Cryptanalysis of Short Secret Exponent and Large Public Exponent of RSA

Chien-Yuan Chen
Department of Information Engineering,
Kaohsiung Polytechnic Institute, Tahsu, Kaohsiung, Taiwan 840, R.O.C.
E-mail: cyChen@csa500.kpi.edu.tw
Chin-Chen Chang
Institute of Computer Science and Information Engineering,
National Chung Cheng University, Chiayi, Taiwan 621, R.O.C.
E-mail: ccc@cs.ccu.edu.tw
Wei-Pang Yang
Department of Computer and Information Science,
National Chiao Tung University, Hsinchu, Taiwan 300, R.O.C.

Abstract

Wiener proved that in RSA, the secret exponent d can be discovered if $d < N^{1/4}$ *and* $N^{3/4} < e < N$, *where e is the public exponent and N is the modulus. However, he also presented an open problem that whether there exists an attack on RSA when d is short and* $e > N$. *In this paper, we improve Wiener's method to solve the case that* $d < N^{1/4}$ *and* $N^{7/4} < e < N^2$. *Furthermore, we show that the secret exponent d can be easily recovered when* $d < \frac{N^{1/4}}{(3t)^{1/2}}$ *and* $N^{t-1/4} < e < N^t$, *where t is a small integer.*

Keywords: RSA , continued fraction

1. Introduction

Since RSA was presented by Rivest et al. [6], many various attacks on it have been made. Though no attack can completely crack RSA, there are many restrictions on prime factors p, q, the public exponent e, and the secret exponent d of RSA. [3, 5, 8] An interesting one on RSA, which was developed by Wiener [7], resulted in a restriction on the secret exponent d. Wiener's attack, using the continued fraction, can recover the secret exponent d on the condition that $d < N^{1/4}$ and $N^{3/4} < e < N$. However, when $e > N$, Wiener's attack is in vain even if d is short. It is not surprising, therefore, that it is acceptable to choose small secret exponent for reducing the computation required from smart card in server-aided computation scheme. [2]

In this paper, we improve Wiener's method such that the secret exponent d can be recovered if $d < N^{1/4}$ and $N^{7/4} < e < N^2$. Furthermore, when $d < \frac{N^{1/4}}{(3t)^{1/2}}$ and $N^{t-1/4} < e < N^t$, where t is a small integer, the secret exponent d can also be found.

This paper is organized as follows. In Section 2, we review Wiener's method. Section 3 describes our proposed scheme. The last section gives some discussions and conclusions.

2. Wiener's method

According to the RSA system, the public exponent e and the secret exponent d have the following relationship

$$ed \equiv 1 \pmod{l.c.m.(p-1, q-1)}, \qquad (2.1)$$

where *l.c.m.* (a, b) means the least common multiple of a and b. There must exist an integer K such that

$$ed = K\, l.c.m.(p-1, q-1) + 1. \qquad (2.2)$$

Equation (2.2) can be rewritten as

$$ed = \frac{K}{G}(p-1, q-1) + 1 \qquad (2.3)$$

$$= \frac{k}{g}(p-1, q-1) + 1, \qquad (2.4)$$

where $G = g.c.d.(p-1, q-1)$, $\frac{K}{G} = \frac{k}{g}$ and $g.c.d.(k, g) = 1$. Here *g.c.d.* (a, b) denotes the greatest common divisor of a and b. Dividing both sides of Equation (2.4) by dpq, we have

$$\frac{e}{pq} = \frac{k}{dg}\left(\frac{(p-1)(q-1)}{pq}\right) + \frac{1}{dpq}$$

$$= \frac{k}{dg}\left(1 - \frac{p+q-1-\frac{g}{k}}{pq}\right)$$

$$= \frac{k}{dg}(1 - \delta), \text{ where } \delta = \frac{p+q-1-\frac{g}{k}}{pq}. \quad (2.5)$$

