Journal of Computer Science

Original Research Paper

Elliptic Curve Signcryption Scheme with Low Computational Cost for Conventional Key Exchange Solution

Manoj Kumar and Pratik Gupta

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

Article history
Received: 21-11-2017
Revised: 23-04-2018
Accepted: 07-05-2018

Corresponding Author:
Pratik Gupta
Department of Mathematics and Statistics, Gurukula Kangri Vishwavidyalaya, Haridwar (Uttrakhand) 249404, India
Email: pratikgupta1810@gmail.com

Abstract: Signcryption is a cryptographic scheme that connects the function of digital signature and asymmetric key encryption logically into a single step and have less computational cost than that of symmetric signature -then- encryption method, is known as signcryption. There are various significant applications of signcryption performed by several researchers. For efficient critical applications, signcryption scheme are specially suitable 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 single small data packet, secure ATM networks as well as light weight electronic transaction protocols and multi-casting over the internet. In this research paper we had improved authentication scheme of signcryption symmetric key solutions, using elliptic curves by reducing computational cost. This makes it more crucial than others.

Keywords: Elliptic Curve, Signcryption, Digital Signature, Authentication, Cryptographic Nonce

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. To overcome from high computation and communication costs signcryption is an alternative and effective approach for STE method. In Zheng (1997) 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.

Diagramatical representation of a STE scheme is shown in Fig. 2.

Using the terminology in cryptography, signcryption consists a pair (S,U) is a polynomial time algorithm consist in signcryption scheme (Zheng and Imai, 1998a) 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 scheme's parameters

Diagrammatically a signcryption scheme can be described as in Fig. 1.

