Cryptanalysis of Multi Prime RSA with Secret Key Greater than Public Key

Navaneet Ojha and Sahadeo Padhye

(Corresponding author: Sahadeo Padhye)

Department of Mathematics, Motilal Nehru National Institute Of Technology
Allahabad (U.P.), India.
(Email : sahadeomathrsu@gmail.com)

(Received Apr. 15, 2012; revised and accepted July 24, 2012)

Abstract

The efficiency of decryption process of Multi prime RSA, in which the modulus contains more than two primes, can be speeded up using Chinese remainder theorem (CRT). On the other hand, to achieve the same level of security in terms integer factorization problem the length of RSA modulus must be larger than the traditional RSA case. In [9], authors studied the RSA public key cryptosystem in a special case with the secret exponent d larger than the public exponent e. In this paper, we show that how such attack is performed in the multi-prime RSA case.

Keywords: Coppersmith technique, cryptanalysis, lattice basis reduction, RSA

1 Introduction

The RSA cryptosystem [10] invented by Rivest, Shamir and Adleman in 1978 is one of the most popular and practical public key cryptosystem in the history of cryptology. In the RSA cryptosystem, let $N = pq$ be an RSA modulus, where p and q are primes of equal bit size. Let e be the public exponent and d be the secret exponent satisfying $ed \equiv 1\ mod\ (\phi(N))$, where $\phi(N)$, the Euler totient function. Multi-prime RSA [5] is a generalization of the standard RSA cryptosystem in which the modulus contains more than two primes. In the traditional RSA decryption using Chinese remainder theorem requires two full exponentiations modulo $\frac{n}{2}$- bit numbers, whereas, in the Multi prime RSA (where modulus is product of r primes) the decryption with Chinese remainder theorem requires r full exponentiations modulo $\frac{n}{r}$- bit numbers. Thus the theoretical speed up of Multi prime RSA decryption is $\frac{r^2}{4}$ $(= \frac{2(\frac{n}{2})^3}{r.(\frac{n}{r})^3})$ times than the traditional RSA decryption. Hence, the Multi-prime RSA might be a practical alternative to improve the efficiency of decryption process (for a fixed RSA modulus size). As a consequence, the choice of RSA parameters to achieve a certain level of security is based on the estimated current and future performance of integer factorization algorithms. In another words, numerous attacks have been developed that are not related to the "integer factorization problem (IFP)" and show vulnerabilities of specific instances of the RSA cryptosystem. Boneh [2] gave an excellent survey on this matter.

In [5, 6], a little work has been reported on how such attacks apply to multi-prime RSA. Most practical interest are the cases of 3- and 4-prime RSA. Commercial implementations of 3-prime RSA is given in [4]. In 2008, Luo et al. [9] have shown that the RSA public key cryptosystem with private exponent d larger than the public exponent e may be insecure in some special cases. They have shown that if $N^{.25} \leq e \leq N^{.915}$, $d > e$, the cryptanalytic attacks based on "Lenstra- Lenstra- Lov'asz (LLL)" [8] lattice based reduction algorithm can be performed in RSA cryptosystem under some assumption.

In this article, we discuss how the attack on RSA, given in [9], can be extended to the multi prime RSA case, and how they perform in the new setting. We see that RSA is insecure if $N^{.25} \leq e \leq N^{.915}$ for RSA 2-prime, if $N^{.4} \leq e \leq N^{.7}$ for RSA 3-prime, if $N^{.5} \leq e \leq N^{.6}$ for RSA 4-prime. Thus the range of encryption key e decreases if number of factors in the RSA modulus increases. Thus the multi prime RSA is less vulnerable to current attack on RSA.

Rest of the Section is as follows. Section 2 gives preliminaries about Multi prime RSA, and the Lattices. In Section 3, we give an out look of small inverse problem. Section 4 gives our main result. Finally we conclude our result in Section 5.

2 Preliminaries

We introduce some notations and state some known facts about Multi prime RSA and Lattices.

Multi prime RSA [5]. This RSA variant is based on modifying the structure of the RSA modulus. For any integer $r \geq 2$, r-prime RSA consists of the following three algorithms.

