A PUBLIC KEY CRYPTOSYSTEM BASED ON PELL EQUATION

Sahadeo Padhye
School of Studies in Mathematics,
Pt.Ravishankar Shukla University,
Raipur (C.G.),India.
Email: *sahadeo_mathrsu@yahoo.com*

Abstract. RSA type public key cryptosystems based on the Pell's equation are proposed in the honor of an Indian mathematician Brahmgupta who studied Pell's equation long before European mathematicians came to know about it. Three RSA type schemes are proposed, first two are not semantically secure where as the other two schemes are semantically secure. The decryption speed of the proposed schemes is about two times as fast as RSA for a 2 log n-bit message. It is shown that the proposed schemes are more secure than the RSA scheme when purely common plaintexts are encrypted in the broadcast application and are as secure as the RSA scheme against ciphertext attack. In addition the proposed schemes are also secure against partially known plaintext attack. First two are not semantically secure but the third one is semantically secure.

Key Words : Pell's Equation , Public key cryptosystem, RSA scheme, KMOV scheme.
2000 Mathematical Classification No. 94A60.

1. Introduction

The investigation related to the construction of safe and effective public key cryptosystem (PKC) begun with the seminal paper of Diffie and Hellman [9] using hard mathematical problem. Today, discrete logarithm and the integer factorization problem are the problems commonly used in the construction of PKC [27]. The factorization problem was first time used in 1978, by Rivest, Shamir and Adleman for the construction of public key cryptosystem, known as RSA [26] PKC. The number theoretic problem used in the standard RSA is based on the structure of the multiplicative group $\mathbb{Z}_n^\star$ where n is the product of two large primes. In the 1980s, researchers noticed another source, the nonsingular cubic curve (elliptic curve) [15, 21], which can be used as hard problem for PKC construction. The elliptic curves are found remarkably useful in a wide range of applications such as primality testing and integer factorization [19, 20]. Another potential use

Key words and phrases. Singular Curve, RSA, Signature Scheme.
This work is supported under CSIR (JRF) scheme, India (2002).

of elliptic curve is designing the public-key cryptosystems analogue to the existing schemes. Koyama et al [14] introduced first analogue of the RSA scheme, called KMOV scheme, based on elliptic curve. However, the decryption speed of the KMOV scheme is 5.8 times as slow as RSA scheme. Later, Demytko [8] introduced more advanced analogue of RSA scheme based on elliptic curve to overcome the shortcomings of KMOV scheme. The decryption speed of the Demytko scheme is but, slower than the KMOV scheme. The problem of nonsingular cubic curve was than replaced by singular cubic curve in the papers of Koyama [16] and Kuwadado et al [12, 13] for the construction of an analogue to the RSA scheme. The decryption speed of the scheme given by Koyama [16] is about two times faster then the RSA scheme. But its encryption is slower than RSA scheme. Also the schemes based on cubic curve such as [12, 14, 16, 13] are not secure against partially known plaintext attack [24]. Now, we replace the singular cubic curve by Pell's equation to increase the encryption speed and propose three RSA type public key cryptosystems.

It is not out of place to mention that the equation now known as Pell's equation was studied in depth for 1000 years before Pell was born by an Indian mathematician Brahmagupta in 628 AD [6, 28, 18]. He gave a method called *Samasa* and made number of discoveries regarding Pell's equation. Eular, who named it Pell's equation, was unaware of this fact at that time. In 1150, another Indian mathematician Bhaskara II, gave an algorithm called *Chakravala* to produce a solution to Pell's equation [6]. During 14^{th} century, Narayana, also an Indian mathematician, gave an example of said method of Bhaskara II [6]. Hence, the public key cryptosystems we present here to honor the said work of Brahmgupta. Although, some efforts were made to use Pell's equation for PKC construction [22, 2] but either the techniques were found less feasible mathematically or the technique was not so efficient. In addition, the system [2] is not semantically secure.

The significance of the proposed cryptosystems is that those are two times faster than the RSA scheme and also somewhat faster than the scheme given by Koyama [16]. The proposed schemes are as secure as RSA scheme against chosen ciphertext attack. The proposed schemes are also secure against partially known plaintext attack [24]. We show that the proposed schemes are more secure than RSA scheme when purely common plaintexts are encrypted in the broadcast application. In addition, the addition operation in the proposed schemes is computationally less expensive than the schemes based on the cubic curve [12, 14, 16, 13].Thus the encryption processes are more efficient than the other RSA type cryptosystems based on the cubic curve. Our proposed first two schemes are not semantically secure. Kouchi et al [17]proposed a variant of RSA cryptosystem with the property of semantic security. Some other variants of RSA with semantic security are [4, 25]. Finally, using the idea of Kouchi et al [17] we improve our second scheme to semantically secure public key cryptosystem.

