Kuwait J.Sci., Vol.49, No.(1),January.2022,pp(1-11)

Cryptanalysis and improvement of an encryption scheme that uses elliptic curves over finite fields

Malik Zia Ullah Bashir*, Rashid Ali

Dept. of Mathematics
Capital University of Science and Technology, Islamabad, Pakistan

**Corresponding author: ziamalik199@gmail.com*

Abstract

In this paper, we cryptanalyzed a recently proposed encryption scheme that uses elliptic curves over a finite field. The security of the proposed scheme depends upon the elliptic curve discrete logarithm problem. Two secret keys are used to increase the security strength of the scheme as compared to traditionally used schemes that are based on one secret key. In this scheme, if an adversary gets one secret key then he is unable to get the contents of the original message without the second secret key. Our analysis shows that the proposed scheme is not secure and unable to provide the basic security requirements of the encryption scheme. Due to our successful cryptanalysis, an adversary can get the contents of the original message without the knowledge of the secret keys of the receiver. To mount the attack, Mallory first gets the transmitted ciphertext and then uses public keys of the receiver and global parameters of the scheme to recover the associated plaintext message. To overcome the security flaws, we introduced an improved version of the scheme.

Keywords: Cryptanalysis; elliptic curve cryptography; encryption; finite field; information security.

1. Introduction

Cryptography is the science of hiding the contents of secret information from unauthorized parties. Depending upon the keys used, cryptography is divided into two branches namely, the public key and the private key cryptography. Public key cryptography was invented by Diffie & Hellman (1976) to overcome the problem of exchanging the secret keys. Their protocol depends upon the hardness of solving discrete logarithm problem. They present a new model that uses two keys, one is called a public key and the other is known as a private key. Miller (1985) and Koblitz (1987) independently proposed a new public key cryptography based on the computations in an elliptic curve group. An elliptic curve over a finite field $\mathbb{F}_p$ is the set of points satisfying the equation

$$y^2 = x^3 + ax + b \mod p$$

with a point O at infinity and a,b ∈ F with 4a +27b = 0. The security of elliptic curve cryptography (ECC) depends upon elliptic curve discrete logarithm problem (ECDLP). The main advantage of elliptic curve cryptography is its smaller keys which provides the same level of security as compared to other public key cryptosystems like RSA (Rivest et al., 1978) and El-Gamal (1985).

Zheng & Imai (1998) introduced a new elliptic curve based signcryption scheme. The proposed scheme reduces the communication and computational cost as compared to existing signcryption schemes. Bailey & Paar (2001) proposed an efficient method for working with elliptic curve arithmetic using finite fields. Han & Yang (2006) introduced a new elliptic curve based signcryption scheme that is suitable for multiple recipients. Their scheme provides security properties of integrity, unforgeability, confidentiality, non-repudiation and authentication. Mohammad & Elkamchouchi (2009) introduced a new elliptic curve based scheme which provides forward secrecy and encrypted message authentication. The security of their scheme depends upon elliptic curve discrete logarithm problem. Toorani & Shirazi (2009) introduced a new elliptic curve based scheme which provides additional security property of forward secrecy. The proposed scheme is efficient and considered to be best in resource constrained devices. King (2009) proposed a new method for converting the arbitrary message of any size into an elliptic curve point without any modification in the original message. Rao & Setty (2010) introduced two different methods for mapping of any arbitrary message into elliptic curve points over the finite fields. Li & Lee (2012) analysis showed that the proposed scheme of He *et al.* (2011) is not secure and is vulnerable to eavesdropping attack. The user anonymity of the scheme is compromised and the participants have to bear a long identity (128 bit) in the login phase. To overcome these issues, they introduced a modified version of the compromised scheme that is suitable for mobile wireless networking. Ahirwal & Jain (2013) proposed a new elliptic curve based signcryption scheme. In their scheme, the ciphertext is transmitted in the form of elliptic curve points generated from elliptic curve point addition. The proposed signature generation technique has less computational time as compared to existing schemes that uses hash function. The cryptanalysis performed by Hu *et al.* (2014) shows that the presented scheme in (Li & Lee, 2012) is not secure and vulnerable to offline password guessing attack. To overcome this security issue, they proposed an improved version of the scheme. Their analysis shows that the improved scheme is secure against the existing attacks and is more efficient than the scheme of Li & Lee (2012). The security of an elliptic curve based signcryption scheme of Iqbal *et al.*(2013) is investigated by Zia & Ali (2018) and is proved to be insecure against existing attacks. To overcome the security flaws, a modified and improved version of this scheme is proposed. The modified scheme is then further tested against known attacks and proved to be secure. Recently, some researchers proposed different encryption and authetication schemes and their related applications (Huang & Tu, 2015; Som, 2015; Avci, 2016; He *et al.*, 2017; Athena *et al.*, 2018; Zia & Ali, 2019; Mohammed *et al.*, 2020).