Key Generation. Let N be the product of r randomly chosen distinct primes $p_1....p_r$. Compute Euler's Totient function of N: $\phi(N) = \prod_{i=1}^{r}(p_i - 1)$. Choose an integer e, $1 < e < \phi(N)$, such that $gcd(e, \phi(N)) = 1$. The pair (N, e) is the public key. Compute the integer $d \in Z_N^*$ such that $ed \equiv 1 \; mod \; \phi(N)$, here d is the private key.

Encryption. For any message $M \in Z_N$, the ciphertext is computed as $C \equiv m^e \; mod \; N$.

Decryption. Decryption is done using the Chinese remainder theorem. Let $d_i \equiv d \; mod \; (p_i - 1)$. To decrypt the ciphertext C, one first computes $M_i \equiv C^{d_i} \; mod \; p_i$ for each i, $1 \leq i \leq r$. One then combines the M_i's using the CRT to obtain $M \equiv C^d \; mod \; N$.

We call N the Multi-prime RSA modulus, the RSA modulus (when $r = 2$), or simply the modulus. The integer e is called the public (or encrypting) exponent and d is called the private (or decrypting) exponent. When $r = 2$ we have the original RSA encryption scheme. Superficially, the only difference between RSA and Multi-prime RSA with $r > 2$ is the number of primes in the modulus. We now give some notations and assumptions about Multi prime RSA.

For Multi-prime RSA with r- primes, the modulus, $N = \prod_{i=1}^{r} p_i$, is simply the product of r distinct primes. As with RSA, we only consider Multi prime RSA with balanced primes. That is, if we label the primes so that $p_i < p_{i+1}$, for $i = 1, ...r - 1$, we assume that

$$4 < \frac{1}{2}N^{1/r} < p_1 < N^{1/r} < p_r < 2N^{1/r}. \qquad (1)$$

The key generation algorithm for Multi-prime RSA is essentially the same as for RSA, except that the modulus requires r-random distinct balanced primes instead of two. We will assume that the public and private exponents are defined modulo $\phi(N) = \prod_{i=1}^{r}(p_{i-1})$. Thus e and d must satisfy

$$ed \equiv 1 \; mod \; \phi(N),$$

which we call the key relation. From this equivalence, we have the key equation

$$ed = 1 + k \; \phi(N),$$

where k is some positive integer. As with RSA, we use $\wedge$ to denote the difference between the modulus N and Euler's Totient function $\phi(N)$. That is, $N = \phi(N) - \wedge$.

Expanding $\phi(N)$ and defining the set $S_r = 1, ..., r$, we can write $\wedge$ as

$$\wedge = N - \phi(N) = \sum_{i \in S} \frac{N}{p_i} - \sum_{\substack{i,j \in S_r \\ i \neq j}} \frac{N}{p_i p_j} + ... + (-1)^r.$$

As is shown in [5], a simple computation using the expression for $\wedge$ and Equation (1) (condition for balanced primes) shows that $\wedge$ satisfies

$$| \wedge | < (2r - 1)N^{1-1/r}.$$

Thus, $\phi(N)$ and N have roughly an $(r - 1)/r$ fraction of their most significant bits in common. The encryption algorithm for Multi-prime RSA is identical to that of RSA. The public (encrypting) exponent will usually be denoted by $e = N^\alpha$.

Lattices [3]: Let $u_1, ..., u_w$ be linear independent vectors in R^n. We define by

$$L(u_1, ..., u_w) = \{\sum_{i=1}^{w} z_i \; u_i | z_i \in Z\},$$

the set of all linear integer combinations of the u_i's. This set is called the lattice and $u_1, ..., u_w$ a basis of that lattice. Let $u_1^\star, ..., u_w^\star$ be the results of Gram-Schmidt orthogonolization on $u_1, ..., u_w$, then the determinant of the lattice is defined by

$$det(L) = \prod_{i=1}^{w} ||u_i^\star||,$$

where $||.||$ denotes Euclidean norm of the vectors. We have the following lemma about the lattice basis reduction algorithm (L^3).

