JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.406-415
https://publishoa.com
ISSN: 1309-3452

On Modification and Extension of Chua-Ling Cryptosystem

Shalini Gupta [1], Nitish Thakur [2], Awneesh Kumar [3]
Department of Mathematics & Statistics, Himachal Pradesh University, Summer- Hill-171005, Shimla, India.

ABSTRACT
For the security of the data and messages over the communicating medium, various algorithms for the security of information are widely used since the advent of communication over internet. Elliptic Curve Cryptography (ECC) is one of the most efficient techniques that are used for this issue, because it is difficult for the adversary to solve elliptic curve discrete logarithm problem to know the secret key that is used in encryption and decryption process. In this paper, we propose a modification of the Chua-Ling Cryptosystem that gives security and makes difficult for adversary to reduce that system into Rabin-William Cryptosystem . Further , We provide the authentication scheme for the system based on Digital Signature Algorithm that provides both Integrity and Authentication.

Keywords— Elliptic curve cryptography, Chua-Ling Cryptosystem, Encryption, Decryption, Authentication

1. Introduction

Cryptography is one of the efficient technique that ensures security of information over non-secure communicating channel. Public Key Cryptography (asymmetric key cryptography) is one of the famous mathematical techniques used recently [11]. The private key of the sender is different from the private key of the receiver whch is used to decipher the ciphertext to unveil the message [3]. Both sender and reciever are exchanging their public keys, which are not secret by using Elliptic Curve Diffie Hellman technique [2]. In 1977, a public key cryptosystem known as RSA was developed by Rivest-Shamir-Adleman that is widely used for secure data transmission and its security relies on practical difficulty of factoring product of two large prime numbers [1]. In 1985, the use of group of points of elliptic curves over finite fields in public key cryptography was suggested by Koblitz [12] and Miller [10]. The security of the cryptosytem depends on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is difficult to be solved by the adversary. Lenstra in 1987, gave an important role for the elliptic curves in integer factorization [4]. Later Vanstone et.al. proposed to use elliptic curves over the ring Z/nZ, where n is the product of two large prime numbers [15]. The security of their public key cryptosystem is based on the factorization problem for n. They use elliptic curves of special form such that the factorization of n directly gives the order of the group $E(Z/nZ)$. As an analogue of the RSA Cryptosystem , the security of these systems are based on the difficulty of factoring n. Demytko's elliptic curve cryptosystem uses only x coordinate of the point on an elliptic curve [16]. In 1991, Koyama and Kuwakado proposed an elliptic curve cyptosystem which can be considered as special case of Demytko's scheme and complemented in terms of restriction on prime numbers, gives one way trapdoor function similar to the RSA on elliptic curves over ring [17]. In 1996, Meyer-Müller proposed RSA type cryptosystem based on elliptic curves over the ring and public encryption exponent equals to 2[9]. But this cryptosystem can also be reduced to Rabin- WIlliams cryptosytem by using the data of cipher text[7]. After reduction messages can be recovered by using the algorithm of Coppersmith for low exponent attack [14]. For further interest, Chua-Ling proposed a special cyptosystem using singular cubic curves instead of standard elliptic curves[5]. But it can be futher reduced to Rabin Williams cryptosystem that reduces security of the cryptosystem. In this work, a modified method is proposed for the Chua-Ling cryptosystem that can't be reduced to Rabin- William cryptosystem that increases its security . Authenticaticy of the user remains a difficult task that provides integrity and authentication to the cryptosystem and an authenticaion via digital signature scheme has been developed since past few years[8]. So, further we have proposed an authentcation scheme via digital signature that provides both Integrity and Authentication to the cryptosystem.

This paper is organised as follows: Section 2 presents preliminaries related to t elliptic curve over the ring and brief overview of Chua-Ling cryptosytem, its reduction to Rabin Williams cryptosystem. Section 3 explains the method of modification for the Chua-Ling Cryptosystem and authentication scheme with illustration and finally displays concluding remarks.

