A Generalization of de Weger’s Method

Chien-Yuan Chen  
Department of Computer Science and  
Information Engineering  
National University of Kaohsiung  
Kaohsiung 811, Taiwan  
E-mail: cychen07@nuk.edu.tw

Chih-Cheng Hsueh  
Department of Information and  
Commerce  
Aletheia University  
Tainan, 72147, Taiwan  
E-mail: jrcheng@mt.au.edu.tw

Yu-Feng Lin  
Department of Computer Science and  
Information Engineering  
National University of Kaohsiung  
Kaohsiung 811, Taiwan  
E-mail: aorborcord@gmail.com

Abstract—This paper generalizes de Weger’s method if the ratio of two RSA primes $\frac{p}{q}$ is close to a simple fraction $\frac{b}{a}$.

We can discover the secret exponent $d < N^{1/\tau}$ from the convergents of $\frac{e}{N+1-a+b\sqrt{N}}$ for $|ap-bq| = N^{\tau}$. Our method is thus reduced to Maitra and Sarkar’s method.

Keywords- RSA; continued fraction attack

I. INTRODUCTION

When the smart card uses RSA [9] for communications, it would be desirable for the smart card to have a short secret exponent. However, the short secret exponent $d$ can be easily attacked by Wiener’s method [13] if $d < \frac{1}{3} N^{1/3}$ and $e < N$, where $d$, $e$, and $N$ denote the secret exponent, the public exponent, and the modulus, respectively. Extending Wiener’s method, Verheul and van Tilborg [11] attacked $d < N^{1/3}$ by using an exhaustive search of about $8+2\tau$ bits. Dujella [3] proposed a variant of Wiener’s method similar to Verheul and van Tilborg’s attack.

In 2002, de Weger [12] improved Wiener’s bound to $d < N^{1/\delta}$ assuming that $N$ has a small difference between its prime factors $|q-p| = N^\delta$ for $\frac{1}{4} \leq \delta \leq \frac{1}{2}$. When $|q-p| = N^\delta$ is too large, de Weger’s method is in vain. Maitra and Sarkar [6] found that $|2p-q| = N^\delta$ is small for large $|q-p| = N^\delta$ because $p < q < 2p$. So, they attack $d < N^{1/\delta_{q-p}}$ from the convergents of $\frac{e}{N+1-\frac{3}{\sqrt{2}}\sqrt{N}}$ for a small number $\tau$. For simplicity, we round off the denominator when computing the convergents. For more variants of Wiener’s method, refer to [1, 2, 7, 8].

The de Weger method motivates us to discuss the security of RSA when the ratio of two RSA primes $\frac{p}{q}$ is close to a simple fraction $\frac{b}{a}$, where $a$ and $b$ are positive integers less than $\log N$. Let $|ap-bq| = N^\tau$. Assume that $(b(a^2+1)p-a(b^2+1)q)(ap-bq) > 0$. We can discover $d < N^{1/\tau}$ from the convergents of $\frac{e}{N+1-a+b\sqrt{N}}$. Our method is thus reduced to de Weger’s method if $a/b=1$. When $b/a = 1/2$, our method is reduced to Maitra and Sarkar’s method.

II. REVIEW OF DE WEGESE’S METHODS

Let $p$ and $q$ be RSA primes satisfying $p < q < 2p$. This implies that $2\sqrt{N} \leq p+q \leq \frac{3}{\sqrt{2}}\sqrt{N}$ [6]. In RSA, the public exponent $e$ and the secret exponent $d$ satisfy the relationship $ed = 1 \mod \phi(N)$, (2.1) where $\phi(N) = (p-1)(q-1)$. It means that $ed = 1 + k\phi(N)$, (2.2) where $k$ is an integer. Dividing both sides of Equation (2.2) by $d\phi(N)$, we get $\frac{e}{\phi(N)} = \frac{1}{d\phi(N)} + \frac{k}{d}$. (2.3)

In the above equation, de Weger used $\frac{e}{N+1-2\sqrt{N}}$ to estimate $\frac{e}{\phi(N)}$ and obtained that
Let $p$ and $q$ be RSA primes satisfying $p < q < 2p$. If \( \frac{p}{q} \) is close to \( \frac{b}{a} \) such that
\[
(b(a^2+1)p - a(b^2+1)q)(ap-bq) > 0,
\]
then
\[
\frac{a+b}{\sqrt{ab}} \sqrt{N} - (p+q) < \frac{(ap-bq)^2}{(a+b+2)\sqrt{N}}.
\]

