Cryptanalysis of Multi-Prime RSA with Small Prime Difference

Hatem M. Bahig, Ashraf Bhery, and Dieaa I. Nassr

Computer Science Division, Department of Mathematics,
Faculty of Science, Ain Shams University,
Cairo 11566, Egypt

Abstract. We show that the attack of de Weger on RSA using continued fractions extends to Multi-Prime RSA. Let (n, e) be a Multi-Prime RSA public-key with private key d, where $n = p_1 p_2 \cdots p_r$ is a product of r distinct balanced (roughly of the same bit size) primes, and $p_1 < p_2 < \ldots < p_r$. We show that if $p_r - p_1 = n^\alpha, 0 < \alpha \leq 1/r, r \geq 3$ and $2d^2 + 1 < \frac{n^{2/r-\alpha}}{6r}$, then Multi-Prime RSA is insecure.

Keywords: continued fractions, RSA, Multi-Prime RSA, Wiener's attack, de Weger's attack.

1 Introduction

The RSA cryptosystem, invented by Rivest, Shamir and Adleman [18] in 1977, is one of the most important public key cryptosystems. For example, it is used by Web servers and browsers to secure Web traffic. In RSA, an integer $n = pq$ (the RSA modulus) is a product of two large distinct primes of the same bit size. The public exponent $e < \phi(n)$ and the private exponent $d < \phi(n)$ satisfy the equation $ed \equiv 1 \bmod \phi(n)$, where $\phi(n) = (p-1)(q-1)$ is Euler's totient function. The public key is the pair (n, e) and the private key is d.

Multi-prime RSA (MPRSA) is a simple extension of RSA in which the modulus has three or more distinct primes. It was patented by Compaq in 1997 [7,1]. In MPRSA with r primes, the modulus is $n = p_1 \cdots p_r$, where $p_1 < p_2 < \ldots < p_r$. As with RSA, we only consider $\frac{1}{2}n^{1/r} < p_i < 2n^{1/r}$ for $1 \leq i \leq r$. In this case n is said to be a product of distinct r-balanced primes. Clearly, we have

$$\frac{1}{2}n^{1/r} < p_1 < n^{1/r} < p_r < 2n^{1/r}.$$

The key generation of MPRSA is similar to RSA. It is as follows.

- Let n be the product of r randomly chosen distinct balanced primes $p_1, \ldots, p_r$, where $p_1 < p_2 < \ldots < p_r$.
- 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 $\gcd(e, \Phi(n)) = 1$.
- Compute the multiplicative inverse $d = e^{-1} \ mod \ \Phi(n)$.

T.W. Chim and T.H. Yuen (Eds.): ICICS 2012, LNCS 7618, pp. 33–44, 2012.

n is called the MPRSA modulus. The public-key is (n, e) and the private key is d.

In general, the running time of generating (n/r)-bits primes for MPRSA will decrease with increasing number of primes [11].

The encryption of MPRSA is identical to that of RSA. For any message $m \in Z_n$, the ciphertext is

$$c = m^e \ mod \ n.$$

The standard decryption of MPRSA is the same as standard decryption of RSA. For any ciphertext $c \in Z_n$, the plaintext is

$$m = c^d \ mod \ n.$$

When Chinese Remainder Theorem (CRT) is used in decryption, the MPRSA takes time less than in RSA. A speed-up of a factor at least $r/2$ (and at most $r^2/4$) is estimated [11]. A speed-up of 1.73 has been achieved in practice for 3-prime RSA compared to RSA using CRT with a 1024-bit modulus [5,11].

In other words, there are two practical reasons to use more than two primes.

1. The primes are smaller and key generation takes less time despite there being more of them.
2. Decryption takes less time if one uses CRT.

Many attacks on RSA are extended to MPRSA. For examples, small private exponent attacks on RSA by Wiener [24] (when the private key $d < n^{1/4}$) is extended to MPRSA by Ciet *et al.* [6] and Hinek *et al.* [12]. Boneh and Durfee attack [4] on RSA using lattice reduction technique [13] and Coppersmiths method [8] for $d < n^{0.292}$ is also extended to MPRSA by Hinek *et al.* [12]. The generalization of Blömer and May's lattice based attack for arbitrary public exponents RSA [2,16] is extended to MPRSA by Ciet *et al.* [6]. Some of the partial key exposure attacks on RSA are extended to MPRSA, see [11, Ch.9] for some details.