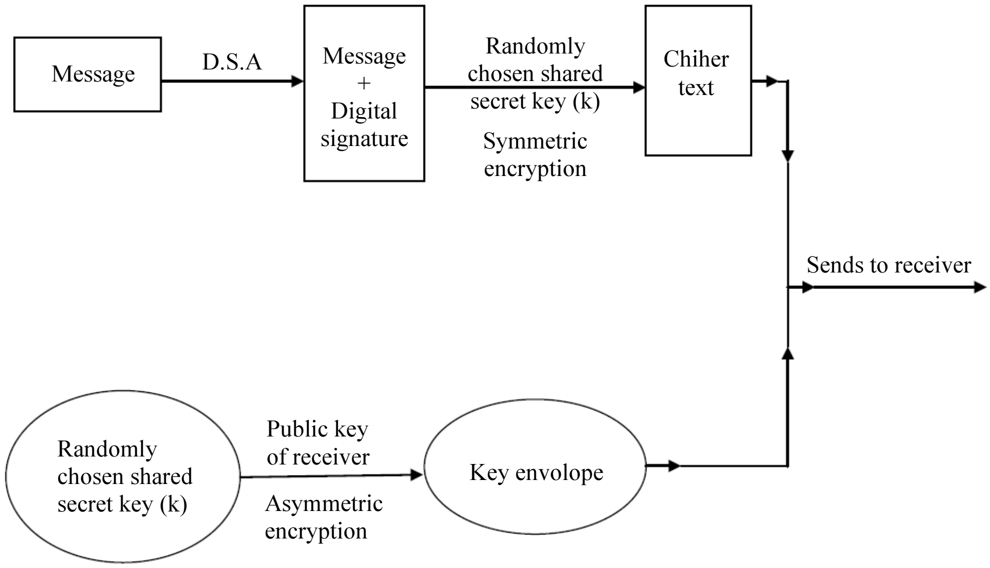

Fig. 1: Signature-then-encryption scheme

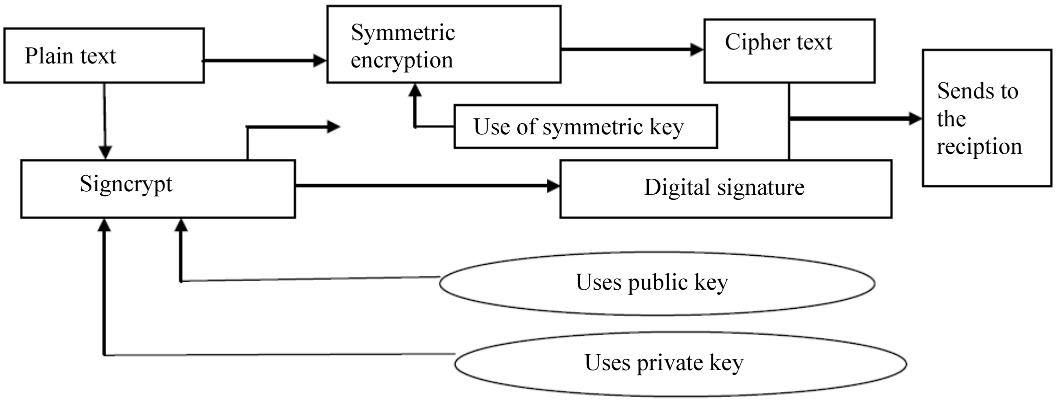

Fig. 2: Signcryption scheme

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 (Zheng and Imai, 1998b), secure ATM networks (Carnage *et al*., 1997) as well as light weight electronic transaction protocols (Hanaoka *et al*., 1998) and multi-casting over the internet (Matsuura *et al*., 1998). 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 proposed signcryption scheme based on elliptic curves. In section five we use our signcryption scheme for key establishment. Section six analyses security of the designed scheme. The paper is closed by section seven where we compared our proposed scheme with existing STE schemes.

DOI: 10.3844/jcssp.2018.■■■.■■■

Parallel Work

It defines the hierarchy of developments in area of cryptography. But it is not beneficial for common use. In present time it evaluated in many branches like signcryption that is the most Now a days it developed in many terms like signcryption which is the most authentic in the history of security. Some signcrption researches are based on modular exponential while others are based on elliptic curves (Zheng and Enos, 2014; Yanwei *et al*., 2015; Rao, 2017; Song *et al*., 2017).

Zheng (1997) was the first person who proposed signcryption cryptography technique in 1997. He combines two function digital signature and encryption algorithm to come up with authenticity and confidentiality features of cryptography 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 (1998). It cannot be verified publically and Jung *et al.* (2001) shows that it does not provide forward secrecy of message confidentiality when the sender's private key disclosed rather Gamage *et al.* (1999) enhanced it can be verify the signcryption of cipher text publically. Zheng and Imai (1998a) 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 it requires forward secrecy. Toorani and Shirazi (2008) comes with new feature of ECC based signcryption scheme has all the security component which takes more computational time.

To overcome these drawbacks we need new scheme →with message authentication, low communication cost, forward secrecy, less computational time as well as public verification. That is lacking in signcryption scheme stated above.

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 exists on arithmetic of elliptic curves (Gupta *et al*., 2017; Hankerson *et al*., 2004; Silverman, 1986; Stinson, 2006; Washington, 2008) a simple and easier arithmetic of elliptic curves is given by the following (Kumar and Gupta, 2016).

An elliptic curve $E(F_p)$ over a finite field is F_p 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:

- $P + O = O + P$, $\forall\, P \in E(F_p)$
- 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 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 $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1-x_3) - y_1$ and $\lambda = (y_2-y_1)/(x_2-x_1)$
- 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 $\lambda(3x^2+a)/2y$

Geometrically, the addition of two distinct points P and Q on an elliptic curve is shown in Fig. 3, while Fig. 4 shows the doubling of a point P (addition of two equal points).

