Malaysian Journal of Mathematical Sciences 11(S) August: 45 - 57 (2017)
Special Issue: The 5th International Cryptology and Information Security Conference (New Ideas in Cryptology)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

A New Attack on the RSA Cryptosystem Based on Continued Fractions

Bunder, M.[1] and **Tonien, J**[2]

[1]*School of Mathematics and Applied Statistics, University of Wollongong, Australia*
[2]*School of Computing and Information Technology, University of Wollongong, Australia*

E-mail: joseph_tonien@uow.edu.au

ABSTRACT

This paper presents a new improved attack on RSA based on Wiener's technique using continued fractions. In the RSA cryptosystem with public modulus $N = pq$, public key e and secret key d, if $d < \frac{1}{3}N^{\frac{1}{4}}$, Wiener's original attack recovers the secret key d using the convergents of the continued fraction of $\frac{e}{N}$. Our new method uses the convergents of the continued fraction of $\frac{e}{N'}$ instead, where N' is a number depending on N. We will show that our method can recover the secret key if $d^2e < 8N^{\frac{3}{2}}$, so if either d or e is relatively small the RSA encryption can be broken. For $e \approx N^t$, our method can recover the secret key if $d < 2\sqrt{2}N^{\frac{3}{4}-\frac{t}{2}}$ and certainly for $d < 2\sqrt{2}N^{\frac{1}{4}}$. Our experiments demonstrate that for a 1024-bit modulus RSA, our method works for values of d of up to 270 bits compared to 255 bits for Wiener.

Keywords: RSA, Wiener's attack, continued fractions.

1. Introduction

The RSA public-key cryptosystem is one of the most popular systems in use today. The key setup involves picking two large prime numbers p, q to form a product $N = pq$ and selecting two integers $e, d < \phi(N) = (p-1)(q-1)$ such that $ed = 1 \pmod{\phi(N)}$. Messages can be encrypted using the public key (N, e), whereas ciphertexts can be decrypted using the secret key (p, q, d). It is well known that RSA is not secure if the secret key d is relatively small.

An attack on RSA with low secret key d was given by Wiener (Wiener, 1990) about 25 years ago. Wiener showed that using continued fractions, one can efficiently recover the secret key d from the public information (N, e) as long as $d < \frac{1}{3}N^{\frac{1}{4}}$ (see also (Boneh and Durfee, 2000, Nassr et al., 2008)). In 2005, Steinfeld et al (Steinfeld et al., 2005) showed that for linear attack $N^{\frac{1}{4}}$ is the best bound in the sense that for any fixed $\epsilon > 0$ and all sufficiently large modulus lengths, Wiener's attack succeeds with negligible probability over a random choice of $d < N^{\delta}$ as soon as $\delta > \frac{1}{4} + \epsilon$. Exploiting a non-linear equation satisfied by the secret key, Boneh and Durfee (Boneh and Durfee, 2000) presented a lattice-based attack that succeeds in polynomial-time when $d < N^{0.292}$.

In this paper, we present a new improved attack on RSA based on Wiener's technique using continued fractions. As in Wiener's original attack, our method only uses the public information (N, e). The difference between our attack and Wiener's is that in Wiener's attack one is searching the convegents of the continued fraction of $\frac{e}{N}$ whereas in ours, one is searching the convegents of the continued fraction of $\frac{e}{N'}$ where N' is given by

$$N' = \left\lceil N - (1 + \frac{3}{2\sqrt{2}})N^{\frac{1}{2}} + 1 \right\rceil$$

We will show that our method can recover the secret key if $d^2 e < 8N^{\frac{3}{2}}$. So if $e \approx N^t$, then our method can recover the secret key if $d < 2\sqrt{2}\,N^{\frac{3}{4}-\frac{t}{2}}$ and certainly for $d < 2\sqrt{2}\,N^{\frac{1}{4}}$ – which is more than 8 times the Wiener's bound. In Figure 1, the shaded part shows the area where our method is better than Wiener's (Wiener, 1990) and Boneh–Durfee's (Boneh and Durfee, 2000) ones.