2. Preliminaries

2.1 Elliptic Curve over Ring

The elliptic curve over ring Z_N is of the form

$$E_{a,b}(Z_N): y^2 = x^3 + ax + b$$

where $a, b \in Z_N$, and
g.c.d $(4a^3 + 27b^2, N) = 1$ & $p \times q = N$ (p, q are primes).
In general, over a ring Z_N, the set of points on the curve can be defined as the set of pairs $(x, y) \in Z_N^2$ satisfying $y^2 = x^3 +$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.406-415
https://publishoa.com
ISSN: 1309-3452
$ax + b($ mod $N)$ together with a point O_N at infinity [13]. The set of points in $E_{a,b}(Z_N)$ does not form a group. The same addition rule defined for an elliptic curve over a finite field cannot be extended to the ring Z_N because the inverse of a non-zero number n works in modulo a prime p but does not work in modulo a composite number N, if $g.c.d(n, N) > 1$.
The addition operation on $E_{a,b}(Z_N)$ described above is equivalent to the group operation on $E_p(a,b) \times E_q(a,b)$. By the Chinese Remainder Theorem every element C of Z_N can be uniquely represented as a pair $[C_p, C_q]$ where
$C_p = C$ mod p
and
$C_q = C$ mod q.
Thus, every point $P(x, y)$ on $E_{a,b}(Z_N)$ cab be represented uniquely as a pair
$[P_p, P_q] = [(x_p, y_p), (x_q, y_q)]$

where
$P_p \in Z_p(a, b)$ and $P_q \in Z_q(a, b)$
$x_p = x$ mod p and $y_p = y$ mod p
$x_q = x$ mod q and $y_q = y$ mod q.

The point at infinity O_N is represented by (O_p, O_q) where O_p and O_q are point at infinity on $E_p(a, b)$ and $E_q(a, b)$ respectively.
By this mapping, all elements of $E_p(a, b)$ and $E_q(a, b)$ are exhausted except the pair of points $[P_p, P_q]$ for which exactly one of the point P_p and P_q is the point at infinity.
Thus,
$\#E_{a,b}(z_N) = (\#E_p(a, b) - 1)(\#E_q(a, b) - 1) + 1$

Addition Rule for Elliptic Curve over Ring:

Let $P(x, y)$ corresponding to unique element (P_p, P_q) and $Q(x_1, y_1)$ corresponding to unique element (Q_p, Q_q) be two points on $E_{a,b}(Z_N)$. Then, the addition operation on $E_{a,b}(Z_N)$ is defined by the component wise addition in $E_p(a, b) \times E_q(a, b)$ that is

$$P + Q = (P_p + Q_p, P_q + Q_q).$$

Particularly for the scalar point multiplication formula we have

$$KP = (KP_p, KQ_q)$$

for any Integer K.
If $P(x, y) \in E_{a,b}(Z_N)$ be a point with order greater than two then we can double P, i.e. we can compute $2P(X, Y)$ using the formula
$X = -2x + s^2,$
$Y = -y + s(x - X),$
where

$$s = (3x^2 + a)(2y)^{-1}.$$

2.2 Introduction to Chua- Ling Cryptosystem

Cryptosystem of Chua- Ling is an Asymmetric Key Cryptosystem [5]. This system is based on one-way trapdoor function on elliptic curve over ring. Cryptosystem of Chua- Ling using singular cubic curve of the form :

$$y^2 = x^3 + bx^2$$

over the ring Z_N instead of standard elliptic curve used for cryptography. In ring Z_N, N is publicly known product of two large primes p and q such that
$p = q = 11$ mod 12.
Let us assume that Bob wants to accept encrypted message with Chua- Ling cryptosystem. He selects two large prime p and q such that $p = q = 11$ mod 12. p and q are secret keys of Bob which are kept to be secret. Now, Bob computes

$$N = p \times q$$

where N is public key and Bob announce it publicly. Anyone can send message to Bob using N.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.406-415
https://publishoa.com
ISSN: 1309-3452