Since $(1+\frac{k}{g})$ is far smaller than pq, we know $\delta \approx \frac{p+q}{pq}$. Assume that $\frac{e}{pq}$ has a continued fraction form $a_0 + \cfrac{1}{a_1 + \cfrac{1}{\dots + \cfrac{1}{a_n}}}$, where a_i is a positive integer, $0 \le i \le n$. For simplicity, the above continued fraction can be represented as the notation $[a_0; a_1, \dots, a_n]$. On the other hand, given the continued fraction $[a_0; a_1, \dots, a_n]$, we can reconstruct $\frac{e}{pq}$ to be $\frac{r_n}{s_n}$ by recursively computing r_i and s_i by

$$r_0 = a_0,\ s_0 = 1,$$
$$r_1 = a_0a_1 + 1,\ s_1 = a_1, \text{ and}$$
$$r_i = a_ir_{i-1} + r_{i-2},\quad s_i = a_is_{i-1} + s_{i-2},$$
$$\text{for } i = 2, 3, \dots, n. \quad (2.6)$$

Let $[a_0; a_1, \dots, a_i]$ be the ith convergent of the continued fraction $[a_0; a_1, \dots, a_n]$. It can be easily seen that

$$\frac{e}{pq} < [a_0; a_1, \dots, a_i], \text{ if i is odd,}$$

$$[a_0; a_1, \dots, a_i] < \frac{e}{pq} < [a_0; a_1, \dots, a_i+1],$$
if i is even.

Because $\frac{k}{dg} > \frac{e}{pq}$, which is resulted from Equation (2.5), $\frac{k}{dg}$ can be probably found by using Equation (2.6) to construct the rational number $\frac{r}{s}$ which is equal to

$$[a_0; a_1, \dots, a_i+1], \text{ if i is even, and}$$
$$[a_0; a_1, \dots, a_i], \text{ if i is odd.} \quad (2.7)$$

According to [7], the constructed number $\frac{r}{s}$ can be equal to $\frac{k}{dg}$ if

$$kdg \le \frac{1}{\frac{3}{2}\delta} \quad (2.8)$$

As soon as we guess a certain rational number $\frac{r}{s}$, we have to check whether or not $\frac{r}{s}$ is equivalent to $\frac{k}{dg}$. For simplicity, assume that ed > pq. Consequently, from Equation (2.4), we have k > g. Next, multiplying both sides of Equation (2.4) by g, we have

$$edg = k(p - 1)(q - 1) + g. \quad (2.9)$$

Therefore, we can obtain (p - 1)(q - 1) by calculating $\lfloor edg/k \rfloor$, where $\lfloor . \rfloor$ is the floor operator. If $\lfloor edg/k \rfloor$ is zero, then the guesses of k and dg are not correct. Otherwise, we can discover $\frac{p+q}{2}$ by calculating $\frac{pq - (p-1)(q-1) + 1}{2}$. If the value is an integer, then we compute

$$\left(\frac{p-q}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2 - pq.$$

If the guess of $((p - q)/2)^2$ is perfect square, we know that the original guess of k and dg is correct. From Equation (2.9), we can obtain g by calculating the expression edg mod k. Therefore, the secret exponent d can be recovered by dividing dg by g. Besides, prime factors p and q can be revealed by using (p + q)/2 and (p - q)/2.

Now, let us discuss the restriction on the secret key d. Since $\delta \approx \frac{p+q}{pq}$, in Equation (2.8), we use $\frac{p+q}{pq}$ to substitute for δ, we have

$$kdg \le \frac{pq}{\frac{3}{2}(p+q)}. \quad (2.10)$$

Generally, one can expect g to be short, and k < dg. Inequality (2.10) reveals that

$$kdg < d^2 < \frac{pq}{\frac{3}{2}(p+q)} \approx N^{1/2}.$$

This implies that

$$d < N^{1/4}.$$

From Equation (2.2), e has to be larger than $N^{3/4}$ as a result of ed > N. Therefore, we conclude that the secret exponent d can be recovered if $d < N^{1/4}$ and $N^{3/4} < e < N$.

