Pell's RSA key generation and its security analysis

Chandra segar T
Research Scholar,
School of Information Technology and Engineering
VIT University,
Vellore, India.
chandrasegar.t@vit.ac.in

Vijayaragavan R
Associate Professor,
School of Advanced Sciences,
VIT University,
Vellore, India.
rvijayaraagavan@vit.ac.in

***Abstract*—In this paper, a new variant of RSA has been proposed whose key generation method is distinct with the standard RSA. Generally the RSA family of variants can be applied at the secured channel to enhance its data trust level on various applications such as E-commerce, Internet applications, etc., The boundary level of the private key has been recommended here, to raise over these variant to stay away from the possibility of getting the Small 'd' value either by continuous fraction method of Wiener's attack, or by Coppersmith's lattice based method of Boneh & Durfee attack, or by retrieving the Euler's totient function value by Fermat factorization method. This paper discusses the proposal of Pell's RSA key generation and its security analyses over the standard RSA, N Prime RSA, Dual RSA. Finally the application of Pell's RSA, Blind signatures, are proposed.**

Keywords-component; Cryptography, Cryptanalysis, Public Key Cryptosystem, RSA, Wiener's Attack, Pollard & Rho factorization, Extended Euclids algorithm, mutiplicative inverse.

I. INTRODUCTION

One of the well known Public Key Cryptosystem (PKC) is RSA which was emerged to this universe around 36 years back. This common RSA believed to be one of the most secured cryptosystem which is ultimately stand on the complicatedness of making decision over the known e^{th} root onto the product of two or more prime value 'n'. PKC works on the principle of two distinguishable keys such as public and private keys. Here the encryptor knows only the public key and decryptor knows both of the keys. So the initiator/decryptor shares only the public key with encryptor and hence keeps the private key secret. Common RSA has three main sub components such as key generation, encryption and decryption. In key generation process, the revival of private key exponent might be based on the Euclid's or Extended Euclid's algorithm. Among these two, Extended Euclid's Algorithm is the efficient one whereas the normal Euclid's computational process is typically dependent on the input size of modulus of 'n' and the positive real integer value of 'e'. Before this, the public key exponent 'e' is based on the Euler's totient function $\Phi(n)$, such that by checking the strategy gcd(e, $\Phi(n)$)==1 through the assist of Euclid's algorithm. Once we have these two prime factors and public exponent we can easily determine the private key. But the tough job of this approach is to find these prime factors. It requires a significant amount of computation to get these prime factors. This factoring approach is great deal of research. We need an efficient approach rather than this factoring approach to determine the private key to avoid this significant amount of computation.

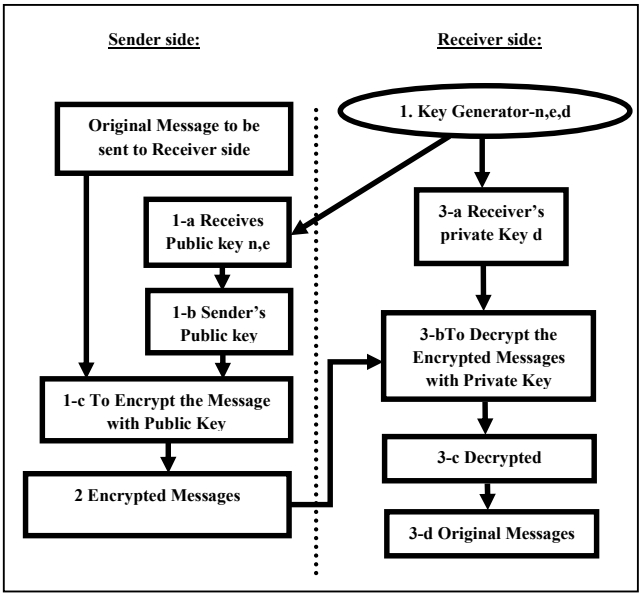

Figure 1. Architecture of Public Key Cryptosystem.