Encryption

Now let Alice wants to send message m to Bob. She chooses randomly $\lambda \in Z_N - \{0, \pm 1\}$ and embeds the message m into a point $P = (m^2, \lambda m^3)$ on $C_b(N)$, where $C_b(N)$ is a curve:

$y^2 = x^3 + bx^2 \mod N$

and

$b = (\lambda^2 - 1)m^2 \mod N.$

Alice also computes

$a = \lambda^3 \mod N$

and

$$Q = 2P = (x_Q, y_Q).$$

Alice can compute the value of x_Q & y_Q by simple method of point doubling. Let $P(x, y)$ be given & $Q(x_Q, y_Q)$ be a point on curve such that $Q = 2P$ i.e. Q is the reflection of point of intersection of tangent through point P and curve $C_b(N)$.

Since,

$$y^2 = x^3 + bx^2$$
$$\therefore 2y\frac{dy}{dx} = 3x^2 + 2bx$$
$$2ym' = 3x^2 + 2bx$$
$$m' = (3x^2 + 2bx)(2y)^{-1}$$

where m' is slope of tangent at P.

Also,

$$m' = (y - y')(x - x')^{-1}$$
$$\therefore \ y = m'(x - x') + y'$$
$$^2 = x^3 + bx^2$$
$$\because \ sumofroots = m'^2 - b$$
$$\therefore \ 2x + x' = m'^2 - b$$
$$x' = m'^2 - 2x - b$$
$$x' = (\frac{3x^2+2bx}{2y})^2 - 2x - b.$$

If $P(x, y) = (m^2, \lambda m^3)$ then,

$$x' = (\frac{3m^4+2bm^2}{2\lambda m^3})^2 - 2m^2 - b$$
$$x' = \frac{(3m^2+2b)^2}{4\lambda^2 m^2} - 2m^2 - b.$$

Since,

$$x_Q = x'$$
$$x_Q = \frac{(3m^2+2b)^2}{4\lambda^2 m^2} - 2m^2 - b \ modN$$
$$y' = y + m'(x' - x)$$
$$y' = y + m'(x_Q - x).$$

Also,

$$y_Q = -y'$$
$$\therefore y_Q = -y + m'(x - x_Q)$$
$$y_Q = -\lambda m^3 + \frac{3m^2+2b}{2\lambda}(m^2 - x_Q) \ modN.$$

Now, corresponding to plaintext m Alice sends ciphertext consisting $a, b, x_Q, t = (\frac{y_Q}{N})$ and $u = lsb \ y_Q$ where $t = (\frac{y_Q}{N})$ is Jacobi's symbol of $y_Q \mod N$.

Decryption

Since Bob knows the factorization of N i.e. he knows p and q so he can recover plaintext m from ciphertext $\{a, b, x_Q, t, u\}$ sent by Alice.

From x_Q Bob computes the unique y_Q satisfying

$y_Q^2 = x_Q^3 + bx_Q^2 \mod N$

with Jacobi's symbol t and $lsb \ u$.

He set

$$Q = (x_Q, y_Q)$$

Since Bob knows the factorization of

$$N = p \times q.$$

Therefore, by taking
$Q_p = Q \mod p$
$Q_q = Q \mod q.$
Bob computes
$P_{i,p} = (x_{i,p}, y_{i,p}), \quad (i = 1,2)$
such that
$2[P]_{i,p} = Q_p$ on $C_p(b)$.

Similarly Bob computes $P_{i,q}$
Next, he computes
$I_p = [i: a^2 = y_{i,p}^6 x_{i,p}^{-9} \ (\mod p)]$.
He does same for the prime q.
Finally, he calculates
$m_p = y_i^3 x_i^{-4} a^{-1} \mod p \quad (i = I_p)$
and in similar manner he computes m_q.
Now, Bob recover m using Chinese Remainder Theorem such that
$m = m_p \mod p$
$m = m_q \mod q.$