Lemma 1. Let L be a lattice spanned by $u_1, ..., u_w$, then the L^3 algorithm produces a new basis $b_1, ..., b_w$ of L satisfying

$$\begin{array}{ll} (i) & ||b_j||^2 \leq 2^{(i-1)}||b_i^\star||^2, 1 \leq j \leq i \leq w \\ (ii) & ||b_1|| \leq 2^{(w-1)/4}det(L)^{1/w}. \end{array}$$

We can find the bound on the norms of the other vectors in the L^3- reduced basis except b_1, due to Jutla's contribution. For a basis $u_1, ..., u_w$ of lattice L, define

$$u_{min}^\star := min_i||u_i^\star||,$$

then we have the following lemma:

Lemma 2. Let L be a lattice spanned by $u_1, ..., u_w$, and let $b_1, ..., b_w$ be the L^3- reduced basis of L. Suppose $u_{min}^\star \geq 1$, then

$$\begin{array}{ll} (i) & ||b_2|| \leq 2^{w/4}det(L)^{1/(w-1)} \\ (ii) & ||b_3|| \leq 2^{w+1/4}det(L)^{w-2}. \end{array}$$

3 Solving The Small Inverse Problem

Let $e = N^\alpha$ and $d = N^\delta$, where $\alpha, \delta \in R^+$. Now following the work given by Luo et al. [9], with slight modifications, we begin with the public-private key equation

$ed - k\phi(N) = 1$. Letting $s = \phi(N) - N$ and $A = N$, we have the following relation

$$ed - k(A + s) = 1.$$

To improve the boundary of Boneh and Durfee [3], Luo et al. assumed the condition that $d > e$. Letting $d \equiv d' \ mod \ e$ and $d' \approx e^{\gamma}$, we have the following result

$$ed' - k(A + s) \equiv \ 1 \ mod \ e^2.$$

Thus the problem is to find d', s and $-k$ such that,$|d'| < e^{\gamma}$, $|s| < e^{1/2\alpha}$ & $|k| = \frac{ed-1}{\phi(N)} < \frac{ed}{\phi(N)} < \frac{2ed}{N} = 2e^{1+\frac{\delta-1}{\alpha}}$, where $\phi(N) > \frac{N}{2}$.

In this section we solve the small inverse problem $ed' - k(A+s) \equiv \ 1 \ mod \ e^2$ stated as follows: given a polynomial $f(x, y, z) = ex + y(A + z) - 1$, find (x_0, y_0, z_0) such that

$$f(x_0, y_0, z_0)) \equiv \ 0 \ mod \ e^2, |x_0| < X, |y_0| < Y, |z_0| < Z, \qquad (2)$$

$X = e^{\gamma}, Y = e^{1+\frac{\delta-1}{\alpha}+\epsilon_2}, Z = e^{\frac{a_r}{\alpha}+\epsilon_r}$. Here $\epsilon_2 = \ln 2$ and $\epsilon_r = \ln(2r - 1)$, where $a_r = 1 - \frac{1}{r}$. Notice that $(d', -k, s)$ is a root of $f(x, y, z)$ mod e^2. Now, a result of Howgrave-Graham [7] allows us to transform the modular equation in Equation (2) into an integer equation. Here we define the norm of a polynomial $h(x, y, z) = \sum_{i,j,k} a_{i,j,k} x^i y^j z^k$ by

$$(||h(x, y, z)||)^2 = \sum_{i,j,k} |a^2_{i,j,k}|.$$

Lemma 3 [7]. Let $h(x, y, z) \in Z[x, y, z]$ be a polynomial which is the sum of w monomials. Suppose that

$$(a) \qquad h((x_0, y_0, z_0)) \equiv 0 \ mod \ e^m,$$

for positive integer m, where $|x_0| < X, |y_0| < Y$ and $|z_0| < Z$, and

$$(b) \qquad ||h(xX, yY, zZ)|| < \frac{e^m}{\sqrt{w}},$$

then $h(x_0, y_0, z_0) = 0$ holds over the integers.