We are going to present an idea to determine private key without using this factoring approach. Our approach is efficient than the already existed approaches and requires less amount of computation. It works more efficiently when the public key is small, since most of public key encryption uses small public key in order to improve the efficiency of encryption. Moreover, the decryption process takes the advantage of Chinese Remainder Theorem (CRT).

II. RELATED WORKS

In this section, the variants of RSA cryptosystem were going to be reviewed as it is. In this paper, the discussion is based on only with the essential breeds of RSA such as standard RSA, N prime RSA, Dual RSA, and its factorization attack through Rho and pollard method. In section IV, the proposed Pell's RSA and its factorization attack are discussed.

Elaine L. Render August et.al [1] RSA Cryptosystem play an important role in credit card payment application, email application and remote login for network application by allowing security and authentication. Without using RSA cryptosystem, the progress of internet is not possible because the main goal of user is security. There are many attacks which are carried out and determined to understand the effectiveness of the system. Before 15 years, Michael Wiener described the continued fraction attack which is very useful for the accomplishment of an error.

Vibhor Mehrotra & Prakash Singh Rana et.al [2] This paper represents a new algorithm program which accesses the RSA scheme. The main of suggested this algorithm is to find the private key of RSA scheme and factoring the modules which are based on public RSA scheme. This algorithm plays an important role in reducing running time and provides more effectiveness in comparison of that algorithms which are already subsist.

B R Ambedkar & S S Bedi et.al [3] Due to generating a pair of keys such as public and private in transmitting node, the safety of RSA algorithm ids depends on the positive integer only. To find the factorization of positive integer N is very complicated. In this paper, to find the factor of positive integer N, a new factorization method is planned. The planned work targets on factorization of trivial and non-trivial integer numbers only. To explain factorization process of RSA module N, some steps are needed. The most important point to representing this paper is that this is based on Pollard rho factorization.

B R Ambedkar, Ashwani Gupta, Pratiksha Gautam& SS Bedi,et.al [4] In this paper, the main aim is to increase the speed of factorization in compare to traditional trial division method. To find the aim a new algorithm named ad trivial division algorithm is used which help in finding all trivial and non trivial values of N. The current work targets on factorization of all trivial and non trivial integer numbers need of steps for factorization of RSA modules N.

Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek, et.al [5] This paper shows a new alternative of RSA algorithm. By using alternative we find the same public and private key supporters. The group of this alternative of RSA algorithm is known as Dual RSA. Dual RSA can be used for scenarios which have two aspects from RSA with decreasing the needs of the storage for keys. Dual RSA having two applications, first one is known as Blind signature and other is known as authentication/security.

Satyendra Nath Mandal & Kumarjit Banerjee, Biswajit Maiti and J. Palchaudhury et.al [6] To provide the security and privacy to digital data, a most important schema RSA cryptosystem is used. RSA algorithm is based on two large prime numbers. Due to based on two large prime number it has problem to handling number because to handle large prime number is a very time taken process. This paper, a new technology named as "modify trial division technique" is used to implement RSA algorithm for large number due solve the problem of range of compiler.

A. Standard RSA

Nowadays, the standard RSA support at the most of 2048 binary bits of values.

1. *Choose any two distinct prime numbers p and q. The integer's p and q values would be chosen at random.*
2. *Compute n=p*q; 'n' act as the modulus value of both public and private key.*
3. *Compute Euler's Totient Function, $\Phi(n) = (p - 1)*(q - 1)$*
4. *Choose an integer **'e'** such that $1<e<\phi(n)$ and GCD (e, $\phi(n)$) =1, i.e., e and $\Phi(n)$ are relatively prime. Hence 'e', is released as public key exponent.*
5. *Determine $d = e^{-1} \pmod{\Phi(n)}$, which implies $(d * e) = 1 \pmod{\Phi(n)}$ here d lies in $(0 \le d \le n)$*
6. *Encryption:*
   Obtain the Cipher Text from message, $C_e(M) = M^e \bmod n$
7. *Decryption:*
   Obtain the message from Encrypted Text, $M_d(C_e) = C^d \bmod n$

B. N prime RSA

Here the size of 'n' is generally dependent on number of primes chosen and on its value.