Namiq *et al.* (2018) proposed a new encryption scheme that uses computations in elliptic curve groups over finite fields. In their scheme, the ciphertext is transmitted through a public channel in the form of an elliptic curve point. The proposed scheme uses two secret keys to increase the security as compared to one secret key based encryption schemes. In their scheme, if one secret key of the sender is compromised even then the attacker will not be able to get the con-tents of original message without the knowledge of second secret key. Our analysis shows that the proposed scheme of Namiq *et al.* (2018) is not secure and an adversary can get the contents of the original message from the ciphertext. Rest of the paper is organized as: Section 2 gives introduction of new encryption scheme of Namiq *et al.* (2018) followed by its cryptanalysis in Section 3, Section 4 describes the modification of the scheme and Section 5 gives the conclusion.

2. Description of the recently proposed encryption scheme

In this section, a new elliptic curve based encryption scheme of Namiq *et al.* (2018) is described. The proposed scheme uses two secret keys for increasing the security as compared to traditionally used schemes with one secret key. The security of the scheme depends upon the elliptic curve discrete logarithm problem. Suppose, Alice wants to send a message M to Bob through unsecured public network. Firstly, Alice converts the message M into elliptic curve point by using the method given in the proposed scheme of Namiq *et al.* (2018).

Global Parameters

First Alice and Bob agreed on the following public parameters:

Variables	**Description**
q	A large prime greater than 2^{128}.
$E(\mathbb{F}_q)$	An elliptic curve $y^2 = x^3 + ax + b$ over finite field $\mathbb{F}_q$.
n	A very large prime number greater than 2^{128} .

After converting M in to a point of elliptic curve $E(\mathbb{F}_q)$, the rest of the the scheme is described in following phases:

Phase 1- Bob

1. Chooses a base point B of an elliptic curve E.
2. Selects an elliptic curve point A and kept it as secret.
3. Selects two secret integers (keys) s_b, $s_{b_1} \in \{1,2,3,\ldots,n-1\}$.
4. Computes elliptic curve points P_B, P_{B_1} and P_{B_2} by using elliptic curve point multiplication as:

$$P_B = [s_b]B, P_{B_1} = [s_{b_1}]A, P_{B_2} = [s_{b_1}](P_B + P_{B_1})$$

5. Sends B, P_B, P_{B_1} and P_{B_2} to Alice through public network.

Phase 2- Alice

1. Receives B, P_B, P_{B_1} and P_{B_2} from Bob.
2. Converts the original message M into an elliptic curve point (Namiq *et al.*, 2018).
3. Selects two secret integers (keys) $s_a, s_{a_1} \in \{1,2,3,\ldots,n-1\}$.
4. Computes elliptic curve points P_A, P_{A_1}, P_{A_2}, K, and K_A as:

$$P_A = [s_a]B, P_{A_1} = [s_{a_1}]P_B, P_{A_2} = [s_{a_1}]P_{B_1}, K = [s_a]P_B, K_A = [s_{a_1}]P_{B_2} + K$$