This lemma shows that if a polynomial has a small norm then all small roots of the polynomial modulo a large modulus are also roots of the polynomial over the integers. The goal is then to construct such a polynomial that has (x_0, y_0, z_0) as a root modulo e^{2m}, for some m. To this end, given a positive integer m and t, define the polynomials

$$g_{i,j,k}(x, y, z) = x^i y^j z^k e^{2(m-k)}, \qquad (3)$$

where $k = 0, ..., m$, and $i + j = 0$, where $r = 0, ..., m - k$, and

$$h_{i,j,k}(x, y, z) = x^i z^j f^k e^{2(m-k)}, \qquad (4)$$

where $k = 0, ..., m$, $i = 0, ..., m - k$ and $j = 1, ...t$. Notice that (x_0, y_0, z_0) is a root of all these polynomials modulo e^{2m}. We would like to find a low norm integer linear combination of the polynomials $g_{i,j,k}(xX, yY, zZ)$ and $h_{i,j,k}(xX, yY, zZ)$. To do this, we construct a lattice that is spanned by the coefficient vectors of the polynomials $g_{i,j,k}$ and $h_{i,j,k}$ for some parameters (i, j, k), that contains some small vectors in it. By a small vector, we mean that the norm of the polynomial corresponding to the vector is small enough to apply Lemma-3. The LLL lattice reduction algorithm can be used to find these small vectors. Following the idea discussed in Luo et al. [9] for given integers m and t, the dimension of the full rank lattice is

$$w = \frac{(m + 1)(m + 2)(m + 3)}{6} + \frac{t(m + 1)(m + 2)}{2}.$$

Suppose that the first three vectors of the LLL- reduced basis satisfy

$$|b_i| < \frac{e^{2m}}{\sqrt{w}},$$

where $i = 1, 2, 3$. Then we can find the corresponding polynomials $g_1, g_2, g_3 \in Z(x, y, z)$, such that

$$g_i(x_0, y_0, z_0) = 0,$$

where $i = 1, 2, 3$ hold over the integers, by Lemma 3. Now computing the resultants

$$\begin{aligned} h_1(y, z) &= Res(g_1, g_2), \\ h_2(y, z) &= Res(g_1, g_3), \\ h'(z) &= Res(h_1, h_2). \end{aligned}$$

Then by solving $h'(z) = 0$, we can get one root such that $z_0 = \frac{p+q}{2}$, which helps the factorization of $N = pq$. The polynomials g_1, g_2, g_3 are linearly independent, but they may not be algebraically independent. In this case the resultants $h_1(y, z)$ and or $h_2(y, z)$ are identically zero and finding z_0 becomes difficult.

4 Main Result

In the paper [3], Boneh and Durfee gave a low private exponent attack on RSA using lattice reduction techniques. This attack renders 2-prime RSA insecure when the private exponent is less than N^{δ}, where, in the most efficient variant of the attack, $\delta = 0.292$ as $N \to \infty$. Hinek [5] showed that how the Boneh-Durfee attack and a modified approach due to Blomer and May [1] can be generalized to r-prime RSA, and obtain corresponding asymptotic upper bounds on the private exponent. In this paper, we discuss the attack given by Luo et al. [9] for the r- prime RSA case.

Given integer $m \geq 1$ and $t \geq 0$, we construct the lattice as follows. For $k = 0, ..., m$, use $g_{i,j,k}(x, y, z)$, for $i + j = 0$, where $r = 0, ..., m - k$ and $h_{i,j,k}(x, y, z)$, for $i = 0, ..., m - k$ and $j = 1, ...t$ as the basis vectors, with $g_{i,j,k}$ and $h_{i,j,k}$ as in Equations (3) and (4). Now we calculate $det(L)$ of the lattice constructed. Since L is spanned by a lower triangular matrix, its determinant only depends on the entries on the diagonal. Following [9], for the given parameters m and t, we count the numbers of X, Y, Z and e elements in these entries, and obtain

$$\begin{aligned} X_{m,t} &= \frac{(m+1)(m+2)(m+3)}{24} + \\ &\quad \frac{tm(m+1)(m+2)}{6}, \qquad (5) \\ Y_{m,t} &= \frac{m(m+1)(m+2)(m+3)}{12} + \\ &\quad \frac{tm(m+1)(m+2)}{6}, \qquad (6) \\ Z_{m,t} &= \frac{m(m+1)(m+2)(m+3)}{24} + \\ &\quad \frac{t(m+1)(m+2)(3t+2m+3)}{12}, \qquad (7) \end{aligned}$$