1. *Choose two or more distinct prime numbers p, q, r and so on values would be chosen at random.*
2. *Compute n=p*q*r; 'n' act as the modulus value of both public and private key.*
3. *Compute Euler's Totient Function, $\Phi(n) = (p - 1)*(q - 1) * (r - 1)$ and so on.*
4. *From Step 4 to Step 7 is similar to Standard RSA.*

Here, the exponentiation time of encryption will be based on the number of primes selection and the plain text value. Through the repeated squaring method, the exponential value over the bound of modulus n can be solved wisely.

C. Dual RSA

There exists two positive integer k_1 and k_2 such that
$ed = 1 + k_1 \phi(N_1)$ *and* $ed = 1 + k_2 \phi(N_2)$

1. *Choose any four distinct prime numbers $(p_1,q_1)$and (p_2,q_2)*
2. *Compute $N_1=p_1q_1$ and $N_2=p_2q_2$*
3. *Now compute the $\phi(N_1)=(p_1 - 1)*(q_1 - 1)$ & $\phi(N_2)=(p_2 - 1)*(q_2 - 1)$*
4. *Choose an integer 'e' such that $\phi(N_1) <e<\phi(N_2)$ & GCD (e, $\phi(N_1)$, $\phi(N_2)$) =1 are relatively prime. Hence "e, N_1, N_2", are released as public key exponent.*
5. *Now determine 'd_1 and d_2' where, $ed_1 \equiv 1 \pmod{\Phi(N_1)}$ & also $ed_2 \equiv 1 \pmod{\Phi(N_2)}$, here d_1 lies in $(0 \le d_1 \le N_1$ & $0 \le d_2 \le N_2)$ Here the private key exponents are $(d_1, d_2, p_1, q_1, p_2, q_2)$*

For Instance: If $p_1=5$; $q_1=11$; $p_2=7$; $q_2=19$
Then $\phi(N_1)=40$ $\phi(N_2)=108$ and so $40 <73<108$
Hence the public key exponents are (73, 55, 133) and the private key exponents are (17, 37, 5, 11, 7, 19)

III. PROPOSED PELL'S RSA KEY GENERATION

Pell's takes the Diophantine equation form,

$$Y^2 - dX^2 = 1$$

1. *Select a secret prime integer "R".*
2. *Generate the pair of initial positive integers X_0 , Y_0 which satisfies the Diophantine equation as* $Y^2 - RX^2 = 1$ *(1)*
3. *Select two large positive odd primes p,q*
4. *Then compute N:=(p*q)*
5. *Compute $\Phi(n) = (p - 1) * (q - 1)$*
6. *Select 'e' in $(1<e<\phi(n))$ & holds GCD $(e, \phi(n)) = 1$*
7. *Compute* α*:* $= [Y_0 + \phi(n)]^2 - R[X_0 + e]^2$

   $\alpha: = [Y_0^2 + \phi(n)^2 + 2Y_0\phi(n)] - R[X_0^2 + e^2 + 2X_0e]$

   $= Y_0^2 - RX_0^2 + \phi(n)^2 + 2Y_0\phi(n) - Re^2 - 2RX_0e$

   $\equiv 1 - Re^2 - 2RX_0e$ *(2)*

   Finally, $\alpha + Re^2 + 2RX_0e \equiv 1 \bmod \phi(n)$ *(3)*
8. *Determine* $d \equiv e^{-1} \pmod{\Phi(n)}$ *lies in* $(0 \le d \le n)$
9. *Compute public key S, such that multiply with* d^3 *on both sides of Eq. (3) we obtain,*