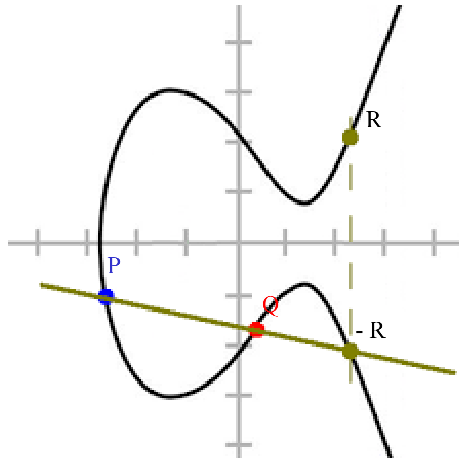

Fig. 3: Addition of 2 points P and Q

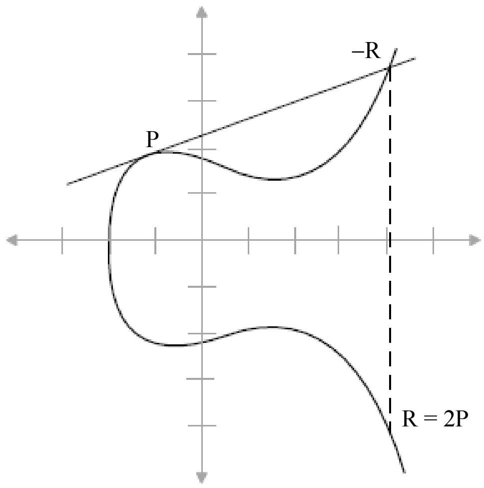

Fig. 4: Doubling of a point P, $R = 2P$

Proposed Signcryption Schemes 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 smaller than q and satisfy $4a^3 + 27b^2 \bmod q \neq 0$
F	The selected elliptic curve over finite field q i.e., $F = \{(x,y): y^2 = (x^3 + ax + b) \bmod q\} \cup \{O\}$
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
$E_{k_1}(\cdot)/D_{k_1}(\cdot)$	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 $e_B = d_B \times G$. They require accessing their certified public keys by the Certificate Authority (CA).

Assume that Alice wants to send a message m to Bob. Alice generates digital signature (R,s) of message m and we use asymmetric encryption for signcryption scheme but our scheme finally encrypted symmetry with secret key k_1 to encrypt m for reducing computational cost as well as achieving security parameter like as confidentiality, authentication, integrity, unforgeability, non-repudiation, forward secrecy, public verification. Let c be cipher text. Alice generates the signcrypted text (R, s, c) as in the Fig. 5.

The following equations evidence the correctness of the proposed scheme:

$$\begin{aligned}
K &= d_B sR + d_B s e_A \\
&= d_B \frac{d}{r+d_A} r\cdot G + d_B \frac{k}{r+d_A} e_A \\
&= d_B \frac{k}{r+d_A} r\cdot G + d_B \frac{k}{r+d_A} d_A \cdot G \\
&= d_B \frac{k}{r+d_A} G\left(r+d_A\right) \\
&= k d_B \cdot G \\
&= k \cdot e_B
\end{aligned}$$

