme, dishonest Bob is the most powerful attacker to forge a signcrypted message, because he is the only person who knows the private key d_B which is required to directly verify a signcryption from Alice. Given a signcrypted text (R, s, c) Bob can use his private key d_B to decrypt the cipher text c and obtain (R, s, m). As we know ECDSA is unforgeable against adaptive attack. Hence it is unforgeable.
- **Non-repudiation.** Non-repudiation is the assurance that someone can not deny something. In this case of denial by sender regarding the sending of the message, recipient can send (R, s, c) required by the judge to verify. In Judge Verification phase, the judge can determine the signature is generated by the sender if equation $(k_1, k_2) = s - d_BR$ holds. Then it ensure the property of non-repudiation.
- **Forward secrecy.** An adversary that obtains d_A will not be able to decrypt past messages. Previously recorded values of (R, s, c) that were obtained before the compromise cannot be decrypted because the adversary that has d_A will need to calculate d_B to decrypt. Calculating d_B requires solving the ECDLP, which is computationally infeasible [20].
- **Public verification.** Verification requires knowing only Alice's public key. All public keys are assumed to be available to all system users through a certification authority or a public directory. For the proposed scheme an interactive zero knowledge key exchange protocol is needed.

Our proposed scheme security analysis compared to other signcryption shemes is summarised in Table 1.

Table 1: The Security Analysis of Different Signcryption Schemes

S/S	**COF**	**IN**	**UNF**	**NR**	**FC**	**PV**
Zheng [1]	Yes	Yes	Yes	Another	No	No
Zheng and Imai [2]	Yes	Yes	Yes	Another	No	No
Bao and Deng [11]	Yes	Yes	Yes	Directly	No	Yes
Gamage *et al.* [15]	Yes	Yes	Yes	Directly	No	Yes
Jung *et.al.* [12]	Yes	Yes	Yes	Another	Yes	No
Toorani *et. al.* [14]	Yes	Yes	Yes	Directly	Yes	Yes
Our scheme	Yes	Yes	Yes	Directly	Yes	Yes

S/S: Singcryption/Schemes; COF: Confidentiality; IN: Integrity; UNF: Unforgeability; NR: Non-Repudation; FC: Forward Secrecy; PV: Public Verification.

7 Conclusion and Cost Analysis of the Proposed Scheme

The Table 2 shows the comparative analysis of computational cost of different signcryption schemes. We try to reduce senders computational cost.It is more efficient than the others. The elliptic curve multiplication only needs 83ms and the modular exponentiation operation needs 220ms for average computational time in the Infineons SLE66CUX640P security controller [12]. The most computational time for elliptic curve multiplication and modular exponentiation operation for various schemes proposed by different researchers, is showed in Table 3.

This paper introduces using elliptic curves nonce based singncryption schemes for secure and authenticated message delivery, which fulfills all the functions of digital signature and encryption with a cost less than that required by the current standard STE method.

Table 2: Comparative Analysis of Computational Cost of Different Sigcryption Schemes

Signcryption schemes	**Participants**	**EXP**	**DIV**	**ECPM**	**EXPA**	**MUL**	**ADD**	**KH(.)**
Zheng [1]	Alice	1	1	-	-	-	1	2
	Bob	2	-	-	-	2	-	2
Zheng and Imai [2]	Alice	1	1	-	-	-	1	2
	Bob	2	-	-	-	2	-	2
Bao and Deng [11]	Alice	1	1	-	-	-	1	2
	Bob	2	-	-	-	2	-	2
Gamage *et al.* [11]	Alice	1	1	-	-	-	1	2
	Bob	2	-	-	-	2	-	2
Toorani *et al.* [14]	Alice	1	1	-	-	-	1	2
	Bob	2	-	-	-	2	-	2
Our scheme	Alice	1	1	-	-	-	1	2
	Bob	2	-	-	-	2	-	2

ECPM = the number of elliptic curve point multiplication operation. ECPA = the number of elliptic curve point addition operation. EXP = the number of modular exponentiation operation. DIV = the number of modular division (inverse) operation. MUL = the number of modular multiplication operation. ADD = the number of modular addition operation. KH(.)= the number of one-way or keyed one-way hash function operation.

As it is obvious from the bar-graph in Figure 7, computational time of our scheme is slightly greater than Zheng and Imai scheme but from the security view of the point our proposed scheme is more secure than Zheng and Imai scheme (see Table 1 in section 6).

Acknowledgments

This research work is supported by University Grant commission (UGC), New Delhi, India, under the Junior Research Fellowship scheme. Authors are thankful to the referees for their precious comments and suggestions, which are really help us to improve the quality of this article.

Table 3: Average Computational Time (in ms) of Major Operations of Different Signcryption Schemes

Signcryption Schemes	**Sender Computational Time(ms)**	**Recipient Computational Time(ms)**
Zheng [1]	$1 \times 220 = 220$	$2 \times 220 = 440$
Zheng and Imai [2]	$1 \times 83 = 83$	$2 \times 83 = 166$
Bao and Deng [11]	$2 \times 220 = 220$	$3 \times 220 = 660$
Gamage *et al.* [15]	$2 \times 220 = 440$	$3 \times 220 = 660$
Toorani *et al.* [14]	$2 \times 83 = 166$	$4 \times 83 = 332$
Our scheme	$2 \times 83 = 166$	$2 \times 83 = 166$