   $S = \alpha d^3 + Rd + 2RX_0d^2 \equiv d^3 \bmod \phi(n)$ *(4)*
10. *Choose the plain text 'M' in the interval (0 to N-1)*
11. *Encrypt: Cipher Text,* $C_s(M) = M^S \bmod n$ *(5)*
12. *Decrypt: Plain Text,* $M_e(C_s) = C^{e^3} \bmod n$ *(6)*

Here the public key exponents are (α, d, R, X_0, n) and private key exponents are (e^3, n)

For Instance Pell's RSA

1. *Let the secret prime integer R=7.*
2. *We get $X_0 = 3$, $Y_0 = 8$, which satisfies the Eq. (1)*
3. *Let primes p =11 and q=13*
4. *N:=(p*q)=143*
5. *$\Phi(n) = (p - 1) * (q - 1) = 120$*
6. *Let e =17, which satisfies GCD (e, 120) =1*
7. *Compute α:=$[Y_0 + \phi(n)]^2 - R[X_0 + e]^2$*

   α:=$[8+120]^2 - 7[3+17]^2 = 13584$

   By putting in Eq. (3) we get

   $[13584 + 2023 + 714] \bmod 120 \equiv 1$

   $16321 \bmod 120 \equiv 1$
8. *Determine $d \equiv 17^{-1} \pmod{120}$ we get d=113*
9. *Compute $S \equiv d^3 \bmod \phi(n) \equiv 113^3 \bmod 120 = 17$*
10. *Let M=19 in (0 to 142)*
11. *Encryption: $C_s(M) = M^S \bmod n = 19^{17} \bmod 143 = 2$*
12. *Decryption: $M_e(C_s) = C^{e^3} \bmod n = 2^{4913} \bmod 143 = 19$*

Here the public key {S, N} is tightly depend on α, d, R, X_0 variables for to compute $(\alpha d^3 + Rd + 2RX_0d^2)$ which is rigorously equivalent to $d^3 \bmod n$.

TABLE I. CYPTOGRAPHY OF STANDARD RSA AND PELL'S RSA.

Text	*ASCII*	***Encryption & Decryption* p=11, q=13, e=17, d=113**	
		Encryption of Std. RSA e=17	***Decryption of Pell's RSA α=13584, R=7, X_0=3***
s	19	2	19
e	5	135	5
c	3	9	3
r	18	83	18
e	5	135	5
t	20	37	20

Initially, the text message "secret" has been converted with its equivalent ASCII integer representation for to apply the encryption and decryption process. Table II. clearly shows that the Pell's Cryptography works well for the input message "secret".

IV. ATTACKS

A. Fermat's Factorization Method

1. *Choose the input value 'n' from the public key exponent (n, e) [i.e., $n = p*q = ((p+q)/2)^2 - (p-q)/2)^2$]*
2. *Compute an positive integer 'k' which is the square root of 'n' and check if $k^2 > n$ else k++*
3. *Now generate the 'h' value until it satisfies $k^2 - n = h^2$*

   i.e., If(h==square)

   Goto Step 4

   Else k++ and Goto Step 3
4. *Now reveal 'n' factor p=(k+h) and q=(k-h)*

For Instance: If n= 21, then $\sqrt{21}$ =4.58 and the ceil value is 4=k. Now checking, is $4^2 > 21$, the constraint is false. Hence k++, again checking $5^2 > 21$, the constraint is true. Now checking for the square value 'h': $5^2 - 21$=Square, the constraint is true and so h=2. Finally, revealing p=(5+2)=7 and q=(5-2)=3

B. Weiner's Continuous Fraction Method

The Wiener's attack, named after cryptologist Michael J. Wiener, is a type of cryptographic attack, which uses the continued fraction method to exploit a mistake made in the use of RSA. This error could be exploited when users are doing transactions using credit card or mobile devices such as phones.

Wiener's Theorem

Let n=p*q with $q<p<2q$ and $d<(N^{0.25})/3)$ with (n,e) with $ed \equiv 1 \bmod(\Phi(N))$, then the attacker can efficiently recover 'd'.