De Weger [23] showed that if $n = pq$ has a small difference between its prime factors $p - q = n^\beta, \frac{1}{4} \leq \beta \leq \frac{1}{2}$, then the private key $d = n^\delta$ of RSA can be recovered when $\delta < \frac{3}{4} - \beta$. In this paper,we show a similar result on MPRSA. Using Wiener's interval proposed by [17], we show that d can be recovered when $2d^2 + 1 < \frac{n^{2/r-\alpha}}{6r} < \phi(n)$, for $r \geq 3$; and when $2d^2 + 1 < 2n^{3/2-2\alpha} + 1$, for $r = 2$ and $\phi(n) > \frac{3}{4}n$.

The paper is organized as follows. In section 2, we review some basic facts about continued fractions, and Wiener's interval. In Section 3, we cryptanalysis MPRSA with small prime difference. In Section 4, we compare between our attacks and other small private exponent attacks. An example of the cryptanalysis is given in Section 5. Finally, Section 6 includes the conclusion.

2 Preliminaries

In this section, we briefly recall some basic definitions and facts that will be used in the paper.

A (*finite*) continued fraction expansion (**CF**) [19] is an m-tuple of integers

$$[q_1, q_2, ..., q_m]$$

with $q_2, ..., q_m > 0$, which is an abbreviation of the following rational number:

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... + \cfrac{1}{q_m}}}.$$

Let a, b be two positive integers satisfying $\gcd(a, b) = 1$ and $a < b$. The rational number $c = \frac{a}{b}$ has a unique **CF** $[q_1, q_2, ..., q_m]$ with $q_m > 1$, which can be computed in time $O(log^2 b)$ using the following algorithm [21]:

- $c_0 = c$.
- compute $c_i = \frac{1}{c_{i-1} - \lfloor c_{i-1} \rfloor}$ for $i = 1, \cdots, m$, where $m \leq 2 \log b$ is the smallest value of i such that $\lfloor c_i \rfloor = c_i$.
- return $[q_1, q_2, \ldots, q_m]$, where $q_i = \lfloor c_i \rfloor$ for $i = 1, \cdots, m$.

If c is an irrational number, then the computation can be continued for $m \to \infty$. In this case, we have *infinite* **CF** :

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... + \cfrac{1}{\cdots}}}.$$

It will be shortened to $[q_1, q_2, \ldots]$.

Theorem 1. (Legendre) [19] *Let α be a real number. If c and d are positive integers such that* $\gcd(c, d) = 1$ *and*

$$\left| \alpha - \frac{c}{d} \right| < \frac{1}{2d^2},$$

then $\frac{c}{d}$ is a convergent of the **CF** *expansion of α.*

Definition 1. *[17] Let m be a real number and (n, e) be an RSA public key with private key d, where $ed - 1 = t\phi(n)$. We define a Wiener's attack on (n, e, m), denoted by* $\mathbf{WA}(n, e, m)$*, as follows:*

$$\mathbf{WA}(n, e, m) = \begin{cases} \frac{t}{d}, & \text{if } \frac{t}{d} \text{ is one of the convergents of the } \mathbf{CF} \text{ expansion of } \frac{e}{m}; \\ \text{failure, otherwise.} \end{cases}$$

$\mathbf{WA}(n, e, m)$ *is said to be succeeds if it returns t/d.*

Definition 2. *[17] Let (n, e) be an RSA public key. An interval $I \subset \Re$ (set of real numbers) is said to be a Wiener's interval for (n, e) if for every $m \in I$,* $\mathbf{WA}(n, e, m)$ *succeeds.*

The following theorem determines a Wiener's interval for an RSA public-key (n, e).

Theorem 2. *[17] Let (n, e) be an RSA public key with private exponent d. Then $I =]\phi(n) - \frac{\phi(n)}{cd^2+1}, \phi(n) + \frac{\phi(n)}{2d^2-1}[$ is a Wiener's interval for (n, e), where*

$$c = \begin{cases} 2, & \text{if } d < \sqrt{\frac{\phi(n)-1}{2}}; \\ \\ 4, & \text{if } \sqrt{\frac{\phi(n)-1}{2}} \leq d < \frac{\phi(n)-1}{4}. \end{cases}$$

Theorem 2 is also true for MPRSA [17].