2. Preliminary

A Diophantine equation of the form

$$x^2 - Dy^2 = 1 \tag{1}$$

where D is a positive integer, is known as Pell's equation.

Let p be an odd prime and D be a nonzero quadratic residue element in F_p. Let C_p denotes the set of solutions $(x, y) \in F_p \times F_p$ to the Pell's equation

$$x^2 - Dy^2 \equiv 1(mod\ n) \tag{2}$$

We define the addition operation $\oplus$ on C_p as follows.

The sum (x_3, y_3) of (x_1, y_1) and (x_2, y_2) in F_p is computed as,

$$(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2) = (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1) \tag{3}$$

If we define the identity by $(1, 0)$ and the inverse of (x, y) by $(x, -y)$, then it is easy to verify that the addition operation $\oplus$ is closed, associative and commutative. Thus, C_p forms an abelian group under the operation $\oplus$. For any positive integer e, the multiplicative operation $\otimes$ is defined as follows,

$$e \otimes (x, y) = \overbrace{(x, y) \oplus (x, y) \oplus (x, y) \oplus (x, y) \oplus (x, y) \oplus .... \oplus (x, y)}^{etimes} \tag{4}$$

We can use the following recursion formulas for the addition operation in $(C_p, \oplus)$

If $i \times (x_1, y_1) = (x_i, y_1)$ then,

$$\begin{aligned} x_{2i} &= x_i^2 + Dy_i^2 = 2x_i^2 - 1 \\ y_{2i} &= 2x_iy_i \\ x_{2i+1} &= 2x_ix_{i+1} - x_1 \\ y_{2i+1} &= 2x_iy_{i+1} - y_1 \end{aligned} \tag{5}$$

Case I : If the value of e is odd then ,

$$\begin{aligned} e \otimes (x, y) = (a_{e,1}x^e + a_{e,2}Dx^{e-2}y^2 + a_{e,3}D^2x^{e-4}y^4 + .. + a_{e,\frac{e+1}{2}}D^{\frac{e-1}{2}}xy^{e-1}, \\ a_{e,\frac{e+1}{2}}x^{e-1}y + a_{e,\frac{e-1}{2}}Dx^{e-3}y^3 + ... + a_{e,2}D^{\frac{e-3}{2}}x^2y^{e-2} + a_{e,1}D^{\frac{e-1}{2}}y^e) \end{aligned} \tag{6}$$

Where

$a_{e,n} = \sum_{i=1}^{e-(2n-3)} S_i$ and $S_i = 1 + \sum_{j=2n-3}^{i+2n-5} a_{j,n-1}$ and $S_1 = 1$.

$a_{e,1} = 1 \forall e$,

$a_{e,2} = 1 + 2 + 3 + 4 + 5 + e - 1^{th}$ terms.

$a_{e,3} = 1 + (1 + a3, 2) + (1 + a3, 2 + a4, 2) + e - 3^{th}$ terms.

$a_{e,4} = 1 + (1 + a_{5,3} + (1 + a_{5,3} + a_{6,3}) + e - 5^{th}$ terms.

.....

.....

.....

$a_{e,\frac{e+1}{2}} = 1 + (1 + a_{e-2}, \frac{e-1}{2})$

Case II :

If e is even integer then ,

$$e \otimes (x,y) = (a_{e,1}x^e + a_{e,2}Dx^{e-2}y^2 + a_{e,3}D^2x^{e-4}y^4 + ... + a_{e,\frac{e}{2}}D^{\frac{e}{2}-1}x^2y^{e-2},$$
$$b_{e,1}x^{e-1}y + b_{e,2}Dx^{e-3}y^3 + b_{e,3}D^2x^{e-5}y^5 + ... + b_{e,\frac{e}{2}}D^{\frac{e}{2}-1}xy^{e-1}) \quad (7)$$

where ,

1. Formula for $a_{e,i}$ is same as for odd value of $e \forall e$ and $i = 1, 2, 3.... \frac{e}{2} + 1$

2. $b_{e,r} = b_{e,s}$ if $r + s = \frac{e}{2} + 1$ and $b_{e,r} = a_{e-1,\frac{e}{2}-r+1} + a_{e-1,r}$.

3.$b_{e,r} = 2 \times a_{e-1,\frac{e+2}{2}}$ if $2 \times r = \frac{e}{2} + 1$.