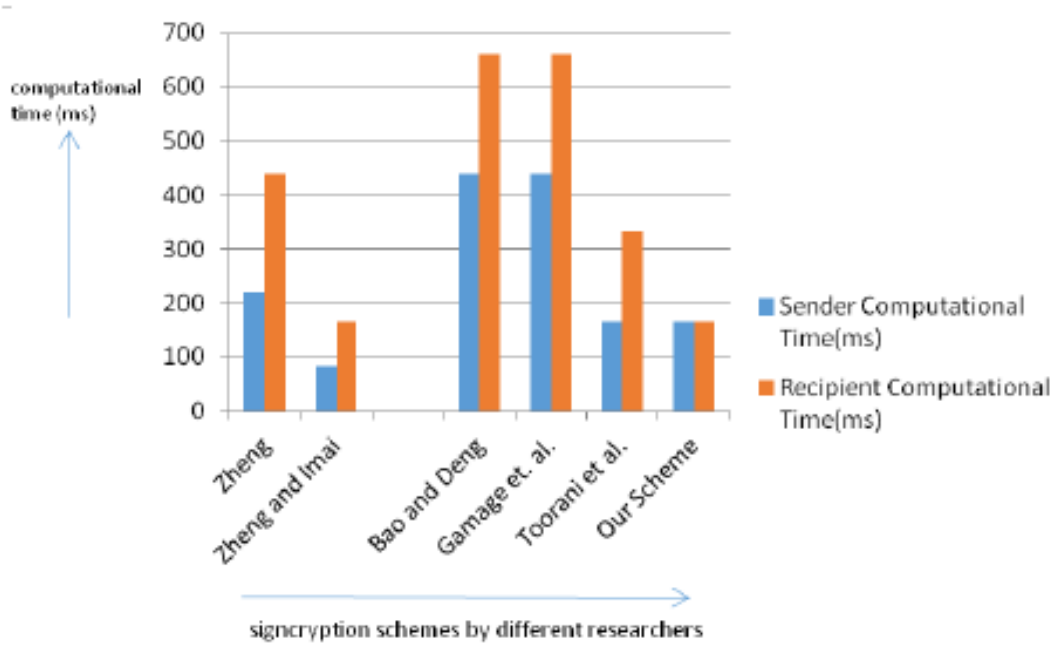


Figure 7: Bar Graph Between Average Computational Time and Different Proposed Signcryption Schemes

References

[1] Zheng, Y. Digital signcryption or how to achieve Cost (Signature and Encryption) Cost (Signature) + Cost (Encryption). *Advances in Cryptology. Springer-Verlag.* 1997.

[2] Zheng, Y. and Imai, H. How to construct efficient signcryption schemes on elliptic curves. *Information Processing Letters* . 1998. 227-233.

[3] Zheng, Y. and Imai, H. Compact and unforgeable session key establishment over an ATM network. *In proc. IEEE INFOCOM.* 1998. 411-418.

[4] Carnage, C., Leiwo,J. and Zheng, Y. A block-based approach to secure ATM networking.

1997.

[5] Hanaoka, G., Zheng, Y. and Imai H. A light-weight secure electronic transaction protocol. *Lecture Notes in Comput. Sci.,Springer-Berlin*. 1998. 215-226.

[6] Matsuura, K., Zheng, Y. and Imai H. Compact and flexible resolution of cbt multicast key-distribution. *Lecture Notes in Comput. Sci.,Springer-Berlin*. 1998. 190-205.

[7] Zheng, Y. and Enos, G. An ID-based signcryption scheme with compartmented secret sharing for unsigncryption. *Information processing letters*. 2014.

[8] Yanwei, Z., Bo, Y. and Wenzheng, Z. Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing. *Discrete applied mathematics*. 2017.

[9] Rao, Y. Attribute-based online/offline signcryption scheme. *John wilay and sons*. 2017.

[10] Song, Y., Li, Z. and Li, J., Attribute-based signcryption scheme based on linear codes, *Information Sciences*. 2017.

[11] Bao, F. and Deng, R.H. A signcryption scheme with signature directly verifiable by public key. In *Proceedings of PKC, Springer-Verlag*. 1998. 55-59.

[12] Jung, H., Chang, K. S., Lee, D.H. and Lim J.I. Signcryption schemes with forward secrecy. In *Proceeding of WISA 2*. 2001. 403-475.

[13] Gamage, A., Leiwo, J. and Zheng Y. Encrypted message authentication by firewalls. *International Workshop on Practice and Theory in Public Key Cryptography, Springer-Verlag*. 1999. 69-81.

[14] Toorani, M. and Shirazi, A. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. In *Proceedings of International Conference on Computer and Electrical Engineering*. 2008. 428-432.

[15] Kumar, M., Gupta, P. and Kumar, A. A Novel and Secure Multi-party Key Exchange Scheme Using Trilinear Pairing Map Based on Elliptic Curve Cryptography. *International Journal of Pure and Applied Mathematics*. 2017.

[16] Kumar, M. and Gupta, P. Cryptographic schemes based on Elliptic Curve over the Ring Zp[i]. *Applied Mathematics*. 2016. 304-312.

[17] Boneh, D. and Lipton, R.J. Algorithms for black-box fields and their application to cryptography. *Advances in Cryptography*. 1996. 283-297.

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

[19] Certicom Research. Standards for efficient cryptography, SEC 1: elliptic curve cryptography. Standards for efficient cryptography group (SECG). 2000.

[20] Batina, L., Preneel, B. and Vandewalle, J. Hardware architectures for public key cryptography. *Integration the VLSI Journal*. 2003. 1-64.