3 The Attack

In this section, we show that the result of de Weger [23] on RSA can be extended to MPRSA using Wiener's interval . By choosing $m = n - \Gamma$, where

$$\Gamma = \sum_{i}^{r} \frac{n}{n^{1/r}} - \sum_{\substack{i,j \\ i<j}}^{r} \frac{n}{n^{2/r}} + \sum_{\substack{i,j,k=1 \\ i<j<k}}^{r} \frac{n}{n^{3/r}} + ... - (-1)^r,$$

we show that m lies in Wiener's interval (Theorem 2).

Now, let

$$\Lambda = n - \phi(n) = \sum_{i}^{r} \frac{n}{p_i} - \sum_{\substack{i,j=1 \\ i<j}}^{r} \frac{n}{p_i p_j} + \sum_{\substack{i,j,k=1 \\ i<j<k}}^{r} \frac{n}{p_i p_j p_k} + ... - (-1)^r;$$

Then we can rewrite Λ and Γ as follows.

$$\Lambda = \Lambda_1 - \Lambda_2 + ... - (-1)^r \Lambda_r,$$

where

$$\Lambda_k = \sum_{\substack{i_1,..,i_k \\ i_1<..<i_k}}^{r} \frac{n}{p_{i_1} p_{i_2} ... p_{i_k}},\ 1 \leq k \leq r.$$

And

$$\Gamma = \Gamma_1 - \Gamma_2 + ... - (-1)^r \Gamma_r,$$

where

$$\Gamma_k = \sum_{\substack{i_1,\ldots,i_k \\ i_1<..<i_k}}^{r} \frac{n}{n^{k/r}} = C_k^r n^{1-k/r},\ 1 \le k \le r$$

and

$$C_k^r = \frac{r!}{k!(r-k)!}(k \le r).$$

Lemma 1. *Let $n = p_1 p_2 ... p_r$ be a product of distinct r-balanced primes and $p_r - p_1 = n^\alpha, 0 < \alpha \le 1/r$. Then*

$$|\Lambda_k - \Gamma_k| < 2^k(2^k-1)C_k^r n^{1+\alpha-\frac{k+1}{r}},$$

where k is a positive integer such that $k \le r$.

Proof

$$\begin{aligned}
|\Lambda_k - \Gamma_k| &\le \sum_{\substack{i_1,\ldots,i_k \\ i_1<..<i_k}}^{r} \left| \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}} - \frac{n}{n^{k/r}} \right| \\
&= \sum_{\substack{i_1,\ldots,i_k \\ i_1<..<i_k}}^{r} \frac{n\left|n^{k/r} - p_{i_1} p_{i_2} \cdots p_{i_k}\right|}{n^{k/r} p_{i_1} p_{i_2} \cdots p_{i_k}} \\
&\le \sum_{\substack{i_1,\ldots,i_k \\ i_1<\ldots<i_k}}^{r} \frac{n\left|p_r^k - p_1^k\right|}{\frac{1}{2^k} n^{2k/r}} \\
&= \sum_{\substack{i_1,\ldots,i_k \\ i_1<\ldots<i_k}}^{r} \frac{2^k n(p_r - p_1)(p_r^{k-1} + p_r^{k-2} p_1 + \ldots + p_1^{k-1})}{n^{2k/r}} \\
&< \sum_{\substack{i_1,\ldots,i_k \\ i_1<\ldots<i_k}}^{r} \frac{2^k n^{1+\alpha}(2^{k-1} n^{\frac{k-1}{r}} + 2^{k-2} n^{\frac{k-1}{r}} + \ldots + 2^0 n^{\frac{k-1}{r}})}{n^{2k/r}} \\
&= \sum_{\substack{i_1,\ldots,i_k \\ i_1<\ldots<i_k}}^{r} \frac{2^k n^{1+\alpha} n^{\frac{k-1}{r}} (2^{k-1} + 2^{k-2} + \cdots + 1)}{n^{2k/r}} \\
&= 2^k(2^k-1)C_k^r n^{1+\alpha-\frac{k+1}{r}}.
\end{aligned}$$

♢

Proposition 1. *Let $n = p_1 p_2 \cdots p_r$ be a product of distinct r-balanced primes and $p_r - p_1 = n^\alpha, 0 < \alpha \le 1/r$. Then*

$$|\Lambda - \Gamma| < \begin{cases} \frac{1}{4} n^{2\alpha - 1/2}, & \text{if } r = 2; \\ 3r n^{1+\alpha-2/r}, & \text{if } r \ge 3, \text{ and } 2^k(2^k-1)C_k^r \le \frac{n^{1/r}}{r-1}\ (2 \le k \le r). \end{cases}$$