2.3 The Reduction of Chua - Ling Cryptosystem to Cryptosystem of Rabin -Williams

If m be the plaintext then we can recover the value of m^2 from ciphertext send by Alice to Bob and the cryptosystem reduced to Rabin- Williams Cryptosystem, which is the draw back of Chua-Ling cryptosystem [7]. Since Alice embeds the plaintext m into a point $P = (m^2, \lambda m^3) \in C_N(b)$ where
$C_N(b): y^2 \equiv x^3 + bx^2 \mod N$
since

$$Q(x_Q, y_Q) = 2P(m^2, \lambda m^3)$$

where
$x_Q \equiv (3m^2 + 2b)^2 (4\lambda^2 m^2)^{-1} - 2m^2 - b \mod N$
Now we construct a polynomial $P_1[X] \in Z_N[X]$ whose root is m^2 by puting $m^2 = X$ in above equation, we get
$x_Q \equiv (3X + 2b)^2 (4\lambda^2 X)^{-1} - 2X - b \mod N$
$\Rightarrow x_Q + 2X + b \equiv (3X + 2b)^2 (4\lambda^2 X)^{-1} \mod N$
$\Rightarrow 4(x_Q + 2X + b)\lambda^2 X \equiv (3X + 2b)^2 \mod N$

Since,

$$b = (\lambda^2 - 1)m^2 \Rightarrow b + m^2 = \lambda^2 m^2 \Rightarrow b + X = \lambda^2 X$$

Therefore

$$4(x_Q + 2X + b)(b + X) - (3X + 2b)^2 \equiv 0 \mod N$$

Thus, $P_1[X] = 4(x_Q + 2X + b)(b + X) - (3 + 2b)^2$ over $Z_N[X]$ be the required polynomial obtained from ciphertext whose one root is m^2.
Also,

$$P(m^2, \lambda m^3) \in C_N(b)$$

$\therefore$ $P(m^2, \lambda m^3)$ satisfy $y^2 \equiv x^3 + bx^2 \mod N$
$\Rightarrow (\lambda m^3)^2 \equiv (m^2)^3 + b(m^2)^2 \mod N$
$\Rightarrow \lambda^2 m^6 \equiv m^6 + bm^4 \mod N$
$\Rightarrow \lambda^2 m^2 \equiv m^2 + b \mod N$

Again we can construct a polynomial $P_2[X] \in Z_N[X]$ whose one root is m^2.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.406-415
https://publishoa.com
ISSN: 1309-3452
Put $m^2 = X$ in above congruence relation, we get

$\lambda^2 X \equiv X + b \mod N.$
On cubing both side, we get
$(\lambda^2 X)^3 = (X + b)^3 \mod N$
$\Rightarrow (\lambda^3)^2 X^3 \equiv (X + b)^3 \mod N$

Since,

$$a = \lambda^3$$

Therefore,
$a^2 X^3 \equiv (X + b)^3 \mod N$
$\Rightarrow a^2 X^3 - (X + b)^3 \equiv 0 \mod N$

Further,

$$P_2[X] = a^2 X^3 - (X + b)^3 \text{ over } Z_N[X].$$

whose one root is m^2.
Since m^2 is root of $P_1[X]$ and $P_2[X]$.
$\therefore$ m^2 is a root of $R[X] = gcd(P_1[X], P_2[X])$. The polynomial $R[X]$ is very likely to be a polynomial of degree one. On solving this polynomial in X we get the value of m^2.

3. Main Result

In the present section, the security of Chua- Ling cryptosystem and Rabin- Williams cryptosystem are equivalent because from the given ciphertext of Chua- Ling cryptosystem it can be reduced to cryptosystem of Rabin- Williams, We propose a method which makes the reduction of Chua- Ling Cryptosystem to Rabin- Williams Cryptosystem difficult. Further, We provide Authentication Scheme for Chua- Ling Cryptosystem based on Digital Signature Algorithm that provides Integrity and Authentication and further makes some concluding remarks.