1. *Take the public key exponent (n, e) where 'e' should be lesser than 'n'.*
2. *Determine all the continued fractions of constant* $d_1 + d_2 + d_3 + ... + d_n$ *on (n, e).*

$$\frac{e}{n} = \frac{1}{d_1 + \frac{1}{d_2 + \frac{1}{d_3 + \frac{1}{d_4 + ... \frac{1}{d_n}}}}} = [d_1 + d_2 + d_3 + ... + d_n]$$

3. *Now determine all the convergent of k for each d.*

$$\frac{k}{d} = 0 + \frac{k_1}{d_1} + \frac{k_2}{d_2} + \frac{k_3}{d_3} + ... + \frac{e}{n}$$

4. *Find the Euler totient function* $\phi(n)$*, by matching the convergent to following equation,*

$ed \ -1/k = \phi(n)$

5. *Now, to solve the following equation,*

$x^2 - ((N - \phi(n) + 1)x + N = 0$

Now, $(N - \phi(n)) = p + q$

6. *Now find the roots of x, we get p & q wisely.*

After the step 4 itself we have got the $\phi(n)$ *in hand, and then we can find multiplicative inverse of e to determine d where,* $d \equiv e^{-1} (1 \bmod \phi(n))$ *Use Extended Euclid's Algorithm.*

For Instance: Let (n, e) = (90581, 17993) respectively.
The continuous fractional division of e/n is given by, $[0, 5, 29, 4, 1, 3, 2, 4, 3]$ *and its corresponding convergents are* $[0,\ 1/5,\ 29/146,\ 117/589,\ 146/735,\ 555/2794,\ 1256/6323,\ 5579/28086,\ 17993/90581]$
$\phi(n)$ *= ((17993*5)-1)/1= 89964 then compute N-* $\phi(n)$ *= 90581-89964=618=379*239=p*q (using roots)*
To find, $d \equiv e^{-1} (1 \bmod n) \equiv 17993^{-1} (1 \bmod 90581)$

TABLE II. FINDIND 'D' THROUGH EXTENDED EUCLID'S ALGORITHM

q	r1= $\phi(n)$	r2=e	r	t1	t2	t=t1-qt2
4	89964	17993	17992	0	1	-4
1	17993	17992	1	1	-4	5
17992	17992	1	0	-4	5	-89964
0	1	0	-	5	-89964	**5**

Finally, the private key exponent d =5.

V. CRYPTANALYSIS OF PELL'S RSA WITH STANDARD RSA

TABLE III. CRYPTANALYSIS OF STANDARD RSA WITH PELL'S

$\|X_2\|$	*Public Key*		*Cryptanalyze of Std. & Pell's RSA*		
	'n'	*'e'*	*Fermat's Factorization*		
			p	*q*	$\phi(n)$
5	21	5	3	7	12
6	55	7	5	11	40
7	91	11	7	13	72
8	253	13	11	23	220
9	481	17	13	37	432
10	1003	19	17	59	928

$|X_2|$ is the binary length; 'n' maximum product value over $|X_2|$.

VI. CONCLUSION

In this Pell's RSA, an efficient public key cryptosystem has been implemented based on Pell's equation which is shown by using different key parameters. From the security analysis, the evaluation of proposed RSA is measured with standard RSA. Through these outcomes, it has been noticed that there is tremendous variations on Pell's key generation with normal RSA which prevents the attack against Wiener's Theorem. Using this Pell's RSA, the security strength gets increased that is taking the private key 'd' above the Wiener's possible range. In this context Pell's RSA and its competence RSA have their own limitations. The values of operands are to be taken in such a way that the overhead is kept at minimum.

REFERENCES

[1] Elaine L. Render August, "Wiener's Attack on Short Secret Exponents", Reference Site -IEEE, Proceedings of August 15, 2007.