For Example :

$2 \times (x,y) = (x^2 + Dy^2, 2xy)$

$3 \times (x,y) = (x^3 + 3Dxy^2, 3x^2y + Dy^3)$

$4 \times (x,y) = (x^4 + 6Dx^2y^2 + D^2y^4, 4x^3y + 4Dxy^3)$

$5 \times (x,y) = (x^5 + 10Dx^3y^2 + 5D^2x^2y^4, 5x^4y + 10Dx^2y^3 + D^2y^5)$

$6 \times (x,y) = (x^6 + 15Dx^4y^2 + 15D^2x^2y^4 + D^3y^6, 6x^5y + 20x^3y^3 + 6D^2xy^5)$

$7 \times (x,y) = (x^7 + 21Dx^5y^2 + 35D^2x^3y^4 + 7D^3xy^6, 7x^6y + 35Dx^4y^3 +$
$21D^2x^2y^5 + D^3y^7)$

$8 \times (x,y) = (x^8 + 28Dx^6y^2 + 70D^2x^4y^4 + 28D^3x^2y^6 + D^4y^8,$
$8x^7y + 56Dx^5y^3 + 56D^2x^3y^5 + 8D^3xy^7)$

$9 \times (x,y) = (x^9 + 36Dx^7y^2 + 126D^2x^5y^4 + 84D^3x^3y^6 + 9D^4xy^8,$
$9x^8y + 84Dx^6y^3 + 126D^2x^4y^5 + 36D^3x^2y^7 + D^4y^9)$

.....

.....

Remarks.

1 $(a \times b) \otimes (x,y) = a \otimes (b \otimes (x,y)) = b \otimes (a \otimes (x,y)) = (a \otimes (x,y)) \oplus (b \otimes (x,y))$

2 $a \otimes \{(x_1,y_1) \oplus (x_2,y_2)\} = a \otimes \{(x_1,y_1)\} \oplus \{a \otimes (x_2,y_2)\}$

Lemma 1. [20] *$(C_p, \oplus)$is a cyclic group of order $p-1$.*

A group $(C_p, \oplus)$ is isomorphic to $F_p{}^\star$. The isomorphism mapping ψ from $(C_p, \oplus)$ to $F_p{}^\star$ is given by the following theorem.

Theorem 1. [20] *The mapping $\psi : C_p \to F_p{}^\star$ defined by*

$$\psi : (1,0) \to 1 \text{ and } \psi : (x,y) \to x - ay (mod\ p)$$

where $(x,y) \in C_p$ and $a^2 \equiv D (mod\ p)$ is an isomorphism. The group isomorphism mapping $\psi^{-1} : F_p{}^\star \to C_p$ is defined by

$$\psi^{-1} : 1 \to (1,0) \text{ and } \psi^{-1} : u \to (\tfrac{u+u^{-1}}{2}, \tfrac{u^{-1}-u}{2a})(mod\ p)$$

Since C_p is a cyclic group of order $p-1$, we have that if $k \equiv 1 (mod\ p-1)$, then $(x,y) \equiv k \otimes (x,y) (mod\ p)$.

Now let n be the product of two large primes p and q. $\mathbb{Z}_n^\star$ denotes a multiplicative group of $\mathbb{Z}_n$. From *Theorem 1* it is easy to develop the following theorem .

Theorem 2. *The mapping $\psi : C_n \to \mathbb{Z}_n{}^\star$ defined by*

$$\psi((1,0)) = 1(mod\ n)\ and\ \psi((x,y)) = x - ay(mod\ n),$$

where $(x,y) \in C_n$ *and* $a^2 \equiv D(mod\ n)$ *is a group isomorphism from* C_n *to* ${\mathbb{Z}_n}^\star$.

And the inverse isomorphism $\psi^{-1} : {\mathbb{Z}_n}^\star \to C_n$ *is defined by*

$$\psi^{-1}(1) = (1,0)(mod\ n)\ and\ \psi^{-1}(u) = (\tfrac{u+u^{-1}}{2}, \tfrac{u^{-1}-u}{2a})(mod\ n)$$

where $u \in {\mathbb{Z}_n}^\star$.

According to the definition of the mapping ψ and the addition $\oplus$ and the multiplication $\otimes$ operation we have the following results over the ring ${\mathbb{Z}_n}^\star$.

Theorem 3. *If* $(x_i, y_i) \equiv i \otimes (x,y)$ *over* C_n, *we have* $(x_i, y_i) \equiv (x - ay)^i (mod\ n)$.

The following theorem is a base of a pair of an encryption and a decryption of public key cryptosystem over C_n.