3. Our method

This section first describes how to recover the secret exponent d if $d < N^{1/4}$ and $N^{7/4} < e < N^2$. Then, we extend our method to discover the secret exponent d if $d < \frac{N^{1/4}}{(3t)^{1/2}}$ and $N^{t-1/4} < e < N^t$, where t is a small integer.

Assume that the public exponent e is large and the secret exponent d is small such that

$N < e < N^2$ and

$$ed = K(l.c.m.\ (p-1, q-1))^2 + 1 \qquad (3.1)$$

, where K is a small integer. From Equation (3.1), we have

$$ed = \frac{K}{G^2}((p-1)(q-1))^2 + 1$$

$$= \frac{k}{g}((p-1)(q-1))^2 + 1, \qquad (3.2)$$

where $G = g.c.d.\ (p-1, q-1)$, $\frac{K}{G^2} = \frac{k}{g}$, and $g.c.d.(k, g) = 1$. Dividing both sides of Equation (3.2) by dp^2q^2, we have

$$\frac{e}{p^2q^2} = \frac{k}{dg}\left(\frac{(p-1)(q-1)}{pq}\right)^2 + \frac{1}{dp^2q^2}$$

$$= \frac{k}{dg}\left(1 - 2\left(\frac{p+q-1}{pq}\right) + \left(\frac{p+q-1}{pq}\right)^2\right) + \frac{1}{dp^2q^2}$$

$$= \frac{k}{dg}\left(1 - 2\left(\frac{p+q-1}{pq}\right) + \frac{(p+q-1)^2 + \frac{g}{k}}{p^2q^2}\right)$$

$$= \frac{k}{dg}(1 - 2\theta) \qquad (3.3)$$

where $\theta = \left(\frac{p+q-1}{pq}\right) - \frac{(p+q-1)^2 + \frac{g}{k}}{2p^2q^2}$. Because $\frac{(p+q-1)^2 + \frac{g}{k}}{2p^2q^2}$ is much smaller than $\frac{p+q-1}{pq}$ and $(p + q)$ is large, θ can be regarded as $\frac{p+q}{pq}$.

Comparing Equation (3.3) with Equation (2.5), we can view 2θ as δ. Therefore, from Inequality (2.8), if

$$kdg \le \frac{1}{\frac{3}{2}2\theta} = \frac{1}{3\theta}, \qquad (3.4)$$

we discover $\frac{k}{dg}$ by calculating the continued fraction of $\frac{e}{p^2q^2}$ like Wiener's method does.

On guessing a certain rational number $\frac{r}{s}$ by using Expression (2.6), we have to check whether $\frac{r}{s}$ is equal to $\frac{k}{dg}$ or not. For simplicity, we assume that $ed > N^2$. As a result, we have $k > g$ from Equation (3.2). Multiplying both sides of Equation (3.2) by g, we have

$$edg = k((p-1)(q-1))^2 + g. \qquad (3.5)$$

Thus, we can compute $(p-1)(q-1) = \sqrt{\lfloor edg/k \rfloor}$. If $\sqrt{\lfloor edg/k \rfloor}$ is an integer, then we discover $\frac{p+q}{2}$ by calculating $\frac{pq - (p-1)(q-1) + 1}{2}$. Next, we calculate $(\frac{p-q}{2})^2$ by $(\frac{p+q}{2})^2 - pq$. If the guess of $((p - q)/2)^2$ is perfect square, we know that the original guess of k and dg is correct. From Equation (3.5), we can obtain g by calculating the expression edg mod k. The secret exponent d, therefore, can be recovered by dividing dg by g.

In general, one can expect g to be short, and $k < dg$. Inequality (3.4) reveals that

$$kdg < d^2 < \frac{pq}{3(p+q)} \approx N^{1/2}.$$

This implies that

$$d < N^{1/4}.$$

According to Equation (3.1), we know that $e > N^{7/4}$ because $d < N^{1/4}$ and $ed > N^2$.