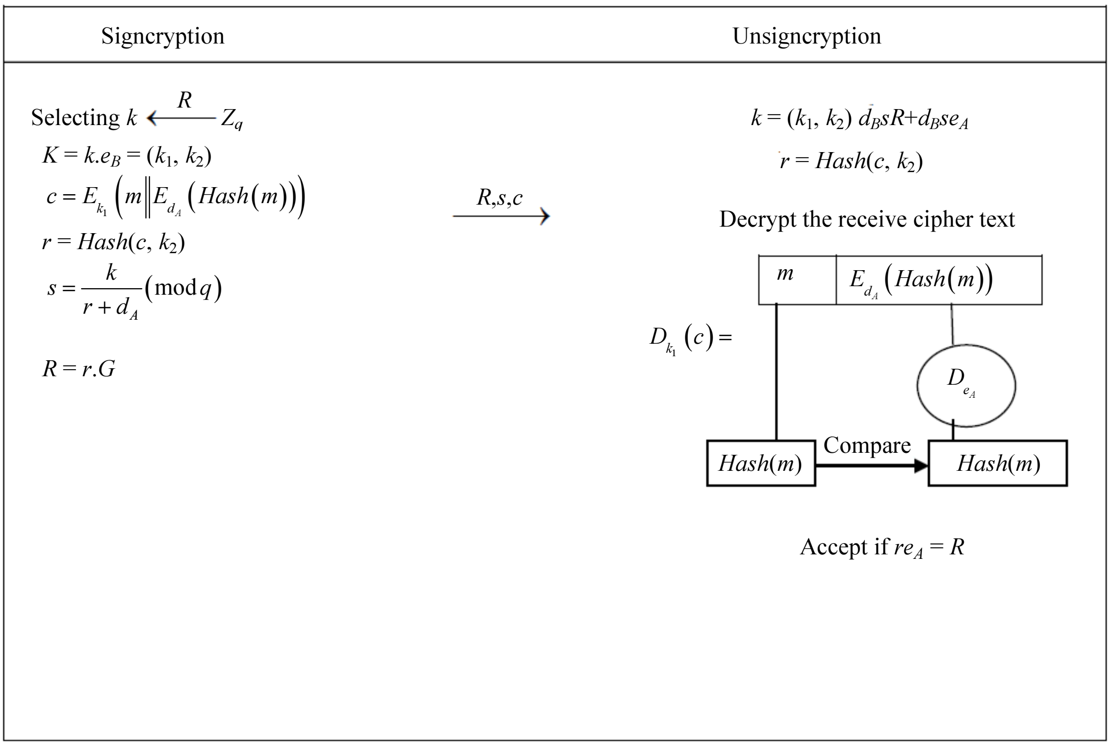

Fig. 5: The proposed scheme

DOI: 10.3844/jcssp.2018.■■■.■■■

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 use the symmetric encryption with 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 Fig. 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 (Boneh and Lipton, 1996) 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:

The Elliptic Curve Discrete Logarithm Problem

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 $t \in Z$ find such that $tP = Q$. It is computationally infeasible to generate *t* from *P* and *Q* (Johnson *et al*., 2001).

The Elliptic Curve Diffie–Hellman Problem

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 $t \in Z$ find such that $t = c.d \times G$. It is assumed computationally infeasible problem SECG (2000).

A		B
$K_A \xleftarrow{R} \{0,1\}^{l_k}$	$\xleftarrow{N_B}$	$N_B \xleftarrow{R} \{0,1\}^{l_k}$
$t \xleftarrow{R} Z_q$		
$K = (k_1, k_2) \leftarrow (t.e_B)$		
$c \leftarrow Enc_{k_1}(K_A)$		
$r \leftarrow hash(k_2, k_A, N_B)$		
$s \leftarrow \frac{t}{r = d_A}(\bmod q)$	$\xrightarrow{c,\ r,\ s}$	$K = (k_1, k_2) \leftarrow s.d_B(e_A + r.G)$
		$K_A \leftarrow Dec_{k_1}(c)$
		Accept K_A if $hash(k_2, K_A, N_B) = r$
		$K_B \xleftarrow{R} \{0,1\}^{l_k}$
		$t^1 \xleftarrow{R} Z_q$
		$K^1 = (k_1^1, k_2^1) \leftarrow (t^1.e_A)$
		$c_1 \leftarrow Enc_{k_1^1}(K_B)$
		$s_1 \leftarrow \frac{t^1}{r^1 = d_A}(\bmod q)$
$K^1 = (k_1^1, k_2^1) \leftarrow s^1.d_B(e_A + r^1.G)$	$\xleftarrow{c^1,\ r^1,\ s^1}$	Compute $K_{AB} \leftarrow K_A \oplus K_B$
$K_B \leftarrow Dec_{k_1^1}(c^1)$		
Accept KB if $hash(k_2^1, K_B, K_A) = r^1$		
Compute $K_{AB} \leftarrow K_A \oplus K_B$		