Theorem 4. *Let* n *be the product of primes* p *and* q, *and* $N = lcm(p-1, q-1)$. *For any integer* k *satisfying* $k \equiv 1(mod\ lcm(p-1, q-1))$, *we have*

$$(x,y) \equiv k \otimes (x,y)(mod\ n)\ ,\ for\ all\ (x,y) \in C_n.$$

3. Construction of PKC

In this section three RSA-type schemes based on Pell's equation over $\mathbb{Z}_n$ are presented. The security of the proposed scheme is based on the difficulty of factoring n, which is the product of two large primes. In these schemes, a plaintext pair (M_x, M_y) with $M_x, M_y \in \mathbb{Z}_n^\star$ is encrypted. The main difference between first two schemes is the way of encryption. One uses formula (3) and (6) while other uses exponentiation by using isomorphism. Since, first two schemes are not semantically secure; we improve **scheme-2** as the **scheme-3** to get semantically secure public key cryptosystem. The key generation of both the schemes is same as given below.

3.1. **Key Generation.** Recipient (R say) chooses two large primes p and q. Let $n = pq$ and $N = lcm(p-1, q-1)$. R determines an integer e satisfying $gcd(e, N) = 1$. Decryption keys d is computed from encryption key e as $d = e^{-1} mod N$ by using the Euclidean algorithm. The pair (e, n) is the public key and secrete key is (p, q, d).

3.2. **Scheme I.** Assume that a sender S wants to sends the messages $M_y \in \mathbb{Z}_n^\star$ to the recipient R.

3.2.1. *Encryption.* To encrypt the messages the sender proceeds as follows:

(1) Compute $Z_1 \equiv M_x M_y (mod\ n)$ and $Y = M_y$.
(2) Solve the equations $X - aY \equiv Z_1$ and $X + aY \equiv {Z_1}^{-1}$ over $\mathbb{Z}_n$.
(3) Get $X \equiv \frac{(Z_1 + {Z_1}^{-1})}{2} (mod\ n)$ and $a \equiv \frac{({Z_1}^{-1} - X)}{Y} (mod\ n)$, $D \equiv a^2 (mod\ n)$. Then (X, Y) is the solution of the Pell equation $x^2 - Dy^2 \equiv 1$ over $\mathbb{Z}_n$.
(4) Using the recursion formula (5) or the equation (3) and (6) ,S computes $(C_x, C_y) \equiv e \otimes (X, Y)$.
(5) Send the complete ciphertext (C_x, C_y, a) to the receiver R.

3.2.2. *Decryption.* After receiving the ciphertext (C_x, C_y, a) recipient R first checks that $({C_x}^2 - a^2{C_y}^2)(mod\ n) \equiv 1$. If yes, he/she then proceeds as follows:

(1) Compute $C \equiv f(C_x, C_y) \equiv C_x - aC_y mod\ n$.
(2) Compute the value $M \equiv C^d (mod\ n)$.
(3) Evaluate $X \equiv \frac{(M^{-1}+M)}{2}(mod\ n)$ and $Y \equiv \frac{(M^{-1}-M)}{2a}(mod\ n)$. Clearly $Z_1 \equiv M$ and $Y \equiv M_y$.
(4) Compute $M_x \equiv \frac{M}{Y} mod\ n$ and $M_y = Y$.

3.3. **Scheme II.** Assume that a sender S wants to send the messages M_x and $M_y \in \mathbb{Z}_n^\star$ to the recipient R.

3.3.1. *Encryption.* To encrypt the messages M_x and M_y sender S proceeds as follows:

(1) Compute $Z_1 \equiv (M_x M_y) mod\ n$ and $Y = M_y$.
(2) Solve the equations $X - aY \equiv Z_1$ and $X + aY \equiv Z_1^{-1}$ over $\mathbb{Z}_n$.
(3) Get $X \equiv \frac{(Z_1+Z_1^{-1})}{2}(mod\ n)$ and $a \equiv \frac{(Z_1^{-1}-X)}{Y}(mod\ n)$, $D \equiv a^2 mod\ n$. Then (X, Y) is the solution to the Pell's equation $x^2 - Dy^2 \equiv 1$ over $\mathbb{Z}_n$.
(4) Using *Theorem 2*, compute $M \equiv (X - aY) mod\ n$ and $C = M^e mod\ n$.
(5) Send the complete ciphertext (C, a) to the recipient R.

3.3.2. *Decryption.* After receiving the ciphertext (C, a) the recipient R proceeds as follows:

(1) Compute $M \equiv C^d (mod\ n)$.
(2) Using *Theorem 2*, compute $X \equiv \frac{(M^{-1}+M)}{2}$ and $Y \equiv \frac{(M^{-1}-M)}{2a}$. This implies that $Z_1 \equiv M$.
(3) Compute $M_y = Y$ and $M_x \equiv \frac{M}{Y}$.

