On the Extension of Wiener Attack on RSA with Short Secret-Exponents

Hung-Min Sun[1], Mu-En Wu[2] and Shiuan-Tung Chen[3]
Department of Computer Science
National Tsing Hua University, Hsinchu, Taiwan 300[1,2,3]
hmsun[1]@cs.nthu.edu.tw; {mn[2]; rickrick[3]}@is.cs.nthu.edu.tw

***Abstract*— *In* 1999*, Wiener took advantage of continued fraction technique to attack short secret-exponent RSA, which is called the Wiener attack. This attack is the first proof to show that we can not choose too short secret-exponent* d *when using RSA. The secret-exponent* d *should be chosen larger than* $N^{0.25}$*. After then, in* 1997*, Verheul and Tilborg proposed an extension of the Wiener attack which can work well over Wiener's boundary. Suppose* $r = \log(d/N^{0.25})$*, their technique costs an exhaustive search for* $2r+8$ *bits in order to attack* d *which is smaller than* $N^{0.25}2^r$*. In this paper, we provide a simpler method to demonstrate a result which is similar to Verheul and Tilborg's . With our method it only costs an exhaustive search for* $2r + 2$ *bits, which is* 6*-bit fewer than Verheul and Tilborg's* $2r + 8$ **bits**

1: INTRODUCTIONS

Since 1978, RSA [8] is the most popular cryptosystem in the world. It is not only built into several operating systems, like Microsoft, Apple, Sun, and Novell, but is also used for securing web traffic, E-mail, smart cards or IC cards. The security of RSA is based on the hardness of factoring problem. Generally we apply 1024-bit RSA modulus to archive the goal of factoring-infeasible, but such large modulus also causes the inefficient in encryption and decryption of RSA. The encryption and decryption in RSA require taking heavy exponential multiplications modulus of a large integer N which is the product of two large primes p and q. Without loss of generality, we assume N is of 1024 bits, and p and q are of 512 bits. Since the RSA encryption and decryption time are roughly proportional to the number of bits in public and secret exponents respectively, many practical issues have been considered when implementing RSA such as how to reduce the encryption time (or signature-verification time), how to reduce the decryption time (or signature-generation time) [9][10].

To reduce the encryption time (or the signature-verification time), one may wish to use a small public-exponent e. The smallest possible value for e is 3, however, it has been proven to be insecure against some small public-exponent attacks [6]. A more widely accepted and used public-exponent is $e = 2^{16} + 1 = 65537$. On the other hand, to reduce the decryption time (or the signature-generation time), one may also wish to use a short secret-exponent d. However, the use of short secret-exponent encounters a more serious security problem due to some powerful short secret-exponent attacks [12][11][2][5]. One of the most famous attacks on short secret-exponent RSA, which is called the Wiener attack, was proposed by Wiener [12] in 1990. He showed that choosing too short secret-exponent is insecure by taking advantage of continue fraction technique. Thus the Wiener attack is also called the continued fraction attack. Indeed, instances of RSA with secret-exponent $d < N^{0.25}$ can be efficiently broken by the Wiener attack. This result had been improved by Boneh & Durfee [2] in 1998. They took advantage of lattice reduction technique and showed that instance of RSA with $d < N^{0.292}$ should be considered insecure. Although their method is heuristic, the experiments demonstrate the effectiveness of the attack.

In 1997, Verheul and Tilborg [11] extend the boundary of the Wiener attack. They showed that there is still some information available for larger value of d. Suppose d is larger than $N^{0.25}$ and smaller than $N^{0.25}2^r$, where $r = \log(d/N^{0.25})$. Their method requires to do an exhaustive search for about $2r + 8$ bits while after applying the Wiener attack. Consider the currently computational ability, suppose we can process complexity up to 2^{64}. This implies Verheul and Tilborg's technique can extend Wiener's boundary up to 28 bits.