Fig. 6: Key exchange protocol

Table 1: The security analysis of different signcryption schemes

Signcryption schemes	Confidentiality	Integrity	Unforgeability	Non-repudiation	Forward secrecy	Public verification
Zheng (1997; Carnage *et al*., 1997)	Yes	Yes	Yes	Another	No	No
Zheng and Imai (1998a)	Yes	Yes	Yes	Another	No	No
Bao and Deng (1998; Hanaoka *et al*., 1998)	Yes	Yes	Yes	Directly	No	Yes
Gamage *et al*. (1999; Matsuura *et al*., 1998)	Yes	Yes	Yes	Directly	No	Yes
Jung *et al*. (2001; Hanaoka *et al*., 1998)	Yes	Yes	Yes	Another	Yes	No
Toorani and Shirazi (2008)	Yes	Yes	Yes	Directly	Yes	Yes
Our scheme	Yes	Yes	Yes	Directly	Yes	Yes

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 verifying equation:

$$D_{k_1}(c) = m$$

apply Hash value:

$$D_{k_1}(c) = Hash(m) \quad (1)$$

$$D_{k_1}(c) = E_{d_A}(Hash(m))$$

Decryption on public key of user A:

$$D_{k_1}(c) = D_{e_A}(E_{d_A}(Hash(m))) \quad (2)$$

If the comparison of Equation (1) and (2) 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 $r = Hash(c, k_2), s = \frac{k}{r + d_A}(\bmod q)$ (3) Integrity. Integrity is a process of maintaining the data that must not be changed by unauthorized person during in transit. In our scheme, getting 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)Rscrequired by the judge to verify. In Judge Verification phase, the judge can determine the signature is generated by the sender if equation $(k_1,k_2) = d_B sR + d_B se_A$ holds. Then it ensures the property of non-repudiation.

Forward Secrecy

An opponent that have d_A will not get the past message after all the opponent that has d_A will have to calculate d_B for the decryption and calculate d_B need to solve ECDLP i.e., computationally infeasible (Batina *et al*., 2003).

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.

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 83 ms and the modular exponentiation operation needs 220 ms for average computational time

DOI: 10.3844/jcssp.2018.■■■.■■■

in the Infineon's SLE66CUX640P security controller (Jung *et al*., 2001). The most computational time for elliptic curve multiplication and modular exponentiation operation for various scheme proposed by different researchers, is showed in Table 3.

This paper introduces nonce based signcryption schemes for secure and authenticated message delivery, using elliptic curves which fulfils all the 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 signcryption schemes

Signcryption scheme	Participants	EXP	DIV	ECPM	ECPA	MUL	ADD	KH(.)
Zheng (1997)	Alice	1	1	-	-	-	1	2
Bao and Deng (1998)	2	-	-	-	2	-	2	
Zheng and Imai (1998a)	Alice	-	1	1	-	1	1	2
Bao and Deng (1998)	-	-	2	1	2	-	2	
Bao and Deng (1998)	Alice	2	1	-	-	-	1	3
Bao and Deng (1998)	3	-	-	-	1	-	3	
Gamage *et al*. (1999)	Alice	2	1	-	-	-	1	2
Bao and Deng (1998)	3	-	-	-	1	-	2	
Toorani and Shirazi (2008)	Alice	-	-	2	-	2	2	2
Bao and Deng (1998)	-	-	4	2	-	-	2	
Our scheme	Alice	-	1	2	-	-	-	2
Bob	-	-	2	-	-	-	2	

where, 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. DI = 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

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 (1997)	1×220 = 220	2×220 = 440
Zheng and Imai (1998a)	1×83 = 83	2×83 = 166
Bao and Deng (1998)	2×220 = 440	3×220 = 660
Gamage *et al*. (1999)	2×220 = 440	3×220 = 660
Toorani and Shirazi (2008)	2×83 = 166	4×83 = 332
Our Scheme	2×83 = 166	2×83 = 166