3.1 Proposed Method

Encryption:

If Alice wants to send a message m to Bob then she chooses

$$\lambda \in Z_N - \{0, \pm 1\}$$

and sets

$$P = (m^2, \lambda m^3).$$

Next, she computes

$$a = \lambda^3 \mod N$$

and

$$b = (\lambda^2 - 1) m^2 \mod N.$$

She finds

$$Q(x_Q, y_Q) = 2P$$

and

$$R(x_R, y_R) = 2Q.$$

Now as a ciphertext Alice send $\{a, b, x_R, t = (\frac{y_R}{N}), u = lsby_R, lsbx_Q, lsby_Q, t' = (\frac{y_Q}{N})\}$ corresponding to plaintext m.

Decryption:

For decryption Bob calculates y_R with symbol t and $lsb\ u$.
He set

$$R = (x_R, y_R)$$

and finds

$$(R_p, R_q).$$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.406-415
https://publishoa.com
ISSN: 1309-3452
Next, he computes

$$Q_{i,p} = (x_{i,p}, y_{i,p}) \quad (i = 1,2)$$

and

$$Q_{i,q} = x_{i,q}, y_{i,q}) \quad (i = 1,2).$$

Because Bob know the factorization of N so he can find all Q_i with the help of Chinese Remainder Theorem such that

$$2Q = R.$$

He select a Q_i with type $lsb\ x_Q$, $lsb\ y_Q$ and $(\frac{y_Q}{N})$. After selecting Q he find P according to Chua-Ling cryptosystem and recover message m.

Now, to recover the value of m^2 Eve have to form a polynomial $P_1[X]$ from

$$x_R = (\frac{3x_Q^2+2bx_Q}{2y_Q})^2 - 2x_Q - b \mod N.$$

Since Eve does not know the value of x_Q and y_Q so he can not find $P_1[X]$ directly.

Also,

$$x_Q = \frac{(3m^2+2b)^2}{4\lambda^2 m^2} - 2m^2 - b \mod N$$

$$y_Q = -\lambda m^3 + \frac{3m^2+2b}{2\lambda}(m^2 - x_Q) \mod N$$

using the values in the above equation we get,

$$x_R = \frac{6}{\lambda m}\left[\frac{(3m^2+2b^2)^2 - 8m^4\lambda^2 + 4bm^2\lambda^2}{-8m^6\lambda^4 + (3m^2+2b)(12m^4\lambda^2 - (3m^2+2b)^2 + 4bm^4\lambda^2)}\right][(3m^2+2b)^2 - 8m^2\lambda^2 - 4bm^4\lambda^2] - \frac{(3m^2+2b)^2}{2m^2\lambda^2} + b$$

From here we can see that Eve can not find a polynomial whose root is m^2. Therefore by this modification in Chua-Ling Cryptosystem , it is difficult to reduce it into Rabin-Williams Cryptosystem which gives more security to modified Chua-Ling Cryptosytem.

3.2 Illustration 1

Let us proceed with the illustration of Chua- Ling cryptosystem to understand this modification. Let, the message $m = 5$ is embeded into the point

$$P = (25,122)$$

over the elliptic curve

$C_{200}(253): y^2 = x^3 + 200x^2 \mod 253.$

Alice encrypts the point P into the point Q, where

$$Q = 2P.$$

Now the point P is encrypted into the point R, where

$$R = 2Q = 4P.$$

From Chua-Ling procedure, Alice knows that $Q = (78,93)$. Now, she calculates R by doubling point Q.

If

$$Q = (x_Q, y_Q)$$

and

$$R = (x_R, y_R).$$

Then,

$$x_R = [\frac{3x_Q^2+400x_Q}{2y_Q}]^2 - 2x_Q - 200 mod 253$$
$$= [\frac{3(78)^2+400\times 78}{2\times 93}]^2 - 2\times 78 - 200 mod 253$$
$$= 243$$

and

$$y_R = -y_Q + [\frac{3x_Q^2+400x_Q}{2y_Q}](x_Q - x_R) mod 253$$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.406-415
https://publishoa.com
ISSN: 1309-3452

$$= -93 + [\frac{3(78)^2+400\times 78}{2\times 93}](78-243) mod 253$$
$$= -93 + 70(-165) mod 253$$
$$= 248.$$