Above two schemes are not semantically secure. To get semantically secure public key cryptosystem we generalize the scheme-II as below.

3.4. **Scheme III.** Assume that the sender S wants to send the messages M_x and $M_y \in \mathbb{Z}_n^\star$ to the recipient R. In this scheme, a one-way function $f : \mathbb{Z}_n^\star \to \mathbb{Z}_n^\star$ is used as a system parameter. For example, we take the one way function defined by Kouichi et al [17] i.e. most significant bits zeroes (MSBZ) function defined below.

Let r be a k-bit random integer in $\mathbb{Z}_n^\star$. The binary representation of r is $r = r_0 2^0 + r_1 2^1 + r_2 2^2 + ... + r_l 2^l + r_{l+1} 2^{l+1} + ... + r_{k-1} 2^{k-1}$. The one-way function introduced by Kouichi et al [17] was $f_{MSBZ}^{e,n}(r) = (r - MSBZ_l(r))^e mod\ n$ where l is large enough. Here, $r - MSBZ_l(r)$ denotes the l most significant bits of r equal to zero i.e. $r - MSBZ_l(r) = r_0 2^0 + r_1 2^1 + r_2 2^2 + ... + r_l 2^l$. This one-way function was named after most significant bits zeroes function $(MSBZ)$.

3.4.1. *Encryption.* To encrypt the messages M_x and M_y the sender S proceeds as follows

(1) Compute $Z_1 \equiv (M_x M_y) mod\ n$ and $Y = M_y$.
(2) Solve the equations $X - aY \equiv Z_1$ and $X + aY \equiv Z_1^{-1}$ over $\mathbb{Z}_n$.
(3) Get $X \equiv ((Z_1 + Z_1^{-1})/2)(mod\ n)$ and $a \equiv ((Z_1^{-1} - X)/Y)(mod\ n)$, $D \equiv a^2 mod\ n$. Then (X, Y) is the solution of the Pell's equation $x^2 - Dy^2 \equiv 1$ over $\mathbb{Z}_n$.
(4) Using *Theorem 2*, compute $M \equiv (X - aY) mod\ n$.
(5) Chose a random element $r \in \mathbb{Z}_n^\star$ and compute $C_0 = r^e mod\ n$.
(6) Compute $C_1 = (f(r) + MC_0) mod\ n$ and $b = (a + r^2) mod\ n$.
(7) Send the complete ciphertext (C_0, C_1, b) to the recipient R.

3.4.2. *Decryption.* After receiving the ciphertext (C_0, C_1, b) the recipient R proceeds as follows:

(1) First compute $r = c_0^d mod\ n$ and $a = b - r^2 mod\ n$.
(2) Compute $M \equiv C_0^{-1}(C_1 - f(r))(mod\ n)$.
(3) Using *Theorem 2*, obtain $X \equiv (M^{-1}+M)/2$ and $Y \equiv (M^{-1}-M)/2a$.
(4) This implies that $Z_1 \equiv M$. Hence the original message is obtained by $M_y = Y$ and $M_x \equiv (M/Y)$.

4. Efficiency and Security

4.1. **Efficiency.**

4.1.1. *Comparison with RSA.* We first compare our schemes with the standard RSA [26] scheme. Here, we focus on the decryption procedure to evaluate the average number of modular multiplications. In general, $M \equiv C^d (mod\ n)$ requires $1.5 log\ d$ multiplications *modulo* n on average. Besides, the cost of isomorphism mapping requires two modular inverses and one modular multiplication. In addition, to compute M_x, one modulo multiplication and one inverse is required during the decryption process. Since, one modulo inverse requires six modulo multiplications [7, 8], the decryption of first two schemes requires $1.5 log\ d + 20$ modular multiplication on average whereas the scheme-III requires $1.5 log\ d + 28$ modular multiplication on average. Neglecting the cost of isomorphic mapping, the proposed schemes have almost the same decryption time as RSA scheme. In our schemes $2 - log\ n$ bit message is encrypted at a time, so block size is two times larger than the standard RSA cryptosystem. In the standard RSA scheme, to decrypt for $2 - log\ n$-bit message requires $3 log\ d$ multiplication *modulo* n on average. Thus, the decryption efficiency of our proposed cryptosystems would be about two times faster than that of the RSA scheme for a k bit long message if $\lceil k/log\ n \rceil$ is even.