**Proof.**

We first compute
\[
\frac{a+b}{\sqrt{ab}} \sqrt{N} - (p+q) = \frac{ab}{a+b+2} \left(\sqrt{N} - (p+q)\right) - \frac{(ap-bq)^2}{(a+b+2)\sqrt{N}}
\]

Because \((b(a^2+1)p - a(b^2+1)q)(ap-bq) > 0\), we get
\[
\frac{a+b}{\sqrt{ab}} \sqrt{N} - (p+q) < \frac{(ap-bq)^2}{(a+b+2)\sqrt{N}}.
\]

**Theorem 1.**

Let $p$ and $q$ be RSA primes satisfying $p < q < 2p$. Let \( |ap-bq| = N' \). If \( \frac{p}{q} \) is close to \( \frac{b}{a} \) such that
\[
(b(a^2+1)p - a(b^2+1)q)(ap-bq) > 0,
\]
then the secret exponent $d < N^{\frac{1}{2}}$ can be discovered from the convergents of
\[
\frac{e}{N+1-2\sqrt{N}}.
\]

**Proposition 1.**

If \( \frac{p}{q} \) is close to \( \frac{b}{a} \) such that \( ap-bq \neq 0 \) for two positive integers $a$ and $b$, then \( \phi(N) > N+1 - \frac{a+b}{\sqrt{ab}} \sqrt{N} \).

**Proof.**

Because \((ap-bq)(bp-aq) < 0\), we get
\[
ab^2 - a^2 pq - b^2 pq + ab^2 < 0.
\]

Then, \( ab(p^2+q^2) < (a^2 + b^2) pq \). By adding \(2abpq\) in both sides, we have \( ab(p+q)^2 < (a+b)^2 pq \). So we get
\[
(p+q) < \frac{(a+b)/\sqrt{ab}}{\sqrt{N}}.
\]

Since \( \phi(N) = N+1 - (p+q) \), we have
\[
\phi(N) > N+1 - \frac{a+b}{\sqrt{ab}} \sqrt{N}.
\]

**Proposition 2.**
Because a and b are less than \( \log N \), we further assume that \( \log N \) is an integer. We thus have

\[
\frac{e}{N - \frac{a + b}{\sqrt{ab}} N + 1} - \frac{k}{d} < \frac{e^{\frac{N^2}{3}}}{\phi(N) N - \frac{a + b}{\sqrt{ab}} N + 1} + \frac{1}{d \phi(N)}
\]

\[
< \frac{e^{\frac{N^2}{3}}}{\phi(N) N - \frac{a + b}{\sqrt{ab}} N + 1} + \frac{1}{d \phi(N)}
\]

Because \( a \) and \( b \) are less than \( \log N \), we further assume that

\[
N - \frac{a + b}{\sqrt{ab}} N + 1 > \frac{3\sqrt{ab}}{(a + b)^2} N, \quad \phi(N) > \frac{3}{4} N \quad \text{and} \quad N > 8d.
\]

We thus have

\[
\frac{e}{N - \frac{a + b}{\sqrt{ab}} N + 1} - \frac{k}{d} < \frac{N^2}{3N N} + \frac{1}{d \phi(N)}
\]

\[
< \frac{N^2}{3} + \frac{1}{6d^2}.
\]

Let \( d < N^{\frac{3}{10}} \). We get

\[
\frac{e}{N - \frac{a + b}{\sqrt{ab}} N + 1} - \frac{k}{d} < \frac{1}{2d^2}
\]

which satisfies Legendre’s theorem. We have showed that \( d < N^{\frac{3}{10}} \) can be discovered from the convergents of

\[
\frac{e}{N - \frac{a + b}{\sqrt{ab}} N + 1}.
\]

According to Theorem 1, we design the following algorithm to discover the secret exponent \( d \).

**Algorithm 1.**

Input: the RSA public key \( (e, N) \)

Output: the secret exponent \( d \)

Step 1. Choose two coprime positive integers \( a \) and \( b \) which are less than \( \log N \). (We can use the Stern-Brocot tree [4] to generate \( a \) and \( b \).)

Step 2. Compute convergents of \( \frac{e}{N - \frac{a + b}{\sqrt{ab}} N + 1} \).

Step 3. For each convergent \( \frac{r}{s} \), solve the equation

\[
x^2 - (N + 1 - \frac{e}{s} - \frac{1}{s^2}) x + N = 0.
\]

If its roots are positive integers less than \( N \), then return the secret exponent \( s \).

Step 4. Return (Failure).