Now Alice sends ciphertext $\{27,200,243,1,8,8,3,1\}$ corresponding the plaintext $m = 5$.
After receiving the ciphertext Bob computes the elliptic curve:
$C_{200}(253): y^2 = x^3 + 200x^2 \mod 253$
and computes

$$y_R^2 = x_R^3 + 200x_R^2 mod 253$$
$$= (243)^3 + 200(243)^2 mod 253$$
$$= 26158707 mod 253$$
$$= 25.$$

Since Bob knows the factorization of 253, so he can calculate the values of y_R.
Possible values of y_R are $5,28,225,248$. From the data given in ciphertext Bob chooses

$$R = (243,248).$$

Bob finds

$$R_{11} = (1,6)$$

$$R_{23} = (13,18)$$

and computes,

$$Q_{11} = (1,5)$$

and

$$Q_{23} = (9,1),$$

such that

$$2Q_p = R_p.$$

With the help of Chinese Remainder Theorem Bob computes

$$Q = (78,93).$$

After computing Q Bob find required message from Chua- Ling decryption procedure.

3.3 Authentication Scheme for Chua-Ling Cryptosystem using Digital Signature Algorithm

We know that for authentication of entity, we produce a digital signature in which message digest is encrypted by private key of sender and message digest is decrypted by public key of sender. Receiver also calculates the message digest of accepted message, if this message digest match with decrypted message digest then message is accepted. This digital signature provide both integrity and authentication. In this section, we provides Digital Signature Algorithm based on Chua-Ling cryptosystem.

Authentication:

For authentication of message m Alice find $H(m)$ where $H(m)$ is message digest of Hash Function[6]. She selects p and q both congruent to $11 \mod 12$ in such a way that $H(m) \in Z_{N^*}$ where $N = p \times q$. Now she embeds $H(m)$ in the point $Q = (H(m), y)$ where y is any number in Z_N. Next she computes

$$b = \frac{y^2 - H(m)^3}{H(m)^2} \mod N.$$

Point Q lies on the singular cubic curve of the form

$C_N(b): y^2 = x^3 + bx^2 \mod N.$

Now, Alice computes Q_p and Q_q where

$$Q_p = Q \mod p$$

and

$$Q_p = Q \mod q.$$

She compute

$$P_{i,p} = (x_{i,p}, y_{i,p}) \ (i = 1,2)$$

such that,

$$2P_{i,p} = Q_p$$

and

$$P_{i,q} = (x_{i,q}, y_{i,q}) \ (i = 1,2)$$

such that

$$2P_{i,q} = Q_q.$$

By using Chinese Remainder Theorem she find all $P_i(i = 1,2,3,4)$ such that $2P_i = Q$. Out of all P_i she select one P_i as P and send $\{P, b, N\}$ as signature for m.

Verification:

For verification Bob finds $2P = Q = (x_Q, y_Q)$ over $y^2 = x^3 + bx^2 \mod N$. He also finds hash value of accepted message m'. If $H(m') = x_Q$ then message accepted.

3.4 Illustration 2

Let 223 be the hash value of message. Alice selects two primes p and q both are congruent to $11 \mod 12$ in such a way that hash value of message i.e. 223 has multiplicative inverse in Z_{223^*}. Alice selects $p = 11$ and $q = 23$. Now, Alice sets $y = 130$ (randomly choosen) and finds

$$b = \frac{y^2 - x^3}{x^2} \ mod 253$$
$$\therefore \ b = \frac{130^2 - 223^3}{223^2} \ mod 253$$
$$b = 105.$$

Alice embed the hash value of message in point $Q = (223,130)$ over curve:
$y^2 = x^3 + 105x^2 \mod 253.$
Now, Alice finds $Q_{11} = (3,9)$ and $Q_{23} = (16,15)$. Alice find one point $P_{11} = (3,2)$ and one point $P_{23} = (13,22)$ such that $2P_{23} = Q_{23}$.
Alice solves

$$x = 3 \ mod 11$$
$$x = 13 \ mod 23$$
$$x = 36$$

and solves

$$y = 2 \ mod 11$$
$$y = 22 \ mod 23$$
$$y = 68.$$

Alice sends $\{(36,68),105,253\}$ as a signature for message.