There are other variants of Wiener's attack but these attacks need more than just the public information (N, e). For example, De Weger's attack (De Weger, 2002) exploited the small distance between the two RSA's secret primes: if $|p - q| = N^{\beta}$ and $d = N^{\delta}$ then d can be recovered if $2 - 4\beta < \delta < 1 - \sqrt{2\beta - \frac{1}{2}}$

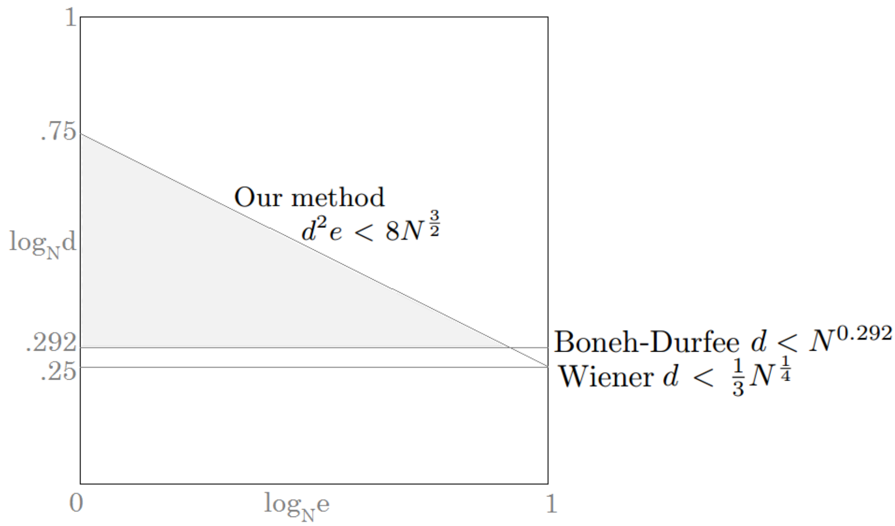

Figure 1: Comparison between our method and Wiener's (Wiener, 1990) and Boneh–Durfee's (Boneh and Durfee, 2000) ones.

or $\delta < \frac{1}{6}(4\beta+5) - \frac{1}{3}\sqrt{(4\beta+5)(4\beta-1)}$. The Blömer and May (Blömer and May, 2004) attack assumed a linear relation between e and $\phi(N)$: $ex + y = 0 \bmod \phi(N)$ with either $0 < x < \frac{1}{3}N^{\frac{1}{4}}$ and $y = \mathcal{O}(N^{-\frac{3}{4}}ex)$ (their Theorem 2) or $x < \frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}}$ and $|y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$ (their Theorem 4). These conditions are much more complex than ours: $d^2 e < 8N^{\frac{3}{2}}$, particularly because they have in addition to p, q and d the unknown x and y. For the case $x = d$ and $y = -1$, used by Wiener and us, our result is better than Blömer–May's Theorem 2 result and also better than their Theorem 4 result if $\frac{9}{8} < \frac{p}{q} < 2$, and theirs is better if $1 < \frac{p}{q} < \frac{9}{8}$. Nassr et al's (Nassr et al., 2008) attack required an approximation $p_o \geq \sqrt{N}$ of the prime p with $|p - p_0| \leq \frac{1}{8}n^{\alpha}$, $\alpha \leq \frac{1}{2}$, $\delta < \frac{1-\alpha}{2}$.

The Blömer and May (Blömer and May, 2001) attack is a variant of the Boneh-Durfee attack (Boneh and Durfee, 2000) which works for $d < N^{0.29}$. Using an exhaustive search of about $8 + 2b$ bits, Verheul and van Tilborg (Verheul and van Tilborg, 1997) improved Wiener's bound to $d < 2^b N^{\frac{1}{4}}$. Another exponential time attack similar to this is due to Dujella (Dujella, 2004).