In this paper, we improve Verheul and Tilborg's result to the case of doing exhaustive search for about $2r + 2$ bits by a simpler way. With our method, we reduce 6 bits exhaustive search while compared with Verheul and Tilborg's result, *i.e.* $2r + 8$ bits. Thus our method is more efficient in extracting the secret-exponent d while $d < N^{0.25}2^r$.

The remainder of this paper is organized as follows: In Section 2, we briefly review some basic results we will use in this paper, includes continued fraction, the Wiener attack and so on. In section 3, we introduce the technique of Verheul and Tilborg's extension. Next, we show our result similar to Verheul and Tilborg's result in Section 4. Finally, we have a conclusion and provide some future work.

2: PRELIMINARY

2.1. Continued Fractions

We review the definition of the continued fraction and a theorem we will use later in the paper. The detail of the theorem can be referenced in [7].

Definition 1: For any two positive integers a and b, with $a < b$ and $\gcd(a, b) = 1$, the rational number can be represented as the following form:

$$\frac{a}{b} = \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_n}}}$$

for some index n, where a_i's are positive integers. We write $\frac{a}{b} = (a_1, a_2, ..., a_n)$ for simplicity. Besides, we call $(a_1, a_2, ..., a_i)$ the i'th convergent of the continued fraction expansion of $\frac{a}{b}$.

Theorem 2: Suppose $\frac{a}{b}$ is a rational number with postive integers a and b and $\gcd(a, b) = 1$, where $a < b$. Suppose there are two unknown co-prime integers x and y satisfying

$$\left|\frac{a}{b} - \frac{x}{y}\right| < \frac{1}{2y^2}$$

, then $\frac{x}{y}$ equals one of the convergents of the contiued fraction expression of $\frac{a}{b}$.

2.2. The Wiener attack

In 1990, Wiener [12] observed that RSA equation $ed = k\varphi(N) + 1$ can be rewritten as the form:

$$\left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| = \left|\frac{1}{d\varphi(N)}\right|. \quad (1)$$

He replaced $\frac{e}{\varphi(N)}$ in (1) with $\frac{e}{N}$ and considered the following inequality:

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}. \quad (2)$$

Note that if the inequality (2) holds, then $\frac{k}{d}$ equals one of the convergents of the continued fraction expression of $\frac{e}{N}$ according to Theorem 2. Since $\gcd(k, d) = 1$, we can actually extract out the values of d and k. Thus we have to find the sufficient condition to satisfy (2). Since $N^{1/2} \approx p \approx q$ and $d \approx k$. We have

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \frac{Nk - ed}{Nd} = \frac{k(p + q - 1) - 1}{Nd} \approx \frac{1}{N^{1/2}}. \quad (3)$$

From (3), we have to set $\frac{1}{N^{1/2}} < \frac{1}{2d^2}$ and this leads to the condition: $d < \frac{1}{3}N^{0.25}$ to achieve the sufficient condition of Theorem 1 to satisfy the condition of (2). To summarize, ignoring the small constant $\frac{1}{3}$ we usually set the boundary of the Wiener attack: $d > N^{0.25}$ to defend the continued fraction attack. However, what can we do if the secret-exponent exceeds $N^{0.25}$ slightly? In 1997, Verheul and Tilborg [11] solved this problem. They provide a technique to slightly extend Wiener's boundary. We will show their technique in Section 3.

2.3. Weger's idea

Recently, Weger [13] showed that choosing an RSA modulus with a small difference of its prime factors yields improvements on the small private exponent attacks, such as Wiener [12] and Bobeh-Durfee attack [2]. The main idea is adding one more variable $\Delta = |p - q|$ into these attacking-formula deductions. Under his consideration, he use more suitable estimate of $\varphi(N)$, that is $N + 1 - 2N^{1/2}$ rather than N. Thus the smaller the Δ is, the closer between $\varphi(N)$ and $N + 1 - 2N^{1/2}$ are. In thie paper, we follow Weger's idea to take $N + 1 - 2N^{1/2}$ to estimate $\varphi(N)$ rather than N.