and

$$E_{m,t} = \frac{m(m+1)(m+2)(m+3)}{4} + \frac{2tm(m+1)(m+2)}{3}. \qquad (8)$$

Hence, we have

$$det(L) = e^{E_{m,t}} X^{X_{m,t}} Y^{Y_{m,t}} Z^{Z_{m,t}}. \qquad (9)$$

Now we required to satisfy the following inequalities

$$|b_i| < \frac{e^{2m}}{\sqrt{w}}, \qquad (10)$$

where $i = 1, 2, 3$. Now from Lemma 1 and Lemma 2, the following inequalities holds

$$det(L) < e^{2m(w-2)}/\eta, \qquad (11)$$

where $\eta = 2^{(w+1)(w-2)/4} w^{(w-2)/2}$. Since it is negligible compared to $e^{2m(w-2)}$ when w is small. Substituting $X = e^{\gamma}, Y = e^{1+\frac{\delta-1}{\alpha}+\epsilon_2}$ and $Z = e^{\frac{a_r}{\alpha}+\epsilon_r}$ in to Equations (5), (6), (7), (8), (9) and (11). We have the following,

$$\begin{aligned} E_{m,t} + \gamma X_{m,t} + (1 + \frac{\delta-1}{\alpha} + \epsilon_2) Y_{m,t} + \\ (\frac{a_r}{\alpha} + \epsilon_r) Z_{m,t} \leq \ 2m(w-2). \qquad (12) \end{aligned}$$

Now simplifying Equation (12), we have the following result:

$$\begin{aligned} &\frac{6a_r}{\alpha} t^2 + (\frac{6a_r}{\alpha} + 4m\gamma + \frac{4m\delta}{\alpha} - 4m - \frac{4m}{\alpha} + \frac{4a_r m}{\alpha}) t \\ &\quad + \{m(m+3)\gamma + 2m(m+3)\frac{\delta}{\alpha} + \frac{96m}{(m+1)(m+2)} \\ &\quad + \frac{a_r - 2}{\alpha} m(m+3)\} \leq 0. \qquad (13) \end{aligned}$$

For optimizing t, we have the following relation

$$\begin{aligned} t &= t_{opt} \\ &= -\frac{\alpha}{12a_r}(\frac{6a_r}{\alpha} + 4m\gamma + \frac{4m\delta}{\alpha} - 4m - \frac{4m}{\alpha} + \frac{4a_r m}{\alpha}). \end{aligned}$$

Table 1: Boundaries for α, γ and δ with $m \to \infty$, ignoring η

α	γ	2-Prime		3-Prime		4-Prime	
		δ_{min}	δ_{max}	δ_{min}	δ_{max}	δ_{min}	δ_{max}
.25	0	.75	.75	.75	.67	.75	.63
.3	0	.7	.752	.7	.667	.7	.628
.4	0	.6	.763	.6	.66	.6	.62
.4	.3	.6	.695	.6	.606	.6	.566
.5	0	.5	.705	.5	.68	.5	.63
.5	.3	.5	.692	.5	.59	.5	.552
.5	.4	.5	.662	.5	.56	.5	.525
.5	.5	.5	.634	.5	.543	.5	.5
.6	0	.6	.802	.6	.69	.6	.64
.6	.2	.6	.732	.6	.62	.6	.576
.7	0	.7	.838	.7	.71	.7	.662
.75	0	.75	.854	.75	.73	.75	.63
.75	.2	.75	.755	.75	.64	.75	.58
.915	0	.915	.916	.92	.78	.92	.72

Putting this value in Equation (13), and by taking $m \to \infty$, we have

$$\delta \leq \frac{a_r}{2} + 1 + \alpha - \alpha\gamma - \frac{\sqrt{3}}{2} a_r \sqrt{1 - \frac{2}{a_r}(\alpha\gamma - 2\alpha)}.$$

Letting $r = 2$, we recover the bound

$$\delta \leq (\alpha + \frac{5}{4} - \alpha\gamma) - \frac{\sqrt{3}}{4}\sqrt{1 - 4\alpha\gamma + 8\alpha},$$

originally obtained in Luo et al. [9].