5. Encrypt the message M in the form of an elliptic curve point as:

$$C = M + K_A$$

6. Sends C, P_A, P_{A_1} and P_{A_2} to Bob through public network.

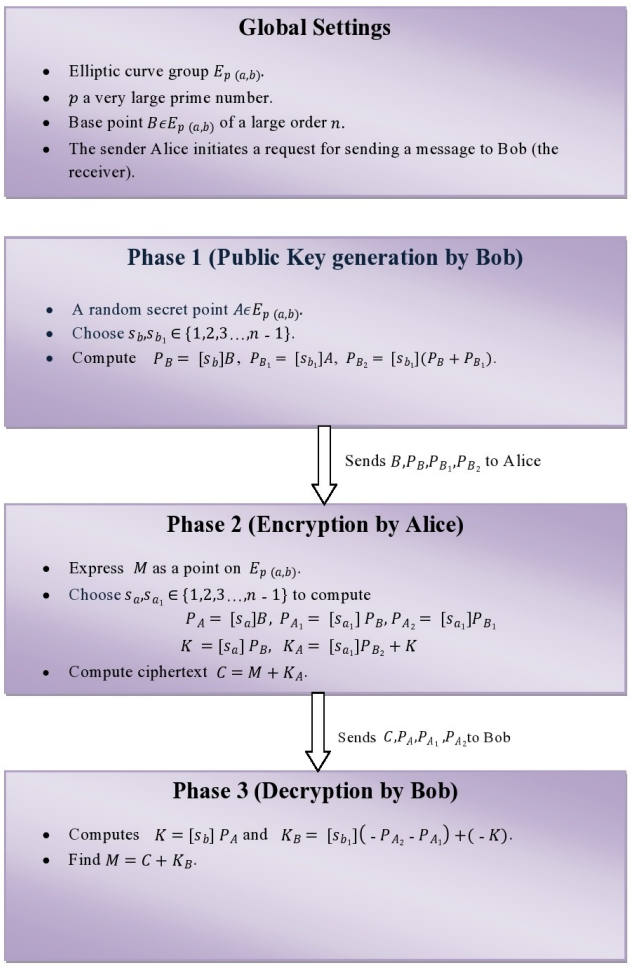

Fig. 1. The proposed Encryption Scheme

Phase 3- Bob

1. Gets C, P_A, P_{A_1} and P_{A_2} from Alice .
2. Computes elliptic curve points as:

$$K = [s_b]P_A, K_B = [s_{b_1}](-P_{A_2} + (-P_{A_1})) + (-K)$$

3. Decrypt the message M as $M = C + K_B$.

Note. It is important to note that the proposed scheme uses different pairs of secret keys for encrypting each message. If pair of secret keys are identical then attacker easily calculates original message from publicly transmitted information.

3. Cryptanalysis

In this section, the security of the encryption scheme proposed by Namiq *et al.* (2018) is investigated. Our analysis shows that the scheme is not secure and an adversary can get the original message with public parameters. The involvement of more than one secret key for increasing the security of the scheme does not improve the security. Mallory (attacker) exploit the common shared key generation and exchange process of the proposed scheme.

Bob first chooses a base Aoint B to generate three points P_B, P_{B_1} and P_{B_2} in $E(\mathbb{F}_q)$ as his public keys. Then he transmits B, P_B, P_{B_1} and P_{B_2} to Alice. Mallory (Attacker) changes the transmitted information before it is received by Alice. She then uses these keys to generate her public keys and common shared secret to encrypt a message M. The encrypted text together with the associated parameter are then transmitted to Bob. But the attacker is already observing the communication between Alice and Bob and therefore gets all the information transmitted by Alice to Bob. This information together with the global parameters is sufficient for Mallory to reveals the original message. The four phases of the cryptanalysis are explained below.

Phase 1- Bob

1. Chooses a base point B of an elliptic curve E.
2. Selects an elliptic curve point A and kept it as secret.
3. Selects two secret integers (keys) $s_b, s_{b_1} \in \{1,2,3,\ldots,n-1\}$.
4. Compute elliptic curve points P_B, P_{B_1} and P_{B_2} by using elliptic curve point multiplication as:
$$P_B = [s_b]B, P_{B_1} = [s_{b_1}]A, P_{B_2} = [s_{b_1}](P_B + P_{B_1})$$
5. Sends B, P_B, P_{B_1} and P_{B_2} to Alice through public channel.

Phase 2- Mallory

1. Intercepts the network traffic between Alice and Bob to get B, P_B, P_{B_1} and P_{B_2}.
2. Changes the elliptic curve points P'_B and P'_{B_2} as:
$$P'_B = B, P'_{B_2} = P_{B_1}$$
3. Sends B, P'_B, P_{B_1} and P'_{B_2} to Alice.