3: VERHEUL AND TILBORG'S EXTENSION ON THE WIENER ATTACK

The extension of the Wiener attack was proposed by Verheul and Van Tilborg [11]. When $d > N^{0.25}$, their attack needs to do an exhaustive search of about $2r + 8$ bits, where $r = \log\left(d/N^{0.25}\right)$. We simply describe their technique in the following.

From RSA equation: $ed = 1 + k(p - 1)(q - 1)$, we know $ed \equiv 1 \bmod (\mathrm{lcm}(p - 1, q - 1))$. Thus there exists an integer K such that $ed = 1 + K(\mathrm{lcm}(p - 1, q - 1))$. Now we set $G = \gcd(p - 1, q - 1)$, then $ed = 1 + K\frac{(p-1)(q-1)}{G}$. After dividing two sides by dpq we get

$$\begin{aligned} \frac{e}{pq} &= \frac{1}{dpq} + K\frac{(p-1)(q-1)}{Gdpq} \\ &= \frac{1}{dpq} + \frac{K}{dG}\frac{pq-p-q+1}{pq} \\ &= \frac{K}{dG}(1 - \delta) \end{aligned}$$

, where $\delta = \frac{p+q-1-\frac{G}{K}}{pq}$.

Let $\frac{k}{g} = \frac{K}{G}$ and $\gcd(k, g) = 1$ then $\frac{e}{pq} = \frac{k}{dg}(1 - \delta)$.

We briefly review some properties of continued fractions as a result of the extension is established on them. First we define the following notations:

Notation 3:

$$\begin{aligned} x &= \langle a_0, a_1, \ldots, a_{m-1}, a_m\rangle \\ x_i &= \frac{p_i}{q_i} = \langle a_0, a_1, \ldots, a_i\rangle \\ y &= \langle b_0, b_1, \ldots, b_{n-1}, b_n\rangle \\ y_i &= \frac{u_i}{v_i} = \langle b_0, b_1, \ldots, b_i\rangle \end{aligned}$$

The basic property of continued fractoin satisfies the following relations. It is not hard to prove these relations by induction [7].

$$\begin{aligned} (-1)^i &= p_{i-1}q_i - p_iq_{i-1}, \\ p_0 &= a_0;\ q_0 = 1, \\ p_1 &= a_1a_0 + 1;\ q_1 = a_1, \\ p_i &= a_ip_{i-1} + p_{i-2}, \text{ where } i \geq 2, \\ q_i &= a_iq_{i-1} + q_{i-2}, \text{ where} i \geq 2. \end{aligned}$$

Proposition 4: Define $A\langle i + 1\rangle = \langle a_{i+1}, a_{i+2}, \ldots, a_m\rangle$. For all i such that $2 \leq i < m$, we have the following property

$$x = \frac{p_m}{q_m} = \frac{\left(a_i + \frac{1}{A(i+1)}\right)p_{i-1} + p_{i-2}}{\left(a_i + \frac{1}{A(i+1)}\right)q_{i-1} + q_{i-2}}$$

Theorem 5: Let $x < y$ and u be an upper bound of $|y - x|$. Suppose j is the largest odd number in $\{1, \ldots, m\}$ satisfying the inequality $|y - x| \leq u \leq |x_j - x|$. Then either $x_j = y$ or all partial quotients and convergents of x and y coincide up to j. Moreover, if q_j denotes the denominator of the j-th convergent of x, then the largest odd number j in $\{1, \ldots, m\}$, such that $q_j \leq \frac{1}{u_j}$ is a lower bound of j.