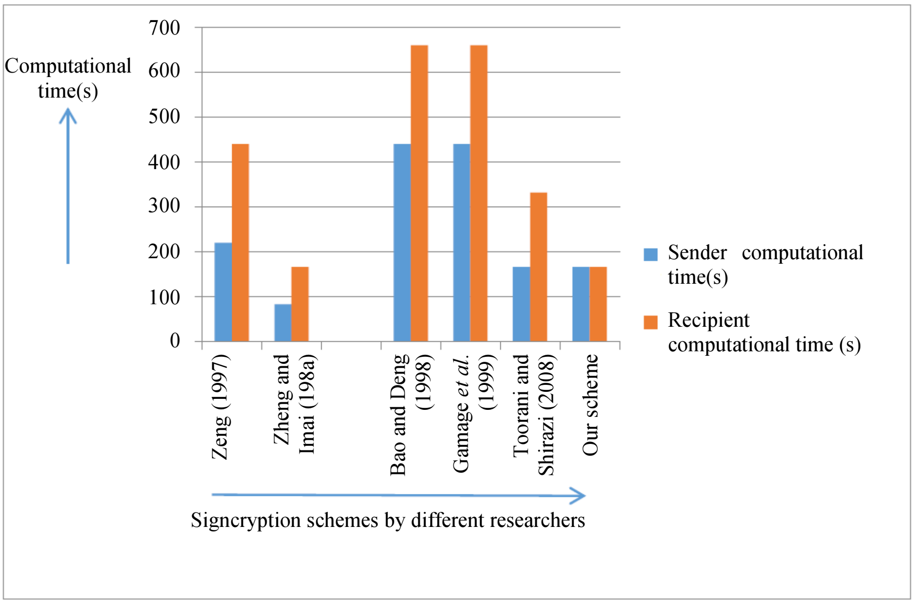

Fig. 7: Bar graph between average computational time and different proposed signcryption schemes

As it as obvious from the Fig. 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 (Table 1 in Section 6).

Acknowledgement

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.

Author's Contributions

Manoj Kumar: Coordinated the data-analysis and contributed to the writing of the manuscript.

Pratik Gupta: All experiments, Designed the research work.

Conflict of Interest

Author has declared that no conflict of interest exist.

References

Bao, F. and R.H. Deng, 1998. A signcryption scheme with signature directly verifiable by public key. Proceedings of the International Workshop on Public Key Cryptography, (PKC' 98), Springer-Verlag, ISBN-10: 978-3-540-69105-1, pp: 55-59.

Batina, L., B. Preneel and J. Vandewalle, 2003. Hardware architectures for public key cryptography Integrat. VLSI J., 34: 1-64. DOI: 10.1016/S0167-9260(02)00053-6

Boneh, D. and R.J. Lipton, 1996. Algorithms for Black-Box Fields and Their Application to Cryptography. In: Advances in Cryptology, Koblitz N. (Ed.), Springer, Berlin, Heidelberg, ISBN-10: 978-3-540-68697-2, pp: 283-297.

Carnage, C., J. Leiwo and Y. Zheng, 1997. A block-based approach to secure ATM networking.

Gamage, A., J. Leiwo and Y. Zheng, 1999. Encrypted message authentication by firewalls. Proceedings of International Workshop on Practice and Theory in Public Key Cryptography, (PKC' 99), Springer-Verlag, pp: 69-81. DOI: 10.1007/3-540-49162-7_6

Gupta, P., M. Kumar and A. Kumar, 2017. A novel and secure multiparty key exchange scheme using trilinear pairing map based on elliptic curve cryptography. Int. J. Pure Applied Math., 116: 37-50. DOI: 10.1007/978-981-10-5687-1_4

Hanaoka, G., Y. Zheng and H. Imai, 1998. A Light-Weight Secure Electronic Transaction Protocol. In: Information Security and Privacy, Boyd, C. and E. Dawson (Eds.), Springer, Berlin, Heidelberg, ISBN-10: 978-3-540-69101-3, pp: 215-226.