Also since $d > e$, we have $\delta \geq max(\alpha, 1 - \alpha)$. We can compare the range of weak keys for RSA r-prime ($r = 2, 3, 4$) in the Table 1 given below.

From the above table we see that RSA becomes insecure if $N^{.25} \leq e \leq N^{.915}$ for RSA 2-prime, if $N^{.4} \leq e \leq N^{.7}$ for RSA 3-prime, if $N^{.5} \leq e \leq N^{.6}$ for RSA 4-prime, as the relation $\delta > \alpha$ is satisfying in the above region. Thus the range of encryption key e decreases if number of factors in the RSA modulus increases. Thus the Multi prime RSA is less vulnerable to current attack on RSA.

Remark: Note that the above table is calculated by taking $m \to \infty$ and neglecting the value of η. As per the relation between w, m and η, if m is large then η can not be neglected. For the moderate values of m and t and considering η, the table given by Luo et al. [9], can also be compared for the Multi-prime RSA and we expect that the range of the encryption key may be decrease for Multi-prime RSA case.

5 Conclusion

We have shown that how the attack given by Luo et al. on RSA can be extended to the Multi prime RSA case, and how they perform in the new setting. If the number of prime factors in the modulus increases, the attack becomes more complex or totally ineffective. So, we can say that the Multi prime RSA is less vulnerable to current attacks on RSA.

References

[1] J. Blomer, A. May, "Low Secret Exponent RSA Revisited," *Cryptography and Lattices CaLC* 2001, LNCS 2146. Springer-Verlag Berlin Heidelberg, 4- 19, 2001.

[2] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *Notices of the American Mathematical Society*, 46(2):203213, 1999.

[3] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," *IEEE Transactions on Information Theory*, vol. 46, nNo. 4, pp. 1339-1349, 2000.

[4] T. Collins, D. Hopkins, S. Langford, and M. Sabin, "Public Key Cryptography Apparatus and Method," US Patent ♯ 5,848,159, Jan. 1997.

[5] M. J. Hinek, "On the security of multi-prime RSA," *CACR Technical Report* CACR 200616, Centre for Applied Cryptographic Research, University of Waterloo, 2006. [http://www.cacr.math.uwaterloo.ca/].

[6] M. J. Hinek, M. K. Low, and E. Teske, "On some attacks on multi-prime RSA," *Selected Areas in Cryptography* SAC 2002, volume 2595 of Lecture Notes in Computer Science, pages 385404. Springer-Verlag, 2003.

[7] N.Howgrave, "Finding small roots of univariate modular equations revis- ited" *Cryptography and Coding* 1997. LNCS, vol. 1355, pp. 131142. Springer, Heidelberg (1997)

[8] A. K. Lenstra, H. W. Lenstra Jr. and L. Lovasz, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515-534, 1982.

[9] P. Luo, H. Zhou, D. S. Wang, and Y. Q. Dai, "Cryptanalysis of RSA for a special case with $d > e$," *Sci China Ser F-Inf Sci*, vol. 52, no. 4, pp. 609-616, Apr. 2009.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptsystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-128, 1978.

Navaneet Ojha received his B.Sc. and M.Sc. degree from Purvanchal University, Jaunpur, Utter Pradesh, India in the year 2001 and 2004 respectively. He is a life member of Cryptology Research Society of India (CRSI). His area of interest is Public Key Cryptosystem based on Factoring Problem. Presently he is pursuing his Ph.D. degree in Motilal Nehru National Institute of Technology, Allahabad, India.

Sahadeo Padhye received his B.Sc.and M.Sc. degree in Mathematics form Pt. Ravishankar Shukla University, Raipur. Chhattisgarh, India in 1999 and 2001. Council of Scientific and Industrial Research (CSIR), India has granted him Junior Research Fellowship (2002-2004). He did his Ph.D. form Pt. Ravishankar Shukla University, Raipur, India. He is a life member of Cryptology Research Society of India (CRSI). His area of interest is Public Key Cryptography based on elliptic curve and ID-Based digital signature. Presently he is working as Assistant Professor in the Department of Mathematics, Motilal Nehru National Institute of Technology, Allahabad, India.