Lemma 6: Suppose $0 < x < y$, and let δ be a number such that $x = (1 - \delta)y$. Let $\delta_{\max}(\delta_{\min})$ be an upper bound (non-negative lower bound) of δ, then $|y - x| \leq \frac{\delta_{\max}}{1-\delta_{\min}}x$. Also, if $y \leq 1$, then $|y - x| \leq \delta_{\max}$.

Afterward we want to estimate $\delta_{\max}$ and $\delta_{\min}$. Without loss of generality we assume that $p < q$. Then

$$\begin{aligned}\delta &= \frac{p+q-1-G/K}{pq} \cong \frac{p+q}{n} \\ &\geq \frac{\sqrt{2pq}}{n} = \frac{\sqrt{2}}{\sqrt{n}}\end{aligned}$$

and

$$\begin{aligned}\delta &= \frac{p+q-1-G/K}{pq} \\ &\leq \frac{2q}{pq} = \frac{2}{p} \approx \frac{4}{\sqrt{n}}\end{aligned}$$

By above lemma we can estimate the boundary of u. Note that u satisfies $|y-x| \leq u \leq |x_j - x|$.

Writing $x = e/pq$ with CF-representation $< a_0, a_1, \ldots, a_m >$ and successive convergents $x_i = p_i/q_i$ and $y = k/dg$ with CF-representation $< b_0, b_1, \ldots, b_n >$. Suppose the index j has the same meaning mentioned above, that is the largest odd number in $\{1, \ldots, m\}$ satisfying the inequality $|y-x| \leq u \leq |x_j - x|$. Since $x < y$, it follows that $a_{j+1} \leq b_{j+1}$. We suppose $b_{j+1} = a_{j+1} + \Delta$. Further, let $B(j+2)$ denote $\langle b_{j+2}, \ldots, b_n \rangle$ and write $B(j+2) = U/V$ with $\gcd(U,V) = 1$. Note that $U \geq V$. Combining above notations we have

$$b_{j+1} + \frac{1}{B(j+2)} = a_{j+1} + \Delta + \frac{V}{U}.$$

>From Proposition 4 and the equalities of the convergents up to j, we have the following proposition:

$$\begin{aligned}\frac{k}{dg} &= \frac{\left(a_{j+1}+\Delta+\frac{V}{U}\right)p_j + p_{j-1}}{\left(a_{j+1}+\Delta+\frac{V}{U}\right)q_j + q_{j-1}} \\ &= \frac{(a_{j+1}p_j + p_{j-1}) + \left(\Delta+\frac{V}{U}\right)p_j}{(a_{j+1}q_j + q_{j-1}) + \left(\Delta+\frac{V}{U}\right)q_j} \\ &= \frac{p_{j+1} + \left(\Delta+\frac{V}{U}\right)p_j}{q_{j+1} + \left(\Delta+\frac{V}{U}\right)q_j} \\ &= \frac{p_{j+1}U + (U\Delta+V)p_j}{q_{j+1}U + (U\Delta+V)q_j}\end{aligned}$$

We claim that the numerator, denoted by N, and the denominator, denoted by D, of the right hand side of this equality are relatively prime, so $N = k$ and $D = dg$. Using the estimate $u = \frac{4}{\sqrt{n}}$ be upper bound of $|y-x|$. By definition of j, we know $|x_{j+2} - x| < \frac{4}{\sqrt{n}}$. On the other hand, writing $A(j+3) = \langle a_{j+3}, \ldots, a_n \rangle$, and thus having $a_{j+3} \leq A(j+3) \leq a_{j+3} + 1$. Thus we have

$$\begin{aligned}|x - x_{j+2}| &= \left|\frac{A(j+3)p_{j+2} + p_{j+1}}{A(j+3)q_{j+2} + q_{j+1}} - \frac{p_{j+2}}{q_{j+2}}\right| \\ &= \left|\frac{p_{j+1}q_{j+2} - p_{j+2}q_{j+1}}{q_{j+2}(A(j+3)q_{j+2} + q_{j+1})}\right| \\ &= \left|\frac{1}{q_{j+2}(A(j+3)q_{j+2} + q_{j+1})}\right| \\ &\geq \left|\frac{1}{q_{j+2}((a_{j+3}+1)q_{j+2} + q_{j+1})}\right|.\end{aligned}$$