For the sake of clarity, as shown in Table 1, we can recover the secret exponent $d = 7$ using the continued fraction of $\frac{e}{N^2}$.

Now, let us consider another case. Assume that the public exponent e is large and the secret exponent d is small such that

$N^{t-1} < e < N^t$ and

$$ed = K(l.c.m.\ (p-1, q-1))^t + 1 \qquad (3.6)$$

, where K and t are small integers. From Equation (3.6), we have

$$ed = \frac{K}{G^t}((p-1)(q-1))^t + 1$$

$$= \frac{k}{g}((p-1)(q-1))^t + 1, \qquad (3.7)$$

where $G = g.c.d.(p\text{-}1, q\text{-}1)$, $\frac{K}{G^t} = \frac{k}{g}$, and $g.c.d.(k, g) = 1$. Dividing both sides of the above equation by dp^tq^t, we obtain

$$\frac{e}{p^tq^t} = \frac{k}{dg}\left(\frac{(p-1)(q-1)}{pq}\right)^t + \frac{1}{dp^tq^t}$$

$$= \frac{k}{dg}\left(1 - t\left(\frac{p+q-1}{pq}\right) + \ldots + \frac{(p+q-1)^t+1}{p^tq^t}\right)$$

$$= \frac{k}{dg}(1-t\theta), \qquad (3.8)$$

where $\theta = \left(\frac{p+q-1}{pq}\right) + \ldots - \frac{(p+q-1)^t + \frac{g}{k}}{tp^tq^t}$

$$\approx \frac{p+q-1}{pq} \approx \frac{p+q}{pq}.$$

Comparing Equation (3.8) with Equation (2.5), we can regard $t\theta$ as δ. Therefore, according to Inequality (2.8), if

$$kdg \leq \frac{1}{\frac{3}{2}tq}, \qquad (3.9)$$

we discover $\frac{k}{dg}$ by calculating the continued fraction of $\frac{e}{p^tq^t}$ like Wiener's method does.

On guessing a certain rational number $\frac{r}{s}$ by using Expression (2.6), we have to verify whether $\frac{r}{s}$ is equal to $\frac{k}{dg}$ or not. For simplicity, we assume that $ed > N^t$. Consequently, we have $k > g$ from Equation (3.7). Then, multiplying both sides of Equation (3.7) by g, we have

$$edg = k((p-1)(q-1))^t + g. \qquad (3.10)$$

Therefore, we can compute $(p-1)(q-1) = (\lfloor edg/k \rfloor)^{\frac{1}{t}}$. If $(\lfloor edg/k \rfloor)^{\frac{1}{t}}$ is not an integer, then the guesses of k and dg are not correct. Otherwise, we can discover $\frac{p+q}{2}$ by computing $\frac{pq - (p-1)(q-1) + 1}{2}$. If the value is an integer, then calculate $(\frac{p-q}{2})^2$ by the following formula:

$$\left(\frac{p-q}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2 - pq.$$

If the guess of $((p - q)/2)^2$ is a square number, the original k and dg is found. From Equation (3.10), we can obtain g by calculating the expression edg mod k. Therefore, the secret exponent d can be discovered by dividing dg by g.

Generally, one can expect g to be small, and $k < dg$. From Inequality (3.9), we have

$$kdg < d^2 < \frac{pq}{\frac{3}{2}t(p+q)} \approx \frac{N^{1/2}}{3t}.$$

This implies that

$$d < \frac{N^{1/4}}{(3t)^{1/2}}. \qquad (3.11)$$

According to Equation (3.6), we know that $e > N^{t-1/4}$ because $d < \frac{N^{1/4}}{(3t)^{1/2}}$ and $ed > N^t$.

On the other hand, because we expect g to be small, from Equation (3.7), we have

$G^t < d$.