Proof

If $r = 2$, then

$$|\Lambda - \Gamma| = |p_1 + p_2 - 1 - (2\sqrt{n} - 1)| = p_1 + p_2 - 2\sqrt{n} = \frac{(p_1-p_2)^2}{p_1+p_2+2\sqrt{n}} < \frac{(p_1-p_2)^2}{4\sqrt{n}} = \frac{1}{4}n^{2\alpha-1/2}.$$

If $r \geq 3$ and $2^k(2^k-1)C_k^r \leq \frac{n^{1/r}}{r-1}$,

$$|\Lambda - \Gamma| < |\Lambda_1 - \Gamma_1| + \sum_{k=2}^{r} |\Lambda_k - \Gamma_k|.$$

Using Lemma 1, for every $2 \leq k \leq r$, we have

$$|\Lambda_k - \Gamma_k| < 2^k(2^k-1)C_k^r n^{1+\alpha-(k+1)/r}$$

$$\leq \frac{n^{1/r}}{r-1} n^{1+\alpha-(k+1)/r}$$

$$= \frac{n^{1+\alpha-k/r}}{r-1} \leq \frac{n^{1+\alpha-2/r}}{r-1}.$$

It follows that

$$|\Lambda - \Gamma| < 2rn^{1+\alpha-2/r} + \textstyle\sum_{k=2}^{r} \frac{n^{1+\alpha-2/r}}{r-1}$$

$$= 2rn^{1+\alpha-2/r} + (r-1)\frac{n^{1+\alpha-2/r}}{r-1}$$

$$< 3rn^{1+\alpha-2/r}.$$ ♢

Theorem 3. *Let $n = p_1p_2\cdots p_r$ be MPRSA modulus, where $p_1, p_2, \cdots, p_r$ are distinct r-balanced primes. If $p_r - p_1 = n^\alpha, 0 < \alpha \leq 1/r$ and*

$$2d^2 + 1 < \begin{cases} 2n^{3/2-2\alpha} + 1, & \text{if } r = 2 \text{ and } \phi(n) > \frac{3}{4}n; \\ \frac{n^{2/r-\alpha}}{6r}, & \text{if } r \geq 3, \text{ and } 2^k(2^k-1)C_k^r \leq \frac{n^{1/r}}{r-1},\ 2 \leq k \leq r \end{cases}$$

then the system is insecure.

Proof: Using Theorem 2, we need only to show that

$$|m - \phi(n)| < \frac{\phi(n)}{2d^2+1},$$

where $m = n - \Gamma$. We have

$$|m - \phi(n)| = |\Lambda - \Gamma|.$$

Thus, by Proposition 1, we have

$$|m-\phi(n)| < \begin{cases} \frac{1}{4}n^{2\alpha-1/2}, & \text{if } r=2; \\ 3rn^{1+\alpha-2/r}, & \text{if } r \geq 3, 2^k(2^k-1)C_k^r \leq \frac{n^{1/r}}{r-1},\ 2 \leq k \leq r. \end{cases}$$

We have two cases.

Case 1: $r = 2$. If $\phi(n) > \frac{3}{4}n$, then

$$\begin{aligned} |m-\phi(n)| &< \tfrac{1}{4}n^{2\alpha-1/2} = \tfrac{1}{4}n^{2\alpha-3/2+1} = \tfrac{1}{4}\tfrac{n}{n^{3/2-2\alpha}} \\ &< \tfrac{1}{4}\tfrac{n}{d^2} < \tfrac{\frac{4}{3}\phi(n)}{4d^2} < \tfrac{\phi(n)}{3d^2} < \tfrac{\phi(n)}{2d^2+1}. \end{aligned}$$

Case 2: $r \geq 3$ and $2^k(2^k-1)C_k^r \leq \frac{n^{1/r}}{r-1}$. We have

$$\begin{aligned} |m-\phi(n)| &< 3rn^{1+\alpha-2/r} = 3r\tfrac{n}{n^{2/r-\alpha}} < 3r\tfrac{2\phi(n)}{n^{2/r-\alpha}} \\ &= \tfrac{\phi(n)}{\frac{n^{2/r-\alpha}}{6r}} < \tfrac{\phi(n)}{2d^2+1}. \end{aligned}$$

♢

Remark 1. 1. if $\alpha = \frac{1}{r}$, then the upper bound of d is $\sqrt{\frac{n^{1/r}-6r}{12r}}$ which is similar to the upper bound $\sqrt{\frac{n^{1/r}}{2(2r^2-1)}}$ in [12].