[2] Vibhor Mehrotra, "An effective Method for Attack RSA Strategy" Int. J. Advanced Networking and Applications 1363 Volume: 03, Issue: 05, Pages: 1362-1366 (2012)

[3] B R Ambedkar & S S Bedi, "A New Factorization Method to Factorize RSA Public Key Encryption", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011 ,ISSN (Online): 1694-0814

[4] B R Ambedkar, Ashwani Gupta, Pratiksha Gautam, "An Efficient Method to Factorize the RSA Public Key Encryption", International Conference on Communication Systems and Network Technologies, 2011.

[5] Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek,"Dual RSA and Its Security Analysis" Reference Site -IEEE Transactions On Information Theory Vol.53,No.8,Augest 2007

[6] Satyendra Nath Mandal & Kumarjit Banerjee, Biswajit Maiti and J. Palchaudhury. "Modified Trail division for Implementation of RSA Algorithm with Large Integers" Int. J. Advanced Networking and Applications Volume: 01, Issue: 04, Pages: 210-216 (2009)

[7] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma" Modified RSA Encryption Algorithm (MREA)" pgno: 426-429 advance Advanced Computing & Communication Technologies (ACCT), 2012, ISBN: 978-1-4673-0471-9

[8] Sonal Sharma, Prashant Sharma, Ravi Shankar Dhakar," RSA Algorithm Using Modified Subset Sum Cryptosystem" Pgno: 457-461, Computer and Communication Technology (ICCCT), 2011, ISBN: 978-1-4577-1385-9

[9] H. C. WILLIAMS," A Modification of the RSA Public-Key Encryption Procedure" pgno: 726-729, IEEE transaction on Information Theory.

[10] Suli Wang, Ganlai Liu," File encryption and decryption system based on RSA algorithm" pgno: 797-800, Computational and Information Sciences (ICCIS), 2011 , ISBN: 978-1-4577-1540-2.

[11] Ying-yu Cao, Chong Fu," An Efficient Implementation of RSA Digital Signature Algorithm", pgno: 100-103, Intelligent Computation Technology and Automation (ICICTA), 2008, ISBN:978-0-7695-3357-5

[12] Mircea Frunza', Luminita Scripcariu' "Improved RSA Encryption Algorithm, For Increased Security of Wireless Networks", pgno: 1-4, Signals, Circuits and Systems, 2007. ISSCS 2007, ISBN: 1-4244-0969-1

[13] Jen-Shiun Chiang; Jian-Kao Chen, "An Efficient VLSI Architecture for RSA Public key Cryptosystem", pgno: 496-499 vol 1, Circuits and Systems, 1999, ISCAS '99, ISBN: 0-7803-5471-0.

[14] Duoli Zhang; Minglun Gao; Li Li; Zuoren Cheng; Xiaolei Wang," An Implementation method of a RSA Crypto Processor Based on modified Montgomery algorithm.",pgno:1332-1336 vol.2, ASIC, 2003. Proceedings, ISBN: 0-7803-7889-X

[15] Ching-Chao Yang; Chein-Wei Jen; Tian-Sheuan Chang," Ic design of high speed RSA processor",pgno: 33-36, Circuits and Systems, 1996, ISBN: 0-7803-3702-6

[16] Sarma, K.V.S.S.R.; Kumar, G.S.K.; Avadhani, P.S., "Threshold cryptosystem using Pell's equation",pgno: 413-416, Information Technology: New Generations (ITNG), 2011, ISBN: 978-1-61284-427-5

[17] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," IEEE Trans. Inf. Theory, vol. 36, no. 3, pp. 553–559, May 1990.

Chandra Segar.T currently pursuing Ph.D at VIT University, Vellore Campus, Vellore, India. His area of specialization includes Linear Cryptanalysis, Public Key Cryptosystems, Fuzzy Systems, Automata and Networking. About his publication, currently holds three International journals and one International conference.

Prof. Vijayaragavan, Ph.D is currently working for VIT University, Vellore, India as Associate Professor in the School of Advanced Sciences.