For the sake of clarity, as shown in Table 1, we can recover the secret exponent \( d = 13049 \) using the continued fraction of \( \frac{e}{N - \frac{a + b}{\sqrt{ab}} N + 1} \), where \( e = 61198413967689 \), \( N = 95764272829453 \), \( a = 3 \) and \( b = 2 \). It is worth noting that three presented methods [6, 12, 13] are in vain because \( d \) cannot be discovered from the convergents of \( \frac{e}{N} \) (Wiener’s method), \( \frac{e}{N - a + b \sqrt{N} + 1} \) (de Weger’s method), or \( \frac{e}{N - \frac{3}{\sqrt{2}} \sqrt{N} + 1} \) (Maitra and Sarkar’s method).

<table>
<thead>
<tr>
<th>Calculated Quantity</th>
<th>How It is Derived</th>
<th>( i = 0 )</th>
<th>( i &gt; 0 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a_i )</td>
<td>continued fraction of ( \frac{e}{N - \frac{a + b}{\sqrt{ab}} \sqrt{N} + 1} )</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( s_i )</td>
<td>([a_0, a_1, \ldots, a_n])</td>
<td>0</td>
<td>...</td>
</tr>
<tr>
<td>( s_i )</td>
<td>See [10]</td>
<td>0</td>
<td>...</td>
</tr>
<tr>
<td>( N = 95764272829453 \times 3 )</td>
<td>13049</td>
<td>13049</td>
<td></td>
</tr>
</tbody>
</table>

\( e^2 - 20057614 x + 95764272829453 = 0 \)

\( N = (7815021 \times 1222359) + 65764272829453 \), \( e = 61198413967689 \), \( a = 3 \) \( b = 2 \)
IV. DISCUSSION

In this section, we compare our method with de Weger’s method and Maitra and Sarkar’s method. If \( a = b = 1 \), we have

\[
(b(a^2 + 1)p - a(b^2 + 1)q)(ap - bq) = (2p - 2q)(p - q) = 2(p - q)^2 > 0.
\]

Our method can discover \( d < N^{\frac{3}{2}} \) from the convergents of \( \frac{e}{N - 2\sqrt{N} + 1} \). Obviously, de Weger’s method and ours has the same result. When \( \frac{b}{a} = \frac{1}{2} \), we get

\[
(b(a^2 + 1)p - a(b^2 + 1)q)(ap - bq) = (5p - 4q)(2p - q).
\]

Because \( 2p - q > 0 \), we must set \( 5p - 4q > 0 \). Thus, the inequality \( p > \frac{2j + 2}{4j + 1}q \) in [6] is satisfied for \( j \geq 1 \). The main difference between Maitra and Sarkar’s method and ours is the estimated value of \( N - \frac{3}{2} \sqrt{N} + 1 \). In Maitra and Sarkar’s method, they assume that \( N - \frac{3}{2} \sqrt{N} + 1 > \frac{3}{4} N \).

We assume that \( N - \frac{3}{2} \sqrt{N} + 1 > \frac{3}{4} \sqrt{2} N \). In fact, our assumption is verified if \( N > 60 \). Therefore, Maitra and Sarkar’s method can use our assumption to get that \( d < N^{\frac{3}{2}} \) is discovered from the convergents of \( \frac{e}{N - \frac{3}{2} \sqrt{N} + 1} \)

\[
|2p - q| = N^\frac{1}{2}.
\]

Obviously, Maitra and Sarkar’s method and ours has the same result if \( \frac{b}{a} = \frac{1}{2} \).

V. CONCLUSIONS

This paper aims at extending de Weger’s method if the ratio of two RSA primes \( \frac{p}{q} \) is close to a simple fraction \( \frac{b}{a} \). Based on our assumption \( (b(a^2 + 1)p - a(b^2 + 1)q)(ap - bq) > 0 \), we have showed that \( d < N^{\frac{3}{2}} \) can be discovered from the convergents of \( \frac{e}{N - \frac{a + b}{\sqrt{ab}} \sqrt{N} + 1} \) for \( \frac{|ap - bq|}{N} = N^\frac{1}{2} \). If \( a = b = 1 \), our method can discover \( d < N^{\frac{3}{2}} \) from the convergents of \( \frac{e}{N - 2\sqrt{N} + 1} \) for \( \frac{|p - q|}{N} = N^\frac{1}{2} \). The de Weger method has the same result. When \( \frac{b}{a} = \frac{1}{2} \), our method can discover \( d < N^{\frac{3}{2}} \) from the convergents of \( \frac{e}{N - \frac{3}{2} \sqrt{N} + 1} \) for \( \frac{|p - q|}{N} = N^\frac{1}{2} \). The same result will be found in Maitra and Sarkar’s method.

ACKNOWLEDGMENT

This research was supported partially by the National Science Council of the Republic of China under grant NSC 97-2221-E-390-012.

REFERENCES