The rest of the paper is organized as follows. In Section 2, we review some preliminary results on continued fractions and Wiener's attack. Section 3 presents our main result which says that the RSA encryption system is not secure if $e \approx N^t$ and $d < 2\sqrt{2}\, N^{\frac{3}{4}-\frac{t}{2}}$. As $t < 1$, this means that RSA encryption is not secure for $d < 2\sqrt{2}\, N^{\frac{1}{4}}$ compared to Wiener's result of $d < \frac{1}{3}N^{\frac{1}{4}}$. In Section 4, we show our experiment result with a 1024-bit modulus and 270-bit secret key. We show that our usage of continued fraction of $\frac{e}{N'}$ is essential because if we use the continued fraction expansion of $\frac{e}{N}$ as in Wiener's attack then the secret key cannot be found.

2. Preliminaries

RSA is a public-key cryptosystem widely used for secure data transmission. In general, such a cryptosystem consists of two functions, *encrypt* and *decrypt*. The encryption function takes a *public encryption key* e and a message m and outputs a ciphertext

$$c = encrypt_e(m),$$

the decryption function is the inverse function, which takes a *secret decryption key* d and a ciphertext c and outputs back the original message

$$m = decrypt_d(c).$$

The algorithm is called a public-key cryptosystem because the encryption key is made public and the decryption key is kept secret. It means that anyone can encrypt messages but only the owner of the secret decryption key can read them.

RSA Key Generation algorithm

- Choose two distinct prime numbers p and q of similar bit-length.
- Compute $N = pq$, $\phi(N) = (p-1)(q-1)$
- Choose e such that $(e, \phi(N)) = 1$
- Determine $d = e^{-1} \pmod{\phi(N)}$
- Keep p, q, d secret, publish N, e.

RSA Encryption-Decryption algorithm

- For a message $m \in (1, N)$, the ciphertext c is

$$c = m^e \pmod{N}$$

- For a ciphertext $c \in (1, N)$, the message m is determined as
$$m = c^d \pmod N$$

The complexity of the decryption algorithm is based on the size of the decryption key d. In a cryptosystem with a limited resource such as a credit card, it is desirable to have a smaller value of d. Wiener's attack, uses the *continued fraction* method to expose the private key d when d is small ($d < \frac{1}{3}N^{\frac{1}{4}}$).

A *continued fraction* is an expression of the form

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$$

The continued fraction expansion of a number is formed by subtracting away the integer part of it and inverting the remainder and then repeating this process again and again. For example,

$$\begin{aligned}
\frac{2000}{123} &= 16 + \frac{32}{123} = 16 + \frac{1}{\frac{123}{32}} = 16 + \cfrac{1}{3 + \cfrac{27}{32}} = 16 + \cfrac{1}{3 + \cfrac{1}{\frac{32}{27}}} \\
&= 16 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{5}{27}}} = 16 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{\frac{27}{5}}}} = 16 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{2}{5}}}} \\
&= 16 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{\frac{5}{2}}}}} = 16 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{2}}}}}
\end{aligned}$$

As we have seen above, the coefficients a_i of the continued fraction of a number x are constructed as follows:

$$x_0 = x, \ a_n = [x_n], \ x_{n+1} = \frac{1}{x_n - a_n}$$

We use the following notation to denote the continued fraction

$$x = [a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$$

If $k \leq n$, the continued fraction $[a_0, a_1, \ldots, a_k]$ is called the k^{th} *convergent* of x. The following theorem gives us the *fundamental recursive formulas* to calculate the convergents.

Theorem 2.1. *The k^{th} convergent can be determined as*

$$[a_0, \ldots, a_k] = \frac{p_k}{q_k}$$

where the sequences $\{p_n\}$ and $\{q_n\}$ are specified as follows[1]*:*

$$\begin{aligned} p_{-2} = 0, \quad p_{-1} = 1, \quad p_n &= a_n p_{n-1} + p_{n-2}, \quad \forall n \geq 0, \\ q_{-2} = 1, \quad q_{-1} = 0, \quad q_n &= a_n q_{n-1} + q_{n-2}, \quad \forall n \geq 0. \end{aligned}$$

The following theorem (Hardy and Wright, 1979) is the basis for Wiener's attack.

Theorem 2.2. *Let p, q be positive integers such that*

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$$

then $\frac{p}{q}$ is a convergent of the continued fraction of x.

The following theorem summarises Wiener's attack (Boneh and Durfee, 2000, Wiener, 1990).