Phase 3 - Alice

1. Receives $B, P'_B = B, P_{B_1}, P'_{B_2} = P_{B_1}$.
2. Converts the original message M into elliptic curve point (Namiq *et al.*, 2018).
3. Selects two secret integers (keys) s_a , $s_{a_1} \in \{1,2,3,\ldots,n-1\}$
4. Computes elliptic curve points P_A, P_{A_1}, P_{A_2}, K' and K'_A as:
$$P_A = [s_a]B, P'_{A_1} = [s_{a_1}]P'_B, P_{A_2} = [s_{a_1}]P_{B_1}, K' = [s_a]P'_B, K'_A = [s_{a_1}]P'_{B_2} + K'$$
5. Encrypt the message M in the form of elliptic curve point as $C' = M + K'_A$
6. Sends C',P_A, P'_{A_1} and P_{A_2} to Bob through public network.

Phase 4 - Mallory

1. Gets the publicly transmitted information C', P_A, P'_{A_1} and P_{A_2}.
2. Computes the original plaintext message as $M = C' - P_{A_2} - P_A$ In this way, Mallory defeats the cryptosystem and able to read the contents of original plaintext message M with public parameters of Alice.

Proof of Cryptanalysis

If an attacker has access to C', P_A and P_{A_2} then he obtains the original message M correctly as:

$$\begin{aligned} C' - P_{A_2} - P_A &= M + K'_A - P_{A_2} - P_A \\ &= M + [s_{a_1}]P'_{B_2} + K' - [s_{a_1}]P_{B_1} - [s_a]B \\ &= M + [s_{a_1}]P'_{B_2} + [s_a]P'_B - [s_{a_1}]P_{B_1} - [s_a]B \\ &= M + [s_{a_1}]P_{B_1} + [s_a]B - [s_{a_1}]P_{B_1} - [s_a]B \\ &= M \end{aligned}$$

3.1 Example

Consider an elliptic curve $y^2 = x^3 + 5x - 12 \mod 73$ over a finite field $\mathbb{F}_{73}$. All 64 points on the elliptic curve are given in Table 1.

Table 1. Points of the Elliptic Curve E defined over finite field $\mathbb{F}_{73}$

(0,34)	(0,39)	(1,33)	(1,40)	(2,15)	(2,58)	(4,27)	(4,46)	(5,24)
(5,49)	(7,1)	(7,72)	(9,18)	(9,55)	(10,4)	(10,69)	(12,30)	(12,43)
(16,21)	(16,52)	(18,17)	(18,56)	(23,15)	(23,58)	(27,13)	(27,60)	(29,33)
(29,40)	(30,36)	(30,37)	(31,2)	(31,71)	(35,25)	(35,48)	(37,23)	(37,50)
(38,9)	(38,64)	(43,33)	(43,40)	(44,36)	(44,37)	(48,15)	(48,58)	(53,8)
(53,65)	(56,10)	(56,63)	(57,22)	(57,51)	(61,5)	(61,68)	(66,11)	(66,62)
(68,35)	(68,38)	(69,14)	(69,59)	(70,26)	(70,47)	(72,36)	(72,37)	$\mathcal{O}$

Phase 1- Bob

1. Chooses a base point $B = (2,15)$ of elliptic curve E.
2. Selects a secret elliptic curve point $A = (1,33)$.
3. Selects two secret integers (keys) $s_b = 3, s_{b_1} = 4$
4. Computes elliptic curve points P_B, P_{B_1} and P_{B_2} by using elliptic curve point multiplication as:

$$\begin{aligned} P_B &= [3](2,15) = (16,21) \\ P_{B_1} &= [4](1,33) = (57,22) \\ P_{B_2} &= [4]((57,22) + (16,21)) = (68,38) \end{aligned}$$