2. Since the maximum numbers of *safe* primes for MPRSA are 3, 3, 4, and 5 for 1024, 4038, 4096, and 8192 bits respectivelly [11], the condition $2^k(2^k-1)C_k^r \leq \frac{n^{1/r}}{r-1}$ in Theorem 3 is always satisfied.

4 Comparison

In this section, we compare between our attack and the previous attacks.

1. For $r = 2$, and $0 < \alpha \leq \frac{1}{2}$, we have two cases:
   (a) If $0 < \alpha < \frac{1}{4}$, then Fermat's method [23] factorizes $n = p_1p_2$ in polynomial time if $p_2 - p_1 = n^\alpha$.
   (b) If $\frac{1}{4} \leq \alpha \leq \frac{1}{2}$, then de Weger's attack [23] finds $d = n^\delta$ when $p_2 - p_1 = n^\alpha$, where $\delta < \frac{3}{4} - \alpha$.
2. To the best of our knowledge, for $r \geq 3$, there is no generalization of Fermat's method for MPRSA. Our attack (Theorem 3) can be considered as an extensions of de Weger's attack since $\alpha \geq 0$ and for $r = 2$, de Weger's attack is a special case of Theorem 3.
   It is important to point that all known small private exponent attacks on MPRSA become less effective when increasing the number of primes in the modulus [11, Section 9.3].
3. When the public exponent e is full sized, our attack is superior than other small private exponent attacks on MPRSA. Figure 1 shows a comparison

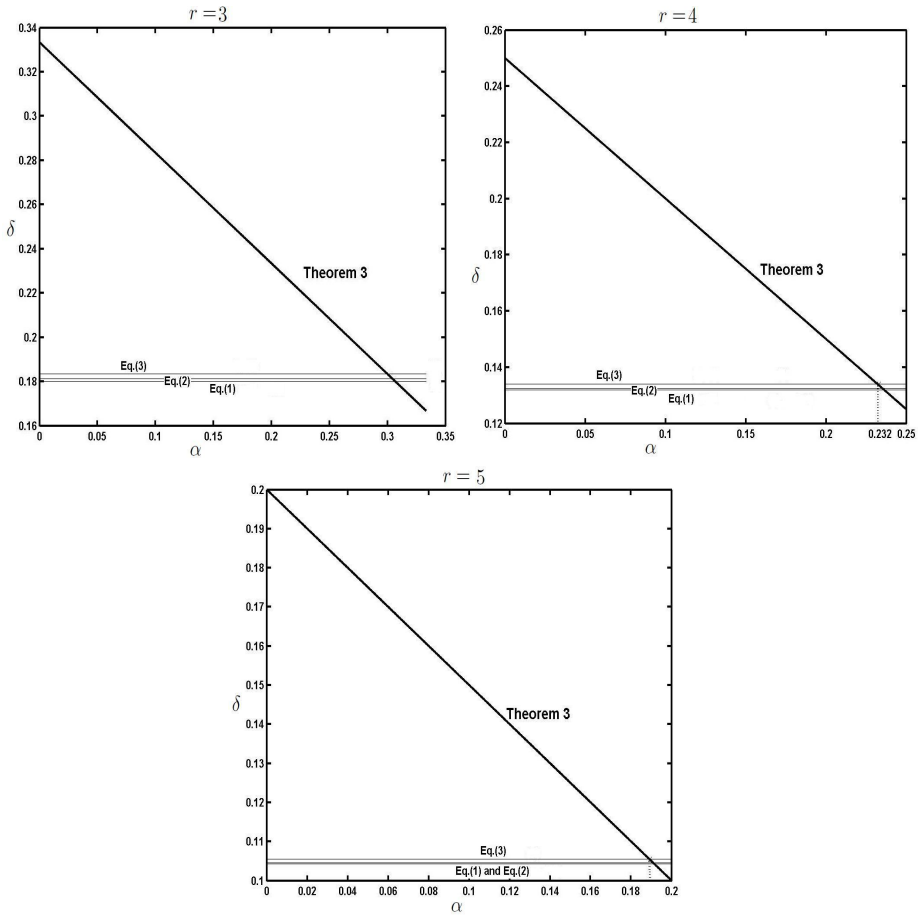

Fig. 1. Comparison between Theorem 3 and previous private exponent attacks on MPRSA