Theorem 2.3. *In a RSA algorithm, if the following conditions are satisfied*

- $q < p < 2q$ *(i.e. p and q are two primes of the same bit size)*
- $0 < e < \phi(N)$

[1]The convergents start with $\frac{p_0}{q_0}$, but it is a convention to extend the sequence index to -1 and -2 to allow the recursive formula to hold for $n = 0$ and $n = 1$

- $ed - k\phi(N) = 1$
- $\boxed{d < \dfrac{1}{3}N^{\frac{1}{4}}}$

then $\frac{k}{d}$ *is a convergent of* $\frac{e}{N}$. *Thus, the secret information* p, q, d, k *can be recovered from public information* (e, N).

Since $\frac{e}{N}$ has $O(\log(N))$ number of convergents, Wiener's algorithm will succeed to factor N and output p, q, d, k in $O(\log(N))$ time complexity.

Example 1. In the following example, we have a 1024-bit modulus N, the upper bound $\frac{1}{3}N^{\frac{1}{4}}$ in Theorem 2.3 is 255-bit, d is 255-bit and we have found the convergent $c_{149} = \frac{p_{149}}{q_{149}} = \frac{k}{d}$ as asserted by Theorem 2.3.

p	12137 2429807756 5612551149 2629609691 9449141205 8680156593 9661850265 4224438815 0519802020 4979508724 3102230079 9409502534 6163494126 0471531617 7098769594 1320931493	512 bits
q	9201 0524322086 3900671386 8662660639 9738950237 2692456878 2613825773 8431082681 6215281513 7070448098 3908271161 4206768781 4447541784 7243525840 6453897707 3778553491	512 bits
N	111675409 0485730823 5978712392 1718417590 8091542898 6532382066 5485087798 8534958587 2419428390 8818158158 7258671440 7683378413 7900981405 8406611299 6495087782 9075022344 5692173775 8022280271 1775885570 7370037539 5363272503 0411307566 7128393688 9712399229 9533595050 1425299028 6693467091 9270372721 8720248761 5489260235 4246992063	1024 bits
$\phi(N)$	111675409 0485730823 5978712392 1718417590 8091542898 6532382066 5485087798 8534958587 2419428390 8818158158 7258671440 7683378413 7900981405 8406611299 6495087782 9075001006 2738043932 8509057735 0483615238 8181946096 3990659030 8135631527 4472872192 2977315695 7483638227 4414797787 3077195775 8659336811 1005191303 1936592933 9147507080	1024 bits
Theorem 2.3 bound $\frac{1}{3}N^{\frac{1}{4}}$	3426637 2625316286 2968546235 7247145632 3454416288 1157194267 8892540948 5361638977	255 bits
e	45643085 8324017120 3133152071 1529402253 9055348712 7592566099 1853899212 7134329984 8723684744 2845550165 4714497720 7173865355 1358820024 8341016147 1746464324 1362580067 0745402653 2892481331 8307985083 2822164891 3129959216 3726940854 8355291478 1683701096 4254131032 8949699809 7582249761 4243019490 2375579169 7150271910 4226716997	1023 bits
d	3426637 2625316286 2968546235 7247145632 3454416288 1157194267 8892540948 5361638973	255 bits
k	1400507 9544612205 2131699024 5626308122 5492430329 4046240953 0743691100 4314600526	253 bits
convergent of $\frac{e}{N}$	found $c_{149} = \frac{p_{149}}{q_{149}} = \frac{k}{d}$	

3. A New Improved Attack Based on Continued Fractions

In this section, we present our main result. Instead of using the convergents of the continued fraction of $\frac{e}{N}$ as in the Wiener's original attack, we will use the convergents of the continued fraction of $\frac{e}{N'}$ where N' is given by

$$N' = \left[N - (1 + \frac{3}{2\sqrt{2}})N^{\frac{1}{2}} + 1\right]$$

We will show that for $e \approx N^t$, the secret key can be recovered if $d < 2\sqrt{2}\,N^{\frac{3}{4}-\frac{t}{2}}$.

First, we need the following auxiliary result.