Hankerson, D., J.A. Menezes and S. Vanstone, 2004. Guide to Elliptic Curve Cryptography. 1st Edn., Springer-Verlag, Germany, ISBN-10: 978-0-387-21846-5, pp: 312.

Johnson, D., A. Menezes and S. Vanstone, 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). Int. J. Inform. Security, 1: 36-63.

Jung, H., K.S. Chang, D.H. Lee and J.I. Lim, 2001. Signcryption schemes with forward secrecy. Proc. WISA, 2: 403-475.

Kumar, M. and P. Gupta, 2016. Cryptographic schemes based on Elliptic Curve over the Ring Zp[i]. Applied Math., 7: 304-312.

Matsuura, K., Y. Zheng and H. Imai, 1998. Compact and Flexible Resolution of CBT Multicast Key-Distribution. Proceedings of the 2nd International Conference on Worldwide Computing and Its Applications, (WCA' 98), Springer, Berlin, pp: 190-205. DOI: 10.1007/3-540-64216-1_49

Rao, Y., 2017. Attribute-Based Online/Offline Signcryption Scheme. 1st Edn., John Wily and Sons.

SECG, 2000. Certicom research, standards for efficient cryptography. SEC 1: Elliptic Curve Cryptography, Standards for Efficient Cryptography Group (SECG).

Silverman, J., 1986. *The* Arithmetic of Elliptic Curves. 1st Edn., Springer, New York, ISBN-10: 0387962034, pp: 400.

Song, Y., Z. Li, Y. Li and J. Li, 2017. Attribute-based signcryption scheme based on linear codes. Inform. Sci., 417: 301-309. DOI: 10.1016/j.ins.2017.06.033

Stinson, D.R., 2006. Cryptography: Theory and Practice. 1st Edn., Chapman and Hall/CRC, United Kingdom.

Toorani, M. and A. Shirazi, 2008. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. Proceedings of International Conference on Computer and Electrical Engineering, Dec. 20-22, IEEE Xplore Press, Phuket, Thailand, pp: 428-432. DOI: 10.1109/ICCEE.2008.147

Washington, L.C., 2008. Elliptic Curves: Number Theory and Cryptography. 2nd Edn., Chapman and Hall/CRC, United Kingdom, ISBN-10: 9781420071474, pp: 436.

Yanwei, Z., Y. Bo and Z. Wenzheng, 2015. Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing. Discrete Applied Math., 204: 185-202. DOI: 10.1016/j.dam.2015.10.018

Zheng, Y. and G. Enos, 2014. An ID-based signcryption scheme with compartmented secret sharing for unsigncryption. Information Process. Lett.

Zheng, Y. and H. Imai, 1998a. How to construct efficient signcryption schemes on elliptic curves. Inform. Process. Lett., 68: 227-233. DOI: 10.1016/S0020-0190(98)00167-7

Zheng, Y. and H. Imai, 1998b. Compact and unforgeable key establishment over an ATM network. Proceedings of the 17th Annual Joint Conference of the Computer and Communications Societies, Mar. 29-Apr. 2, IEEE Xplore Press, San Francisco, pp: 411-418. DOI: 10.1109/INFCOM.1998.665057

Zheng, Y., 1997. Digital Signcryption or How to Achieve Cost(Signature and Encryption) ≪ Cost(Signature) + Cost(Encryption). In: Advances in Cryptology, Kaliski, B.S. (Ed.), Springer-Verlag, Berlin, Heidelberg, ISBN-10: 978-3-540-69528-8, pp: 165-179.