4.1.2. *Comparison with Koyama scheme.* Now we compare our scheme-1 with the Koyama scheme-1 [16], for decryption process by including the

cost of isomorphic mapping. In the Koyama scheme-I, the cost of isomorphic mapping requires seven modular multiplications and three modular inverses. Where as our proposed scheme require one modular multiplication and two modular inverses to perform isomorphic mapping. As result the decryption speed becomes somewhat faster than that of the Koyama scheme if we consider the cost of isomorphism. When we compare encryption speed of our scheme-1 with the scheme-1 given by Koyama [16] then as it is $(5+d)/2$ times slower than the RSA scheme, where d is the ratio of the computation amount of division to that of multiplication, we conclude that our scheme-1 is faster than the Koyama scheme-I.

4.1.3. *Comparison between the schemes I, II and III.* We first compare the scheme-I with the scheme-II. It can be seen from the above paras that the decryption speed of both the schemes I and II is same. Next, if we consider the encryption process without isomorphic mapping, then although, proposed scheme-I requires $4.5log\ e$ multiplication *modulo* n on average as computational time but it is significantly less in proposed scheme-II i.e.$1.5log\ e$ multiplication *modulo* n on average. Next, the block size of the plaintext in both the schemes proposed by us is 2 times than the RSA scheme. To encrypt $2 - log\ n$ bit message using standard RSA scheme required $3log\ e$ multiplication *modulo* n on average. Thus scheme-I is 1.5 times slower than the RSA scheme but the scheme-II is 2 times faster then the RSA scheme. Additionally, in the proposed scheme-1, the size of ciphertext is 3tuples whereas in the proposed scheme-II it is 2tuples. So, the block size of ciphertext of scheme-I is 1.5 times larger than the scheme-II. This means that proposed scheme-I requires additional space, which can help to check ciphertext against accidental corruption.

In scheme-III proposed by us the triples like $(r^e, f(r), r^2)$ can be computed well in advanced, so the encryption process required only two multiplication and one inversion *modulo* n. Due to the observation made by Kouchi et al [17]small encryption exponent can be used in the scheme -III. Hence, encryption process of scheme-III is faster than the scheme-I and scheme-II.

Our proposed scheme-III is an analogue of Kouchi et al [17]scheme over Pell equation. To decrypt $2-log\ n$ bit message using Kouchi et al scheme, it requires around $3log\ d+14$ multiplication *modulo* n on average. Whereas in our proposed scheme-III to decrypt, $2log\ n$ bit message required $1.5log\ d+28$ modulo multiplication on average. Therefore, we conclude that the proposed scheme is somewhat faster than the scheme proposed by Kouchi et al [17] for a k bit long message if $\lceil k/log\ n \rceil$ is even. If the sender sends hash value of (r, m) i.e $H(r, m)$ using the hash function H, then receiver can verify the originality of the message obtained. Thus the scheme-III can be made secure against adaptive chosen message attack by using a one-way hash function H.

To encrypt any plaintext in the scheme-I, one has to compute the equation (6), which is to be done in polynomial time. Since, the values of $a_{e,i}$ and

$b_{e,i}$ do not depend upon the plaintext , therefore it could be computed well in advance. Such precomputation increases the efficiency of the encryption process. In the RSA type cryptosystem based on elliptic curve such as KMOV [14], Demytko [8] and Koyama [16] scheme, the addition operation is computationally more expansive in comparison to our proposed schemes. With this point of view, we can say that the encryption process is more efficient than the KMOV, Demytko and Koyama scheme respectively.

4.2. **Security Analysis.**

4.2.1. *Security under ciphertext attacks.* Under the ciphertext attack, we claim that our proposed schemes are as secure as the RSA scheme.

Theorem 6. *Breaking each one of proposed schemes is computationally equivalent to breaking the RSA scheme under ciphertext attack.*

Proof: Let (C_x, C_y, a) be the ciphertext of our proposed scheme. Assume that there exist algorithm A which can output the solution (M_x, M_y) given the input (C_x, C_y, a) . Now given he ciphertext C in the RSA scheme, one can computes the corresponding plaintext M by using algorithm A as follows.

Firstly, let us randomly select a pair (C_x, C_y) in C_n. Then computes $a = \frac{C_x - C}{C_y}$. Now according to the assumption of algorithm A, the solution pair (M_x, M_y) will be output. Then the original message $M \equiv (M_x - aM_y)(mod\ n)$ is discovered. Similarly it can be easily shown that the ciphertext attack in the RSA scheme is polynomial time seduceable to our proposed shceme. This complete the proof.

So our proposed scheme is as secure as RSA scheme under the cuphertext attack.