Lemma 3.1. *For* $N > 2000000$,

$$\frac{(\frac{3}{\sqrt{2}} - 2)N^{\frac{1}{2}} + 4}{2(N - \frac{3}{\sqrt{2}}N^{\frac{1}{2}})^2} < \frac{1}{16N^{\frac{3}{2}}}.$$

Proof. We have

$$\begin{aligned}
& \frac{(\frac{3}{\sqrt{2}} - 2)N^{\frac{1}{2}} + 4}{2(N - \frac{3}{\sqrt{2}}N^{\frac{1}{2}})^2} < \frac{1}{16N^{\frac{3}{2}}} \\
\Leftrightarrow \quad & 8N^{\frac{1}{2}}((\frac{3}{\sqrt{2}} - 2)N^{\frac{1}{2}} + 4) < (N^{\frac{1}{2}} - \frac{3}{\sqrt{2}})^2 \\
\Leftrightarrow \quad & (12\sqrt{2} - 16)N + 32N^{\frac{1}{2}} < N - 3\sqrt{2}N^{\frac{1}{2}} + \frac{9}{2} \\
\Leftrightarrow \quad & (32 + 3\sqrt{2})N^{\frac{1}{2}} < (17 - 12\sqrt{2})N + \frac{9}{2} \\
\Leftrightarrow \quad & \frac{32 + 3\sqrt{2}}{17 - 12\sqrt{2}} < N^{\frac{1}{2}} + \frac{9}{2(17 - 12\sqrt{2})N^{\frac{1}{2}}}
\end{aligned}$$

This is true because $N > 200000 > \left(\frac{32+3\sqrt{2}}{17-12\sqrt{2}}\right)^2$. $\blacksquare$

This is our main theorem.

Theorem 3.1. *In a RSA algorithm, if the following conditions are satisfied*

- $q < p < 2q$
- $0 < e < \phi(N)$
- $ed - k\phi(N) = 1$
- $N > 2000000$
- $\boxed{d < 2\sqrt{2}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{\frac{1}{4}}}$

and

$$N' = \left[N - (1 + \frac{3}{2\sqrt{2}})N^{\frac{1}{2}} + 1\right]$$

then $\frac{k}{d}$ *is a convergent of* $\frac{e}{N'}$*. Thus, the secret information* p, q, d, k *can be recovered from public information* (e, N)*.*

Proof. Let $\phi_1 = N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}}$ and $\phi_2 = N + 1 - 2N^{\frac{1}{2}}$. It follows from $q < p < 2q$ that $1 < \sqrt{\frac{p}{q}} < \sqrt{2}$, so since the function $f(x) = x + \frac{1}{x}$ is increasing on $[1, +\infty)$,

$$\begin{aligned}
&2 < \frac{p+q}{N^{\frac{1}{2}}} = \sqrt{\frac{p}{q}} + \sqrt{\frac{q}{p}} < \sqrt{2} + \frac{1}{\sqrt{2}} = \frac{3}{\sqrt{2}} \\
&2N^{\frac{1}{2}} < p + q < \frac{3}{\sqrt{2}}N^{\frac{1}{2}} \\
&\phi_1 = N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} < \phi(N) < N + 1 - 2N^{\frac{1}{2}} = \phi_2
\end{aligned}$$

Let $\phi_{mid} = N - (1 + \frac{3}{2\sqrt{2}})N^{\frac{1}{2}} + 1$, then ϕ_{mid} is the midpoint of the interval $[\phi_1, \phi_2]$ and $N' = [\phi_{mid}]$. Since $\phi(N) \in (\phi_1, \phi_2)$,

$$|\phi(N) - N'| < |\phi(N) - \phi_{mid}| + |\phi_{mid} - N'| < \frac{1}{2}(\phi_2 - \phi_1) + 1 = \frac{1}{2}(\phi_2 - \phi_1 + 2)$$