In [4], the distribution of the partial quotients a_i of a random real $x = \langle a_0, a_1, \ldots, a_n \rangle$ is given. Approximately a_i will be 1 with probability 41.5%, a_i will be 2 with probability 17%, etc. Since $q_{j+2} = a_{j+2}q_{j+1} + q_j$ we can estimate $q_{j+2} = 2q_{j+1}$. And from

$$|x - x_{j+2}| \geq \left|\frac{1}{q_{j+2}\left(\left(a_{j+3}+1\right)q_{j+2} + q_{j+1}\right)}\right|$$

, we get $\frac{4}{\sqrt{n}} > |x - x_{j+2}| \geq \frac{1}{10q_{j+1}^2}$. Then we conclude that

$$q_{j+1} > \frac{1}{7}N^{0.25} > \frac{1}{2^3}N^{0.25}.$$

Finally, since g is small and very likely be 1 or 2, the number of bits of dg is that of d plus one. To estimate the complexity of our method for $d > N^{0.25}$, we define $\log d = \log N^{0.25} + r$. Now we can derive $ln_2 N^{0.25} - 3 + \log U \leq \log N^{0.25} + r + 1$ from taking log to two side of $q_{j+1}U \leq dg$. And then $\log U \leq r + 4$. Since $V \leq U$, the same inequality applies to V, that is $\log V \leq r + 4$. Now because the value of Δ is small in general, from

$$\frac{k}{dg} = \frac{p_{j+1}U + (U\Delta + V)p_j}{q_{j+1}U + (U\Delta + V)q_j}$$

we conclude the uncertainty of $\frac{k}{dg}$ is about $2r + 8$ bits. So we just need to do an exhaustive search for about $2r + 8$ bits to find the correct value of $\frac{k}{dg}$.

In this paper, we proposed another look of Verheul and Tilborg's improvement. In our method we only need to do an exhaustive search of about $2r + 2$ bits, where $r = \log\left(d/N^{0.25}\right)$.

4: ANOTHER LOOK ON VERHEUL AND TILBORG'S IMPROVEMENT

4.1. Improvement of the Wiener attack

Take the idea of estimate of $p+q$ proposed by Weger [13], in the remainder of this paper we use $N+1-2N^{1/2}$ to denote our estimate of $\varphi(N)$. That is

$$\varphi(N) \approx N + 1 - 2N^{1/2}.$$

First, we prove if we use $N + 1 - 2N^{1/2}$ instead of N to estimate $\varphi(N)$ on the Wiener attack, then the range of vulnerable secret-exponent d will be more widespread. Note that the sufficient condition that the Wiener attack can work is

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}. \tag{4}$$

Besides, from RSA equation: $ed = k(p-1)(q-1) + 1$ we have

$$\left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| = \frac{1}{\varphi(N)d}.$$

It is not difficult to prove that $\left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| < \frac{1}{2d^2}$, thus the Wiener attack can succeed if we know the exact value of $\varphi(N)$. This observation also point out if we use more suitable estimation of $\varphi(N)$ instead of original N, then the range of vulnerable secret-exponent will be more widespread. Also, Weger's result [13]provides the same point and thus he considers the variable $\Delta = |p-q|$ to his attack. Note that the smaller the Δ is, the closer between $2N^{1/2}$ and $p+q$ are.