5. Sends B, P_B, P_{B_1} and P_{B_2} to Alice.

Phase 2- Mallory

1. Intercepts the network traffic between Alice and Bob and gets B, P_B, P_{B_1} and P_{B_2} from Bob.
2. Changes the elliptic curve points P'_B and P'_{B_2} as:

$$P'_B = B = (2,15), P'_{B_2} = P_{B_1} = (57,22)$$

3. Sends B, P'_B, P_{B_1} and P'_{B_2} to Alice.

Phase 3- Alice

1. Receives B, P'_B, P_{B_1} and P'_{B_2}.
2. Suppose Alice wants to send a message "Go Back" to Bob. First she converts the first letter $G = (4,27)$ in to elliptic curve point by using Table 2.
3. Selects two secret integers (keys) $s_a = 5, s_{a_1} = 6$
4. Computes the elliptic curve points P_A, P'_{A_1}, P'_{A_1}, P_{A_2}, K' and K'_A as:

$$\begin{aligned} P_A &= [5](2,15) = (44,37) \\ P'_{A_1} &= [6](2,15) = (43,40) \\ P_{A_2} &= [6](57,22) = (16,52) \\ K' &= [5](2,15) = (44,37) \\ K'_A &= [6](57,22) + (44,37) = (5,49) \end{aligned}$$

5. Encrypt the message $G = (4,27)$ in the form of elliptic curve point as:

$$C' = (4,27) + (5,49) = (37,50) = j$$

   Similarly, she encrypts all the characters of the message "Go Back" and gets the ciphertext message "jTG8Kgf".

6. Sends P_A, P'_{A_1}, P_{A_2} and C' to Bob.

Phase 4- Mallory

1. Gets P_A, P'_{A_1},P_{A_2} and C' from public channel.
2. Converts the first character of ciphertext message "j" into an elliptic curve point $(37,50)$ from Table 2.
3. Gets the original plaintext message G as:

$$C' - P_{A_2} - P_A = (4,27) = G$$

Similarly, Mallory decrypts all the characters of ciphertext message "jTG8Kgf" and gets the original plaintext message "Go Back". In this way, Mallory gets all the plaintext messages from the knowledge of public parameters of Alice without any secret key.

4. Modified Scheme with the Counter measures

Our analysis shows that the proposed encryption scheme of Namiq *et al.* (2018) is not secure and an adversary gets the original plaintext message from the ciphertext. To overcome the security flaws, we proposed an improved version of this scheme. We modify the key generation (Phase-1) and encryption process to overcome the security issues as described in Section 3. The public key P_B of the receiver is involved both in the encryption and decryption process. Due to these modifications, if an adversary applies the same attack as described in Section 3 then he will not be able to get the contents of the original message. The improved scheme is described below.

Table 2. Conversion of alphanumeric characters in to elliptic curve points

A	(0,34)	B	(0,39)	C	(1,33)	D	(1,40)	E	(2,15)
F	(2,58)	G	(4,27)	H	(4,46)	I	(5,24)	J	(5,49)
K	(7,1)	L	(7,72)	M	(9,18)	N	(9,55)	O	(10,4)
P	(10,69)	Q	(12,30)	R	(12,43)	S	(16,21)	T	(16,52)
U	(18,17)	V	(18,56)	W	(23,15)	X	(23,58)	Y	(27,13)
Z	(27,60)	a	(29,33)	b	(29,40)	c	(30,36)	d	(30,37)
e	(31,2)	f	(31,71)	g	(35,25)	h	(35,48)	i	(37,23)
j	(37,50)	k	(38,9)	l	(38,64)	m	(43,33)	n	(43,40)
o	(44,36)	p	(44,37)	q	(48,15)	r	(48,58)	s	(53,8)
t	(53,65)	u	(56,10)	v	(56,63)	w	(57,22)	x	(57,51)
y	(61,5)	z	(61,68)	0	(66,11)	1	(66,62)	2	(68,35)
3	(68,38)	4	(69,14)	5	(69,59)	6	(70,26)	7	(70,47)
8	(72,36)	9	(72,37)						

Phase 1- Bob

1. Chooses a base point B of an elliptic curve E.
2. Selects an elliptic curve point A and kept it as secret.
3. Selects two secret integers (keys) s_b ,$s_{b_1} \in \{1,2,3,\ldots,n-1\}$
4. Computes elliptic curve points P_B, P_{B_1} and P_{B_2} by using elliptic curve point multiplication as:
$$P_B = [s_b]A, P_{B_1} = [s_{b_1}]B, P_{B_2} = [s_{b_1}](P_B + P_{B_1})$$
5. Sends B, P_B, P_{B_1} and P_{B_2} to Alice through public network.