between our attack and attacks of Hinek *et al.* (Eqs.(1) and (2)) [11,12] and Ciet *et al.* (Eq.(3))[6,11] when $r = 3, 4$, and 5, where

$$\delta < \frac{1}{3r}(4r - 1 - 2\sqrt{(r-1)(4r-1)}) - \epsilon,\ \epsilon > 0 \tag{1}$$

$$\delta < \frac{1}{5r}(6 - 4r + 2\sqrt{4r^2 - 7r + 4}) - \epsilon,\ \epsilon > 0 \tag{2}$$

$$\delta < (r - \sqrt{r(r-1)})/r - \epsilon,\ \epsilon > 0 \tag{3}$$

5 Numerical Example

In this section we give an example for the presented attack. We used Shoup's package [20] NTL in the implementation.

Let $n = p_1p_2p_3p_4$ be a product of four primes each of size 100 decimal digits such that $p_4 - p_1 \leq n^{0.19}$. Thus, $\alpha = 0.19$ and $\delta = 0.15$.

Suppose that e of size 400 decimal digits.

$n = 25573763889872927537617615777695651985936974831528660360885069448895577$
$13240873561141263153256675011291710696981355151597274521278492940446577$
$08310744010276679704862894640223344687429432593752204272004537285252677$
$61909319087570432256645683464670571033014357021713074121467159222772877$
$20142528841621833611993102873657868395542500974683107511901381914226577$
$04633019373012901323148412639226756340320876562656757.$

$e = 12826145240584271570621841656548046666862027139453531607165614567116627$
$14400477970874371504503861100686991120228942885371691652375440581552307$
$69892604327625491593782689356669556162952379150674089128644648923560077$
$21785147253950635172743190949148724984940209259672479885879192200723926$
$35516490877868205804737002779941001636650813971269269387752182110198087$
$38177155732917433260529153810425421897963203104501.$

Now, we compute $m = n - \Gamma$.

$m = 25573763889872927537617615777695651985936974831528660360885069448895577$
$13240873561141263153256675011147861984280940468198992057360325443793217$
$45582639838523183762367859610857277295984254393206641278060230076748837$
$48674569437522275918954110104822367211853537337312799778335814054922087$
$92707297274099290970525439023098990024040746265715839794074250643833167$
$94875626840505790931689488829900292770669173758408.$

and **CF** $(e/m) =$

[0, 1, 1, 162, 2, 1, 63, 1, 4, 5, 2, 1, 1, 1, 1, 9, 2, 1, 1, 2, 1, 5, 1, 1, 278, 1, 10, 3, 2, 1, 3, 1, 1, 1, 1, 2, 1, 7, 3, 11, 7, 15, 1, 1, 1, 17, 4, 5, 2, 2, 2, 8, 1, 2, 3, 1, 6, 1, 1, 1, 1, 4, 2, 2, 1, 1, 2, 3, 1, 1, 14, 1, 2, 7, 1, 1, 3, 2, 2, 1, 1, 1, 2, 5, 143, 1, 2, 1, 1, 1, 10, 1, 7, 18, 1, 4, 3, 1, 1, 101, 1, 8, 2, 1, 32, 1, 6, 2, 8, 1, 2, 53, 11, 3, 3, 1, 1, 1, 1, 1, 2, 1, 164633286127802034691783544536 7, 1, 6, 3, 1, 1, 4, 1, 2, 1, 11, 1, 4, 3, 1, 2, 1, 1, 1, 7, 2, 5, 5, 1, 1, 1, 1, 2, 1, 1, 2, 2, 1, 5, 1, 2, 1, 4, 1, 2, 1, 5, 10, 1, 7, 1, 4, 1, 4, 2, 1, 1, 1, 1, 3, 154, 5, 2, 11, 2, 23, 7, 1, 2, 1, 6, 5, 1, 9, 1, 6, 1, 8, 1, 3, 3, 1, 1, 8, 2, 1, 6, 1, 1, 2, 9, 2, 3, 1, 1, 3, 1, 1, 2, 1, 1, 7, 1, 6, 2, 1, 2, 1, 7, 2, 71, 2, 1, 5, 2, 1, 97, 4, 1, 1, 1, 1, 3, 1, 2, 6, 2, 1, 5, 1, 33, 15, 1, 1, 5, 1, 1, 19, 2, 1, 6, 5, 2, 8, 1, 1, 14, 1, 1, 1, 2, 1, 2, 12, 1, 2, 3, 3, 133, 3, 6, 12, 3, 14, 1, 3, 29, 3, 5, 3, 4, 1, 1, 1, 2, 4, 15, 2, 15, 1, 1, 3, 6, 1, 2, 2, 1, 5, 3, 1, 6, 18, 1, 1, 1, 2, 1, 1, 1, 1, 1, 1, 69, 399, 4, 1, 6, 1, 3, 3, 1, 1, 1, 6, 1, 7, 1, 3, 8, 1, 2, 50, 3, 1, 1, 11, 2, 62, 1, 5, 5, 1, 1, 1, 3, 1, 1, 1, 6, 1, 2, 3, 1, 2, 1, 1, 1, 12, 5, 1, 22, 2, 36, 1, 1, 1, 3, 4, 1,