Then, we have

$$G^t < \frac{N^{1/4}}{(3t)^{1/2}} \qquad (3.12)$$

because of Inequality (3.11). From Inequality (3.12), we have a restriction on t. For example, if the modulus N has 512 bits and G = 2 then we have $t < 84$. Therefore, we conclude that t is small.

4. Discussions and conclusions

Facing the case that the public exponent e satisfying $N^{t-1/4} < e < N^t$, where t is an integer, we may recover the short secret exponent d by using the continued fraction of $\frac{e}{N^t}$. However, guessing the correct $\frac{k}{dg}$, we have to check its correctness by calculating the expression $(\lfloor edg/k \rfloor)^{\frac{1}{t}}$. According to [4], we know that there is a unique positive real number v such that $v^t = \lfloor edg/k \rfloor$. Here we just check whether or not v is an integer. Therefore, we can compute v in polynomial time by using Newton-Raphson method.[1]

The original Wiener's method cannot recover the secret exponent if d is short and $e > N$. However, our proposed method can discover the secret exponent d by calculating the continued fraction of $\frac{e}{N^2}$ if $d < N^{1/4}$ and $N^{7/4}$

$< e < N^2$. Furthermore, we also recover the secret exponent d when $d < \frac{N^{1/4}}{(3t)^{1/2}}$ and $N^{t-1/4} < e < N^t$, where t is a small integer.

References

1. Burden, R. L. and Faires J. D. (1993): Numerical Analysis, 5th ed., PWS-KENT Publishing Company, Boston, 1993, pp. 56.
2. Burns, J. and Mitchell, C. J. (1994): "Parameter Selection for Server-Aided RSA Computation Schemes," IEEE Trans. on Computers, Vol. 43, No. 2, 1994, pp. 163-174.
3. Hastad, J.(1985): "On Using RSA with Low Exponent in a Public Key Network," Proc. of CRYPTO'85, springer-verlag, New York, 1986, pp. 403-408.
4. Knuth, D. E.(1973): The Art of Computer Programming, Vol. 1, Seminumerical Algorithm, 2nd edition, Addison Wesley, Reading, Mass., 1973, pp.21.
5. Pollard, J. M.(1974): "Theorems on Factorization and Primality Testing," Proc. Camb. Philo. Soc., 76(1974), pp. 521-528.
6. Rivest, R. L., Shamir, A., and Adleman, L.(1978): "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. of the ACM, Vol. 21(2), 1978, pp. 120-126.
7. Wiener, M. J. (1990): "Cryptanalysis of Short RSA Secret Exponents," IEEE Trans. on Information Theory, Vol. IT-36, 1990, pp. 553-558.
8. Williams, H. C. (1982): "A p+1 Method of Factoring," Mathematics of Computation, Vol. 39, 1982, pp. 225-234.

Table 1

$N = (587\times503) = 295261$, $e = 15453065283$

Calculated Quantity	How It is Derived	i=0	i=1	i=2	i=3	i=4
a_i	continued fraction of $\frac{e}{N^2}$	0	5	1	1	1
$\frac{r_i}{s_i} = [a_0; a_1, \ldots a_i]$	See Expression (2.6)	$\frac{0}{1}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{2}{11}$	$\frac{3}{17}$
the guess of $\frac{k}{dg}$	$[a_0; a_1, \ldots a_i+1]$ (i even) $[a_0; a_1, \ldots a_i]$ (i odd)	$\frac{1}{1}$	$\frac{1}{5}$	$\frac{2}{11}$	$\frac{2}{11}$	$\frac{5}{28}$
the guess of edg	$e \cdot dg$	15453065283	77265326415	169983718113	169983718113	432685827924
the guess of ((p-1)(q-1))	$\sqrt{\lfloor edg / k \rfloor}$	124310.36	277966.41	291533.63	291533.63	294172
the guess of (p+q)/2	(pq-(p-1)(q-1)+1)/2					545
the guess of $((p-q)/2)^2$	$((p+q)/2)^2$-pq					1764 $=(42)^2$
the guess of g	(edg mod k)					4
secret exponent d	dg/g					7