Phase 2- Alice

1. Receives B, P_B, P_{B_1} and P_{B_2} from Bob.
2. Converts the original message M into an elliptic curve point (Namiq *et al.*, 2018).
3. Selects two secret integers (keys) $s_a, s_{a_1} \in \{1,2,3,\ldots,n-1\}$.
4. Computes elliptic curve points P_A, P_{A_1}, P_{A_2}, K and K_A as:
$$P_A = [s_a]B, P_{A_1} = [s_{a_1}]P_B, P_{A_2} = [s_{a_1}]P_{B_1}, K = [s_a]P_{B_1}, K_A = [s_{a_1}]P_{B_2} + K = (k_1,k_2)$$
5. Encrypt the message M in the form of an elliptic curve point as $C = M + k_1 P_B$
6. Sends C, P_A, P_{A_1} and P_{A_2} to Bob through public network.

Phase 3- Bob

1. Gets C, P_A, P_{A_1} and P_{A_2} from Alice .
2. Computes elliptic curve points as:
$$K = [s_{b_1}]P_A, K_B = [s_{b_1}](P_{A_2} + (P_{A_1})) + (K)$$
3. Decrypt to get the original message M as $M = C - k_1 P_B$.

Proof of Correctness

Our improved scheme is correctly verifiable. Alice and Bob generate the same secret key for encryption and decryption of a message.

$$\begin{aligned} K_B &= [s_{b_1}](P_{A_2} + (P_{A_1})) + K \\ &= [s_{b_1}]([s_{a_1}]P_{B_1} + [s_{a_1}]P_B) + [s_{b_1}]P_A \\ &= [s_{a_1}]([s_{b_1}]P_{B_1} + [s_{b_1}]P_B) + [s_{b_1}][s_a]B \\ &= [s_{a_1}][[s_{b_1}](P_{B_1} + P_B)] + [s_a]P_{B_1} \\ &= [s_{a_1}]P_{B_2} + K \\ &= K_A \end{aligned}$$

If Bob has encrypted the message C and his secret key $K_B = (k_1, k_2)$ then he obtains the message M correctly as:

$$C - k_1 P_B = M + k_1 P_B - k_1 P_B = M$$

The improved scheme provides the confidentiality of the data. Without the knowledge of secret keys s_b, s_{b_1}, an attacker cannot obtain the original plaintext message M from the ciphertext C. If an adversary wants to get the secret keys s_b and s_{b_1} then he has to solve ECDLP in Step 4 of the improved scheme, which is computationally infeasible (Koblitz, 1987). So after the modification in the key generation and encryption processes, it is easy to see that the attack described in Section 3 will not be successful. Step 4 of Phase 1 of the improved scheme shows that P_B and P_{B_1} are computed by choosing random integers from a very large set (as $n > 2^{128}$). To find s_b and s_{b_1} from the knowledge of P_B and P_{B_1}, an adversary has to solve elliptic curve discrete logarithm problem (ECDLP). Recall that solving ECDLP in any elliptic curve group $E_p(a,b)$ of very large order is computationally hard (Koblitz, 1987).

5. Conclusion

Recently, Namiq *et al.* (2018) proposed a new encryption scheme that uses the computations in an elliptic curve group over a finite field. The proposed scheme uses two secret keys for encryption to improve the security as compared to traditionally used one secret key based schemes. Our analysis shows that the proposed scheme is not secure and unable to provide the basic security requirement of encryption scheme. Due to our successful cryptanalysis, an adversary can get the contents of the original message from the ciphertext. We introduced an improved version of this scheme to counter such attacks. As with the proposed parameters and the global settings of the scheme, solving elliptic curve discrete logarithm turns out to be computation-ally infeasible. Because of the way the keys are constructed, the method of attack described in Section A Aill Aot Aork Aor Ahe modified Acheme.

References

Ahirwal, R., & **Jain, A. (2013)**. Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation. International Journal of Computer Applications. 62(**9**), 0975–8887.

Athena, J., Sumathy, V., & **Kumar, K. (2018)**. An identity attribute based encryption using elliptic curve digital signature for patient health record maintenance. International Journal of Communication Systems. 25(**2**), 34-39.

Avci, D. (2016). A novel meaningful secret image sharing method based on Arabic letters. Kuwait Journal of Science. 43(**4**), 114-124.