4, 15, 1, 3, 1, 3, 2, 1, 1, 1, 3, 1, 5, 2, 2, 1, 1, 17, 1, 16, 1, 2, 1, 1, 6, 6, 27, 3, 1, 4, 2, 2, 10, 2, 1, 2, 3, 2, 1, 1, 4, 4, 11, 2, 3, 1, 10, 1, 1, 2, 1, 1, 2, 20, 13, 1, 2, 1, 3, 3, 1, 1, 1, 1, 11, 3, 1, 1, 97, 1, 4, 12, 3, 6, 2, 73, 1, 1, 1, 1, 3, 1, 1, 16, 8, 4, 5, 1, 2, 60, 1, 1, 10, 1, 3, 2, 1, 1, 2, 20, 1, 1, 1, 2, 1, 61, 1, 3, 1, 44, 2, 13, 1, 1, 6, 3, 4, 1, 3, 1, 2, 202, 1, 4, 1, 9, 1, 2, 2, 1, 40, 1, 8, 2, 6, 99, 3, 2, 3, 1, 10, 2, 22, 1, 4, 1, 3, 4, 1, 3, 1, 15, 2, 10, 5, 1, 1, 1, 427, 1, 3, 1, 2, 3, 2, 2, 91, 1, 1, 1, 2, 1, 1, 2, 1, 23, 1, 3, 12, 6, 2, 13, 1, 16, 1, 1, 8, 4, 1, 2, 44, 1, 2, 22, 2, 1, 1, 4, 1, 3, 27, 1, 2, 3, 1, 2, 7, 1, 6, 1, 1, 1, 6, 5, 1, 1, 1, 1, 1, 1, 5, 4, 1, 1, 15, 2, 1, 4, 18, 1, 1, 1, 2, 2, 3, 2, 4, 13, 4, 1, 9, 3, 1, 2, 11, 1, 1, 6, 30, 2, 2, 2, 11, 17, 1, 1, 1, 1, 1, 2, 7, 7, 1, 2, 2, 1, 2, 1, 3, 7, 31, 1, 3, 1, 2, 452, 1, 19, 9, 11, 1, 2, 1, 1, 2, 6, 1, 28, 10, 4, 1, 2, 3, 2, 5, 2, 1, 15, 1, 3, 2, 42, 5, 1, 1, 2, 1, 1, 4, 1, 1, 9, 2, 1, 3, 8, 6, 32, 1, 3, 2, 12, 1, 4, 1, 11, 2, 1, 41, 4, 1, 6, 2, 1, 1, 48, 2, 2, 3, 2, 2, 4, 2, 4, 4, 10, 1, 12, 14, 4, 1, 2, 92].

Thus, we can conclude that

$$d = 189877018016769650162234978064222550351916979376481456967901.$$

$$p_1 = 71112944731410736200936098026102194286183896202223461645293266435374\backslash 24133992279467748393278156440741.$$

$$p_2 = 71112944731410736200936161704354259548674079134065376681839091861977\backslash 76492054347020753847107491042031.$$

$$p_3 = 71112944731410736200936135161274092520974419744378917664439975869666\backslash 14471703183603466271783937017379.$$

$$p_4 = 71112944731410736200936153839445191771143086686623743978164216730335\backslash 75558876657813072394314100437063.$$

6 Conclusion and Futures Work

Let $n = p_1 p_2 \cdots p_r$, and $p_r - p_1 = n^\alpha$. Based on Wiener's Interval , we have showed that MPRSA is insecure if $2d^2 + 1 < \frac{n^{2/r-\alpha}}{6r} < \phi(n)$, for $r \geq 3$; and $2d^2 + 1 < 2n^{3/2-2\alpha} + 1$, for $r = 2$ and $\phi(n) > \frac{3}{4}n$.