Now we replace N in (4) by $N+1-2N^{1/2}$. The new sufficient condition that Continued-Fraction Theorem (Theorem 1) can work is

$$\left|\frac{e}{N+1-2N^{1/2}}-\frac{k}{d}\right|<\frac{1}{2d^2}.$$

Here we show how much extension of vulnerable secret-exponent if we use the better estimation $N+1-2N^{1/2}$ to estimate$\varphi(N)$ rather than N. Our question can be presented in the following:

Question:

Consider the RSA equation: $ed=k(p-1)(q-1)+1$, what range of d does it satisfy the following conditions?

$$\left|\frac{e}{N}-\frac{k}{d}\right|>\frac{1}{2d^2} \text{ and } \left|\frac{e}{N+1-2N^{1/2}}-\frac{k}{d}\right|<\frac{1}{2d^2}. \quad (5)$$

The left inequality above is the sufficient condition that the Wiener attack fails and the right inequality is the sufficient condition that Theorem 1 can apply to work. Now we simplify two inequalities in (5):

>From $\left|\frac{e}{N}-\frac{k}{d}\right|>\frac{1}{2d^2}$ we get $\frac{kN-[k(N-p-q+1)+1]}{Nd}>\frac{1}{2d^2}$, which is equivalent to

$$2dk[(p+q)-1]-2d>N. \quad (6)$$

Similarly, from the right inequality in (5) we get $\frac{k\left(N+1-2N^{1/2}\right)-[k(N-p-q+1)+1]}{d\left(N+1-2N^{1/2}\right)}<\frac{1}{2d^2}$, which is equivalent to

$$2dk[(p+q)-2N^{1/2}]-2d<N+1-2N^{1/2}. \quad (7)$$

Combine (6) and (7), we have the following equivalent conditions of (5):

$$N+2d<2dk[(p+q)-1]<N+(2dk-1)(2N^{1/2}-1)+2d. \quad (8)$$

From (5) we know the better estimation of $\varphi(N)$ actually allows the widespared range of vulnerable secret-exponent d. Even though in the representation of power of N the boundaries are both $N^{0.25}$.

4.2 Another Proof for Verheul and Tilborg's Extension

In this section we provide another proof to show Verheul and Tilborg's result [11]. That is: for $r=\log\left(d/N^{0.25}\right)$, Verheul and Tilborg's technique has to do an exhaustive search for $2r+8$ bits to extract out the secret-exponent d. Our method need to do an exhaustive search for $2r+2$ bits, which is less 6 bits than Verheul and Tilborg's.

In (8), if we replace $N^{1/2}$ by $\frac{p+q}{2}$, the right side of formula (8) changes to

$$2dk(p+q-1)<2dk(p+q-1)+\varphi(N)+2d$$

, which is always hold for any secret-exponent d. Here we define another variable "Λ", where $\Lambda=\frac{p+q}{2}-N^{1/2}$ to denote the difference between $\frac{p+q}{2}$ and estimation $N^{1/2}$. Thus we have $N^{1/2}=\frac{p+q}{2}-\Lambda$. Applying "$N^{1/2}=\frac{p+q}{2}-\Lambda$" to the right side of inequality (8) we get

$$\begin{aligned} & 2dk(p+q-1) \\ < \;& N+(2dk-1)\left(2(\tfrac{p+q}{2}-\Lambda)-1\right)+2d \\ = \;& 2dk(p+q-1)+\varphi(N)-2\Lambda(2dk-1)+2d \end{aligned} \quad (9)$$

Therefore, we conclude (9) is equivalent to

$$2\Lambda(2dk-1)-d<\varphi(N). \quad (10)$$

Now we have a conclusion that the sufficient condition that Continued Fraction Theorem can work is to satisfy the inquuality (10). Note that we have to take $2N^{1/2}$ to replace $p+q$ in the case of estimation $\varphi(N)=(N+1)-(p+q)\approx(N+1)-2N^{1/2}$. However, if we do exhaustive search to find the most significant bits (MSBs) of Λ, then the estimation of $\varphi(N)$ will be more correct and the boundary of vulnerable secret-exponent d can be extended again.