We have

$$\begin{aligned}\left|\frac{e}{N'}-\frac{k}{d}\right| &= \left|\left(\frac{e}{N'}-\frac{e}{\phi(N)}\right)+\left(\frac{e}{\phi(N)}-\frac{k}{d}\right)\right| = \left|\frac{e(\phi(N)-N')}{N'\phi(N)}+\frac{1}{d\phi(N)}\right| \\ &= \left|\frac{e(\phi(N)-N')}{N'\phi(N)}+\frac{e}{\phi(N)(k\phi(N)+1)}\right| \\ &< \frac{e|\phi(N)-N'|}{N'\phi(N)}+\frac{e}{\phi(N)(k\phi(N)+1)} \\ &< \frac{e(\phi_2-\phi_1+2)/2}{\phi_1^2}+\frac{e}{\phi_1^2} < \frac{e(\phi_2-\phi_1+4)}{2(\phi_1-1)^2} = e\,\frac{(\frac{3}{\sqrt{2}}-2)N^{\frac{1}{2}}+4}{2(N-\frac{3}{\sqrt{2}}N^{\frac{1}{2}})^2}\end{aligned}$$

For $N > 2000000$, by Lemma 3.1, we have

$$\frac{(\frac{3}{\sqrt{2}}-2)N^{\frac{1}{2}}+4}{2(N-\frac{3}{\sqrt{2}}N^{\frac{1}{2}})^2} < \frac{1}{16N^{\frac{3}{2}}}.$$

Therefore,

$$\left|\frac{e}{N'}-\frac{k}{d}\right| < \frac{e}{16N^{\frac{3}{2}}} < \frac{1}{2d^2}. \quad \blacksquare$$

The boxed condition in Theorem 3.1 amounts to $d^2e < 8N^{\frac{3}{2}}$, so if either d or e is relatively small then RSA encryption can be broken. When e is relatively small, the Wiener attack cannot be applied, whereas ours can.

This result is superficially like that of Blömer-May (Blömer and May, 2004)(Theorem 4), which is

Theorem 3.2. *(Blömer and May, 2004) Given an RSA public key tuple (N, e), where $N = pq$. Suppose that e satisfies an equation $ex + y = 0 \pmod{\phi(N)}$ with*

$$0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p-q} \text{ and } |y| \leq \frac{p-q}{\phi(N)\,N^{\frac{1}{4}}}ex$$

then N can be factored in time polynomial in $\log N$.

With $x = d$ and $y = -1$, these conditions amount to

$$ed^2 < \frac{\phi(N)\,N^{\frac{3}{2}}}{9(p-q)^2} \tag{1}$$

and

$$\phi(N)\, N^{\frac{1}{4}} < (p-q)ed, \tag{2}$$

whereas our only condition is $ed^2 < 8N^{\frac{3}{2}}$. Let R be the ratio between our bound and Blömer-May's bound (1)

$$R = \frac{8N^{\frac{3}{2}}}{\frac{\phi(N)\, N^{\frac{3}{2}}}{9(p-q)^2}} = \frac{72(p-q)^2}{\phi(N)}$$

then

$$R = \frac{N}{\phi(N)} \frac{72(p-q)^2}{pq} = \frac{N}{\phi(N)} \frac{72(\frac{p}{q}-1)^2}{\frac{p}{q}}$$

Since $q < p < 2q$, the quotient $\frac{p}{q}$ ranges in the interval $(1, 2)$. Consider the graph of the function $f(x) = \frac{72(x-1)^2}{x}$ for $x \in (1, 2)$, we can see that $f(x) < 1$ for $x \in (1, \frac{9}{8})$ and $f(x) > 1$ for $x \in (\frac{9}{8}, 2)$. Therefore, if $\frac{p}{q} \in (\frac{9}{8}, 2)$ then $R = \frac{N}{\phi(N)} f(\frac{p}{q}) > 1$ and our bound is better than Blömer-May's bound. Our experiment result in Section 4 also confirms this.

From Theorem 3.1, we have

Corollary 3.1. *In a RSA algorithm, if the following conditions are satisfied*

- $q < p < 2q$
- $0 < e < \phi(N)$
- $ed - k\phi(N) = 1$
- $N > 2000000$
- $\boxed{d < 2\sqrt{2}N^{\frac{1}{4}}}$

and

$$N' = \left[N - (1 + \frac{3}{2\sqrt{2}})N^{\frac{1}{2}} + 1 \right]$$

then $\frac{k}{d}$ *is a convergent of* $\frac{e}{N'}$. *Thus, the secret information* p, q, d, k *can be recovered from public information* (e, N).