Many interesting questions arise from the work presented above. For examples:

1. The possibility to generalize Fermat's method to MPRSA. It seems that $p_r - p_1 = n^\alpha$, $\alpha = \frac{1}{r}$.
2. Uses of lattice instead of CF.
3. Improve the condition $2d^2 + 1 < \frac{n^{2/r-\alpha}}{6r}$.

References

1. Alison, C., Paixão, M.: An efficient variant of the RSA cryptosystem, http://eprint.iacr.org/2003/159
2. Blömer, J., May, A.: A Generalized Wiener Attack on RSA. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 1–13. Springer, Heidelberg (2004)
3. Boneh, D.: Twenty years of attacks on the RSA cryptosystem. Notices of the American Mathematical Society 46(2), 203–213 (1999)
4. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. on Information Theory 46(4), 1339–1349 (2000)
5. Boneh, D., Shacham, H.: Fast Variants of RSA. CryptoBytes 5(1), 1–9 (2002)
6. Ciet, M., Koeune, F., Laguillaumie, F., Quisquater, J.-J.: Short private exponent attacks on fast variants of RSA. UCL Crypto Group Technical Report Series CG-2003/4, Universite Catholique de Louvain (2003)
7. Collins, T., Hopkins, D., Langford, S., Sabin, M.: Public key cryptographic apparatus and method. US patent #5, 848, 149 (January 1997)
8. Coppersmith, D.: Small solutions to polynomial equations and low exponent vulnerabilities. Journal of Cryptology 10(4), 223–260 (1997)
9. Durfee, G., Nguyen, P.: Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt 99. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 14–29. Springer, Heidelberg (2000)
10. Hinek, M.J.: On the security of multi-prime RSA. Journal of Mathematical Cryptology 2(2), 117–147 (2008)
11. Hinek, M.J.: Cryptanalysis of RSA and its variants. Chapman & Hall/CRC (2010)
12. Hinek, M.J., Low, M.K., Teske, E.: On Some Attacks on Multi-prime RSA. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 385–404. Springer, Heidelberg (2003)
13. Lenstra, A.K., Lenstra, H.W., Lovasz, L.: Factoring polynomials with rational coefficients. Mathematische Annalen 261, 513–534 (1982)
14. Lim, S., Kim, S., Yie, I., Lee, H.: A Generalized Takagi-Cryptosystem with a Modulus of the Form $p^r q^s$. In: Roy, B., Okamoto, E. (eds.) INDOCRYPT 2000. LNCS, vol. 1977, pp. 283–294. Springer, Heidelberg (2000)
15. Maitra, S., Sarkar, S.: Revisiting Wiener's Attack – New Weak Keys in RSA. In: Wu, T.-C., Lei, C.-L., Rijmen, V., Lee, D.-T. (eds.) ISC 2008. LNCS, vol. 5222, pp. 228–243. Springer, Heidelberg (2008)
16. May, A.: New RSA Vulnerabilities using Lattics Reduction Methods. Ph.D. Dissertation. University of Paderborn (2003)
17. Nassr, D., Bahig, H.M., Bhery, A., Dauod, S.: A New RSA Vulnerability Using Continued Fractions. In: Proceeding of the Sixth IEEE/ACS International Conference on Computer Systems and Applications (Security and Information Assurance Track), April 31- May 4, pp. 694–701 (2008)
18. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communication of ACM 21, 120–126 (1978)
19. Rosen, K.H.: Elementary Number Theory. Addison-Wesley, Reading Mass (1984)
20. Shoup, V.: NTL: A Library for doing Number Theory, http://www.shoup.net/ntl/index.html
21. Steinfeld, R., Contini, S., Pieprzyk, J., Wang, H.: Converse Results to the Wiener Attack on RSA. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 184–198. Springer, Heidelberg (2005)

22. Verheul, E.R., van Tilborg, H.C.A.: Cryptanalysis of 'less short' RSA secret exponents. Applicable Algebra in Engineering, Communication and Computing 8, 425–435 (1997)
23. de Weger, B.: Cryptanalysis of RSA with small prime difference. Applicable Algebra in Engineering, Communication and Computing 13(1), 17–28 (2002)
24. Wiener, M.: Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory 36, 553–558 (1990)