Bailey, D. V., & **Paar, C. (2001)**. Arithmetic in Finite Field Extensions with Application in Elliptic Curve Cryptography. Journal of Cryptology. 14(**3**), 153-76.

Diffie, A., & **Aellman, A. A1976)**. New Airections in Aryptography, AEEE Aransactions on Information Aheory. A2(**6**), A44–654.

ElGamaL, T. (1985). A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory. 31(4), 469–472.

Han, Y., & **Yang, X. (2006)**. Elliptic Curve based Generalized Signcryption Scheme. Key Lab on Network and Information Security of Armed Police Force Department of Electronic Technology. 11, 2003-2012.

He, D., Ma, M., Zhang, Y., Chen, C., & **Bu, J. (2011).** A strong user authentication scheme with smart cards for wireless communications. Computer Communications, 34(**3**), 367-374.

He, A., Aang, A., Aang, A., Ahen, J., & **Yang, A. A2017)**. Afficient Aertificateless anonymous multi-receiver Ancryption Acheme Aor mobile Aevices Soft Aomputing. A(**21**), 6801-6810.

Hu, B., Bao, M., & **Dong, N. (2014)**. Improvement of user authentication protocol with anonymity for wireless communications. Kuwait Journal of Science, 41, 1, 155-169.

Huang, B., & **Tu, A. A2015)**. Strongly Aecure Aertificateless one-pass authenticated Aey agreement Acheme. Kuwait Journal of Science. A2(**1**), A1-108.

Iqbal, A., Afzal, A., & **Ahmad, A. A2013)**. An Afficient Alliptic Aurve Based Signcryption Scheme Aor Airewalls. And National Aonference on Anformation Assurance (NCIA). AOI: 10.1109/NCIA.2013.6725326, ASBN: A78-147991288-9, AEEE Aomputer Society.

King, B. A2009). Aapping an Arbitrary Aessage Ao an Alliptic Aurve Ahen Aefined over AF (2n). Anternational Journal of Network Security. A(**2**), A69-173.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. Mathematics of Computation. 177, 203–209.

Li, C. T., & **Lee, C. C., (2012)**. A novel user authentication and privacy-preserving scheme with smart cards for wireless communications. Mathematical and Computer, 55(**1-2**), 35-44.

Miller, V. S. (1985). Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques, Springer, Berlin, Heidelberg. 417-426.

Mohammad, E., & **Elkamchouchi, E. (2009)**. Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy, International Journal of Computer Science and Network Security. 9(**1**), 395-398.

Mohammed, N. F., Jawad, M. J., & **Ali, S. A. (2020)**. Biometric-based medical watermarking system for verifying privacy and source authentication. Kuwait Journal of Science. 47(**3**), 2-13.

Namiq, M. R., Kadir, W. K., & **Ahmed, A. M. (2018)**. A New Cryptosystem For Encryption and Decryption Using Elliptic Curves in Cryptography over Finite Fields. Journal of Theoretical Applied Information Technology. 96(**1**). 1992-8645.

Rao, O. S., & **Setty, S. P. (2010)**. Efficient Mapping methods for elliptic curve cryptosystem. International journal of engineering and technology. 2 (**8**), 3651-3656.

Rivest, R. L., Shamir, A., & **Adleman, L. (1978)**. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. 21(**2**), 120–126.

Som, S. (2015). Encryption Technique Using Elliptic Curve Cryptography Through Compression and Artificial Intelligence. In Cyber Security Proceedings of CSI, Springer Singapore. 447-457.

Toorani, M., & **Shirazi, A. B. (2009)**. An Elliptic Curve based Signcryption Scheme with Forward Secrecy. Journal of Applied Sciences. 9(**6**), 1025- 1035.

Zheng, Y., & **Imai, H. (1998)**. How to construct efficient signcryption schemes on elliptic curves. Information processing letters. 68(**5**), 227-33.

Zia, M., & **Ali, R. (2018)**. Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls. PLOS ONE. 13, 1-11.

Zia, M., & **Ali, R. (2019)**. Cryptanalysis and Improvement of Blind Signcryption Scheme Based on Elliptic Curve. Electronics Letters. 55(**8**), 457-459.

Submitted: 05/09/2019
Revised: 19/02/2020
Accepted: 19/02/2020
DOI: 10.48129/kjs.v49i1.8325