Note that Corollary 3.1 has $d < 2\sqrt{2}\, N^{\frac{1}{4}}$ while Wiener's result had $d < \frac{1}{3} N^{\frac{1}{4}}$.

4. Experiment Result

We will use the same 1024-bit modulus as in Example 1. With this 1024-bit modulus, the Wiener's upper bound $\frac{1}{3}N^{\frac{1}{4}}$ is 255-bit. Here, we show an example of a 270-bit secret key.

N	111675409 0485730823 5978712392 1718417590 8091542898 6532382066 5485087798 8534958587 2419428390 8818158158 7258671440 7683378413 7900981405 8406611299 6495087782 9075022344 5692173775 8022280271 1775885570 7370037539 5363272503 0411307566 7128393688 9712399229 9533595050 1425299028 6693467091 9270372721 8720248761 5489260235 4246992063	1024 bits
Theorem 3.1 N'	111675409 0485730823 5978712392 1718417590 8091542898 6532382066 5485087798 8534958587 2419428390 8818158158 7258671440 7683378413 7900981405 8406611299 6495087782 9075000568 2159570564 0981693044 2093595665 5130899532 7328449321 6820552021 8559771355 1247634195 5201901221 0109431097 4104405733 7196789666 1898135689 1959781693 7504572404	1024 bits
e	9497738493 9533670765 7042840968 7659484313 7084252195 6357612333 8847198573 4448278894 7630928901 1796460405 3837337081 2904542700 5252696553 0732537894 7443876974 8735584808 1502373619 6458971201 9372820861 3917977593 0646731395 1290537294 6709829003 9830064227 6485488318 8298864198 1593551375 9303722339 5282843022 6076170323	997 bits
d	16 8426074727 9546104062 9984578341 1702121043 1469393463 8412655292 6172702449 5099104827	270 bits
k	1432 4253002139 3318566580 1576488907 6467402086 1953632340 7603167662 3143713764	244 bits
convergent of $\frac{e}{N}$ convergent of $\frac{e}{N'}$	not found, $c_i \neq \frac{k}{d}$, $\forall i$ found $c_{146} = \frac{p_{146}}{q_{146}} = \frac{k}{d}$	

This experiment result shows that our usage of continued fractions of $\frac{e}{N'}$ is *essential*. If we use continued fractions of $\frac{e}{N}$ as in Wiener's original attack then no convergent c_i is found for which $c_i = \frac{k}{d}$.

For this example, the Blömer and May Theorems 2 and 4 results, with $x = d$ and $y = -1$, do not apply as neither of $d < \frac{1}{3}N^{\frac{1}{4}}$ and $d < \frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}}$ hold.

References

Blömer, J. and May, A. (2001). Low secret exponent RSA revisited. In *Cryptography and Lattices*, pages 4–19. Springer.

Blömer, J. and May, A. (2004). A generalized Wiener attack on RSA. In *International Workshop on Public Key Cryptography*, pages 1–13. Springer.

Boneh, D. and Durfee, G. (2000). Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE transactions on Information Theory*, 46(4):1339–1349.

De Weger, B. (2002). Cryptanalysis of RSA with small prime difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17–28.

Dujella, A. (2004). Continued fractions and RSA with small secret exponent. *arXiv preprint cs/0402052*.

Hardy, G. H. and Wright, E. M. (1979). *An introduction to the theory of numbers*. Oxford University Press.

Nassr, D. I., Bahig, H. M., Bhery, A., and Daoud, S. S. (2008). A new RSA vulnerability using continued fractions. In *Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on*, pages 694–701. IEEE.

Steinfeld, R., Contini, S., Wang, H., and Pieprzyk, J. (2005). Converse results to the Wiener attack on RSA. In *International Workshop on Public Key Cryptography*, pages 184–198. Springer.

Verheul, E. R. and van Tilborg, H. C. (1997). Cryptanalysis of 'less short' RSA secret exponents. *Applicable Algebra in Engineering, Communication and Computing*, 8(5):425–435.

Wiener, M. J. (1990). Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information theory*, 36(3):553–558.