Take 1024-bit RSA modulus N for example. Suppose we do exhaustive search to find s MSBs (most significant bit) of Λ defined in (10). Write $\Lambda=(2^{512-s})\Lambda_1+\Lambda_2$, where $\Lambda_1\in\left[2^{s-1},2^s\right]$, and $\Lambda_2\in\left[2^{511-s},2^{512-s}\right]$. With high probability Λ is about 512 bits due to $\Lambda=\frac{p+q}{2}-N^{1/2}$, which is a difference of two 512-bit numbers. Note that Λ_1 is known by exhaustive search and Λ_2 is still an unknown item. However, with such information Λ_1, $\varphi(N)$ can be estimated more correctly since $\frac{p+q}{2}\approx N^{1/2}+(2^{512-s})\Lambda_1$, which is also closer to $\frac{p+q}{2}$ than the original estimation $N^{1/2}$. Conclusively, we have the new estimation of $\varphi(N)$, that is

$$\varphi(N)\approx(N+1)-2[N^{1/2}+(2^{512-s})\Lambda_1]. \quad (11)$$

Now we take the new estimation of $\varphi(N)$ into (4) to replace N. That is,

$$\left|\frac{e}{(N+1)-2[N^{1/2}+(2^{512-s})\Lambda_1]}-\frac{k}{d}\right|<\frac{1}{2d^2} \quad (12)$$

Similar simplification of (12) like above, we have

$$\begin{aligned} & \left|\tfrac{e}{(N+1)-2[N^{1/2}+(2^{512-s})\Lambda_1]}-\tfrac{k}{d}\right| \\ = \;& \left|\tfrac{ed-k\left((N+1)-2[N^{1/2}+(2^{512-s})\Lambda_1]\right)}{d\left((N+1)-2[N^{1/2}+(2^{512-s})\Lambda_1]\right)}\right| \\ = \;& \tfrac{k(p+q)-k\left(2[N^{1/2}+(2^{512-s})\Lambda_1]\right)-1}{d\left((N+1)-2[N^{1/2}+(2^{512-s})\Lambda_1]\right)} \\ = \;& \tfrac{k(2\Lambda_2)-1}{d(\varphi(N)+2\Lambda_2)}<\tfrac{1}{2d^2} \end{aligned} \quad (13)$$

Thus the inequality in (10) is equivalent to

$$2d\left(k\left(2\Lambda_2\right)-1\right)<\varphi(N)+2\Lambda_2 \quad (14)$$

Rearranging (14) to the form of (10) we get

$$2\Lambda_2(2dk-1)-2d<\varphi(N). \quad (15)$$

Now, the quantity of Λ_2 is about $(512 - s)$ bits. In order to satisfy the inequality in (15), we know the bit-length of $2\Lambda_2(2dk - 1)$ in the left side of (15) is

$$1 + (512 - s) + 1 + |l_d| + |l_k|$$

which is mainly determined by $2\Lambda_2 \times 2dk$, where $|l_d|$ and $|l_k|$ means the bit-length of d and k respectively. Furthermore,the bit-length of $\varphi(N)$ is 1024. We have to set

$$1 + (512 - s) + 1 + |l_d| + |l_k| < 1024. \tag{16}$$

Note that we can assume $|l_d| = |l_k|$ because the bit-length of d and k are almost the same with high probability in the key-generation algorithm of RSA. Thus we suppose $|l_d| = |l_k| = 256 + r$. *i.e.*, the secret-exponent d exceeds 256 bits ($N^{0.25}$) more r bits. Applying to (15) we have

$$1 + (512 - s) + (1 + 2(256 + t)) < 1024$$

, which is equivalent to

$$2r + 2 < s. \tag{17}$$

With the above inequality of (17) we get a result that to extend the Wiener's boundary r bits, we only have to do an exhaustive search for about $2r + 2$ bits, where $r = \log\left(d/N^{0.25}\right)$. Compared with Verheul and Tilborg's result [11], which costs an exhaustive search for $2r + 8$ bits, our result is 6 bits fewer than Verheul and Tilborg's. Thus it is more efficient to applying our method on the extension of the Wiener attack to extract the secret-exponent.