Verification:

Bob accepts the message m' from Alice and $\{(36,68),105,253\}$ as a signature for message. He set $P = (36,68)$ and find $2P = Q$ for curve
$y^2 = x^3 + 105x^2 \mod 253.$
If x- coordinate of Q is equal to hash value of m' i.e. $H(m')$ then message is accepted.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.406-415
https://publishoa.com
ISSN: 1309-3452

3.5 Conclusion

In this paper we modify Chua- Ling Cryptosystem which makes it difficult to reduce it into Rabin-William Cryptosystem. Our proposed method provides difficult for adversary to attack this modified cryptosystem which provides security to the cryptosystem and further we have propose the authentication scheme that provides integrity and authenticity to the cryptosystem.

****

References

[1] Hankerson, Darrel, Menezes, Alfred J., Vanstone, Scott, Guide to Elliptic Curve Cryptography, Springer-Verlag,2004.

[2] Diffie, W. and Hellman, "New Directions in Cryptography."IEEE Trans On Information Theory, IT-22, vol.6, pp.644-654, 1976.

[3] T. ElGamal. "A Public Key Cryptosystem and Signature Scheme based on Discrete Logarithms." IEEE Trans. On Information Theory 31 vol.4, pp.469-472, 1985.

[4] H. W. Lenstra, "Factoring integers with elliptic curves", Annals of Mathematics 126, pp. 649-673,1987.

[5] Chua, S.K. and Ling S., A Rabin-type scheme based on $y^2 = x^3 + bx^2$ mod n., International Computing and Combinatorics Conference., Springer, Berlin, Heidelberg, 1997.

[6] Ganesan, G. and Sobti, R., Cryptographic hash functions review, International Journal of Computer Science Issues (IJCSI) 9.2,461, 2012.

[7] Joye, M. and Quisquater, J.J., Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams, Designs, codes and Cryptography 14.1, 53-56, 1998.

[8] Leonard, A.M., Shamir, A. and Rivest, R.L., A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 26.1, 96-99, (1983).

[9] Meyer, B. and Müller, V., A public key cryptosystem based on elliptic curves over Z_n equivalent to factoring, International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1996.

[10] Miller, V.S., Use of elliptic curves in cryptography. Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1985.

[11] Mohammed, F. and Nisha, S., RSA Public Key Cryptography Algorithm–A., International Journal of Scientific and Technology Research 6,187-191,2017.

[12] Neal, K., Elliptic curve cryptosystems, Mathematics of computation 48, 177, 203-209, 1987.

[13] Vo, S.C., A Survey of Elliptic Curve Cryptosystems, NASA Advanced Supercomputing Division, NAS Technical Report—NAS-03-012 (2003).

[14] K. Kurosawa, K. Okada, S. Tsujii: Low exponent attack against elliptic curve RSA, Advances in Cryptology-ASIACRYPT ’94, Lecture Notes in Computer Science,917 (1995), Springer-Verlag, 376-383.

[15] Koyama, K., Maurer, U., Okamoto, T., Vanstone, A., New public-key scheme based on elliptic curves over the ring Z_n, pp. 252-266, LNCS 576, Advances in Cryptography -Crypt’91. Santa Barbara, California, Joan Feigenbaum (ed.), Springer-Verlag, 1992.

[16] N. Demytko, A new elliptic curve based analogue of RSA, pp. 40-49, LNCS 765, Adances in Cryptography-Eurcrypt '93, Lofthus, Norway, Tor HElleseth (ed.) Springer-Verlag, 1994.

[17] Koyama, K., Kuwakado, H., Efficient cryptosystem over elliptic curves based on a product of form-free primes, pp. 1309-1318, IEICE Transactions of Fundamentals on Electronic Communications Computer Science, E77-A,8,1994.