Remark. Above theorem proves security of scheme-I and scheme-II for chosen ciphertext attack for the passive adversary. It is not a proof against active attack "adaptive chosen ciphertext attack". The scheme-III is semantically secure and can be made secure against adaptive chosen ciphertext attack by using one-way hash function. So the scheme-III is secure against adaptive chosen ciphertext attack using he observation made by Kouchi et al [17].

4.2.2. *Security in the broadcast application.* In the broadcast application, as we know that the standard RSA scheme is not secure if encryption key e is small. Let (n_i, e) be the public key for the receiver R_i $(1 \leq i \leq k)$. The common plaintext m is encrypted as $c_i \equiv m^e mod\ n_i$ $(1 \leq i \leq k)$ for k receivers . If , $k \geq e$, then the system of congruences $c_i \equiv m^e mod\ n_i$ $(1 \leq i \leq e)$ can be transformed into the equation $c = m^e$, where c is the combined ciphertext from c_i via Chinese Remainder Theorem. Hence, the plaintext m can be computed as $m \equiv c^{\frac{1}{e}}$ over the real field, even if, the known

terms like $userID$ are included in the plaintext such that $m_i \equiv \alpha_i m + \beta_i$, where α_i and β_i are publicly known. For obtaining m, Hasted has shown that similar attacks are successful by solving a set of k congrunces of polynomials $\sum_{j=1}^{u} t_{i,j} m^j \equiv 0 \mod n_i$ [10] . The inequality condition for a successful attack is given by :

$$\prod_{i=1}^{k} n_i > N^{\frac{u(u+1)}{2}} (k+u+1)^{\frac{k+u+1}{2}} 2^{\frac{(k+u+1)^2}{2}} (u+1)^{u+1} \tag{8}$$

where$N = min(n_i)$.

Now we evaluate the security of our proposed cryptosystem in broadcast application, in which plaintext is purely common or linearly related. For this purpose, there is a recursive formula for computing x_i such that $(x_i, y_i) = i \otimes (x_1, y_1)$ over C where $(x_1, y_1) \in C$ is the initial point :

$$x_{i+1} = x_1 x_i + (x_1^2 - 1)(x_i^2 - 1)^{\frac{1}{2}}, \qquad x_{2i} = 2x_i^2 - 1 \tag{9}$$

Using (9) ciphertext C_x can be expressed as $C_x = 2^{e-1} M_x^e + f_e(x)$ where $f_e(x)$ is a polynomial with degree $e-1$. Thus the system of congruences in M_x with degree e can be obtained as $2^{e-1} M_x^e + f_e(x) - C_x \equiv 0 \mod n_i$. Hence, we have shown that the schemes have the same security as the RSA scheme when linearly related plaintexts are encrypted in broadcast applications.

Next, we show that our schemes are more secured than RSA scheme when purely common plaintext is encrypted in the broadcast application. If we use the RSA scheme with purely common plaintext in broadcast application than the set of congruence generates simple monomial M^e. As consequence, by using Chinese reminder theorem attack is possible in the scheme if the number of receiver $k \geq e$. But in our scheme if the purely common plaintext is encrypted in broadcast application, than Chinese reminder theorem cannot be used for attack. For the reason, the set of congruence are polynomial in M_x in degree e, which is not a simple monomial M^e. Using appropriate choice of β_i [17] one can prevent from Coppersmith attack [5] also. Consequently the Hasted attack [10] is possible here but for the greater value of k. Thus the proposed schemes are more secure than the RSA scheme when purely common plaintexts are encrypted in broadcast applications.

In order to prevent from Hasted attack to the proposed scheme, it is suggested to always keep the number of receivers less than 7 when $e = 3$, less than 16 when $e = 5$, and less than 282 when $e = 19$. Because, the inequality (8) given by Hasted does not hold for said three values of e and k. However, such attack is not possible, what so ever number of receivers we keep when $e \geq 21$. These conditions are true for the RSA scheme only when linearly related plaintexts are encrypted in the broadcast application. Next, due to the observation made by Kouchi et al [17]the scheme-III is secure against low exponent attack [5, 10] for the appropriate choice of parameter l ($l > 114$ for $e = 3$ and $l > 21$ for $e = 7$) for a 1024-bits RSA modulus n. To prevent from other low exponent attack with known related message [3], one recommend to chose $l = 160$ for a 1024-bits RSA modulus n.

Finally, we discuss security of our proposed scheme against the known plaintext attack. Assume that the attacker knows one of the plaintext pair m_x, m_y and the corresponding ciphertext (c_x, c_y, a). To get another part of the plaintext he(she) has to solve the quadratic equation $m_y(m_x + a) \equiv \frac{(m_x m_y + (m_x m_y)^{-}1)}{2} mod\ n$ i.e. $m_x^2 m_y^2 + 2am_x m_y^2 - 1 \equiv 0\ mod\ n$ for m_x or m_y, which seems as hard as factoring. So, the proposed scheme is secure against partially known plaintext attack.