Take the current computational ability for example, we suppose the complexity that the current computer can work is 2^{64}, that means we can brute search for any number whose bit-length less than 64. Apply $2r+8 = 64$ to Verheul and Tilborg's result, we get $r = \frac{64-8}{2} = 28$ bits.This means the secret-exponent should be chosen larger than $\left(\log N^{0.25}\right) + 28$ bits. But with our result: $2r + 2 = 64$, we extend $r = \frac{64-2}{2} = 31$ bits, which is more 3 bits than the 28 bits. Therefore we claim our extension method is better than Verheul and Tilborg's.

5: CONCLUSION AND FUTURE WORK

In this paper we propose a method to mutually prove Verheul and Tilborg's improvement on the extension of the Wiener attack. Our method costs only an exhaustive search for about $2r + 2$ bits , which is 6 bits fewer than Verheul and Tilborg's result, *i.e.*, $2r + 8$ bits.

An open problem has been mentioned many times in the past research. Whether exists a better method to estimate the value of $\varphi(N)$? Currently we usually use $N + 1 - 2N^{1/2}$ to estimate $\varphi(N)$ roughly. If we can estimate $\varphi(N)$ more correctly, then the boundary of the Wiener attack will be raised again.

Acknowledgements:

The authors wish to acknowledge the anonymous reviewers for valuable comments. This research was supported in part by the MOEA research project under grant no. 95-EC-17-A-04-S1-044.

REFERENCES

[1] D. Boneh, "Twenty Years Attacks on the RSA Cryptosystem," Notices of the American Mathematical Society, vol. 46:2, pp. 203-213, 1999.

[2] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," IEEE Trans. on Information, Vol. 46(4), pp. 1339-1349, 2000.

[3] D. Boneh and H. Shacham, "Fast Variants of RSA," CryptoBytes, 2002, Vol. 5, No. 1, Springer, 2002.

[4] Knuth. D, The art of computer programming, Vol. 2, Seminumerical algorithms. 2nd edn, New York: Addison-Wesley 1981.

[5] G. Durfee, P. Q. Nguyen, "Cryptanalysis of the RSA Schemes with Short secret-exponent form Asiacrypt '99," Advances in Cryptology-Asiacrypt'00, LNCS 1976, Springer-Verlag, pp.1-11, 2000.

[6] J. Hastad, "Solving simultaneous modular equations of low degree", SIAM J. of Computing, Vol. 17, pp.336-341, 1988.

[7] I. Niven, H. S. Zuckerman, An Introduction to the Theory of Number, John Wiley and Sons Inc,1991.

[8] R. Rivest, A. Shamir and L. Aldeman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM , vol. 21, No.2, pp.120-126, 1978.

[9] H.-M. Sun, W.-C. Yang and C.-S. Laih, "On the Design of RSA with Short secret-exponent," Advances in Cryptology-ASIACRYPT'99, LNCS 1716, pp.150-164, 1999.

[10] H.-M. Sun and C.-T. Yang, "RSA with Balanced Short Exponents and Its Application to Entity Authentication," Public Key Cryptography 05, LNCS 386, pp.199-215, 2005.

[11] E. Verheul and H. van Tilborg, "Cryptanalysis of less short RSA secret-exponents," Applicable Algebra in Engineering, Communication and Computing, vol. 8, Springer-Verlag, pp. 425-435, 1997.

[12] M. J. Wiener, "Cryptanalysis of RSA with short secret-exponents," IEEE Transactions on information Theory,Vol. 36, pp.553-558, 1990.

[13] B. de Weger, "Cryptanalysis of RSA with small prime difference", Applicable Algebra in Engineering, Communication and Computing, Vol. 13, pp. 17-28, 2002.