References

[1] Bleichenbacher D., On the security of KMOV public key cryptosystem. LNCS Crypto'97v.1294, 235-348(1997).

[2] Chen C.Y., Chang C.C. Yang W.P. Fast RSA type cryptosystem based on Pell equation. Proceeding of International Conf. On Cryptology and Information Security Taiwan, Dec.1-5, 1996.

[3] Coppersmith D., M. Franklin, J. Patarin and M Reiter., Low exponent RSA with related messages. Eurocrypt'96 LNCS 1070, pp 1-9, Springer Verlag (1996).

[4] Catalano D., R. Gennaro, N. Howgraw-Crahan and P. Nguyen,Paillier's cryptosystem revisited. ACM Conference on Computer and Communication Security (2001).

[5] Coppersmith D. , Finding a small root of a bivariate integer equation; factoring with high bits known. Advances in Cryptology-Eurocrypt'96, LNCS vol.1070, Springer-Verlag, 1996, pp.178-189.

[6] O'Connor, J.J and Robertson,E. F. ,February 2002.Pell's Equations.[Online], Available: http/www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html.

[7] Chiou, C.W. and Yang T.C., Iterative modular multiplication algorithm without magnitude comparison. Electronic Letters, v.130, no. 24, 1994 pp.2017-1018.

[8] Demytko N., A new elliptic curve based analogue to RSA. LNCS EUROCRYPT'93, 40-49(1993).

[9] Diffie W.and Hellmann Martin, New direction in cryptography.IEEE Transaction on Information Theory, v.22, 1976, 644-654.

[10] Hasted J., On the using RSA with low exponent in a public key network. LNCS Crytpo'85, V.218 pp. 403-408(1985).

[11] Kaliski Jr.B.S., The Montgomery inverse and its applications. IEEE Transaction on Computers, vo.8, Aug.1995 pp.1064-1065.

[12] Koyama K., H. Kawakado A new RSA type scheme based on singular cubic curve $(y - ax)(y - bx) = x^3 mod\ N$ IEICE Trans. Fund E79-A, pp49-539(1996).

[13] Kuwadado H, Koyama K., Y.Tsuraoka, A new RSA type scheme based on singular cubic curve $y^2 = x^3 + bx^2 mod\ N$, IEICE Trans.Fund E78-A, 27-33(1995).

[14] Koyama K., U.Maurer, T. Okamoto, S.A.Vanstone, New public key schemes based on elliptic curves over the rung Zn, Crypto'91 252-266 (1991).
[15] Koblitz Neal, Elliptic curve cryptosystem, Math.Comput.48.203-209 (1985).
[16] Koyama Kenji, Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 mod\ N$, Eurocrypt'95 329-339 (1995).
[17] Kouichi S. and Tsuyoshi Takagi. New semantically secure public key cryptosystems from RSA-Primitive. LNCS PKC'02 Vol.2274,pp.1-16 (2002).
[18] Lenstra H.W Jr. Solving the Pell equation. Notice of AMS v.49 no.2 186-192 (2002).
[19] Lenstra H.W.Jr. Factoring integers with elliptic curve. Annals of Mathematics 126,pp 649-673(1987).
[20] Menezes A., Elliptic curve pubic key cryptosystem . Kluwer Acad. Pub. 1993.
[21] Miller V., Uses of elliptic curve in cryptography, LNCS CRYPTO'85pp 417-426(1985).
[22] Marc Gysin, Jennifer Sebery, How to use Pell's equation in cryptography.Preprint.
[23] O'Connor, J.J and Robertson,E. F. ,February 2002. Pell's Equations.[Online], Available: http/www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html.
[24] Sahadeo Padhye, Partial known plaintext attack on Koyama scheme. Information Processing Letters, 96/3 pp.96-100(2005).
[25] David Pointcheval, New public key cryptosystem based on the dependent-RSA problem. Eurocrypt'99 LNCS Springer-Verlag , vol.1592, pp.239-254, (1999).
[26] Rivest R.L. , Shamir A. and Adllemann L., A method for obtaining digital signature and public key cryptosystems. Comm. Of the ACM 21 , 2 pp. 120-126 (1978).
[27] Simmons G.J, editor .Contemporary Cryptology-The Science of Information Integrity. IEEE Press, 1992
[28] Well A., Number theory, an approach through history. Birkhausiur Boston 1984. Demytko N., A new elliptic curve based analogue to RSA. LNCS EUROCRYPT'93,40-49(1993).