Cryptanalysis of Short Secret Exponents Modulo RSA Primes

Chien-Yuan Chen
Department of Information Engineering,
I-Shou University, Kaohsiung County, Taiwan,
84008 R.O.C.
Email: cychen@csa500.isu.edu.tw

Abstract

An attack on the short secret exponent d_q modulo a larger RSA prime q is presented. When $d_q < (\frac{2q}{3p})^{1/2}$ and $e < (pq)^{1/2}$, we can discover d_q from the continued fraction of $\frac{e}{pq}$, where e and pq denote the public exponent and the modulus, respectively. Furthermore, the same attack on unbalanced RSA is also given. According to our analysis, unbalanced RSA will be broken if $d_q < (\frac{2}{3})^{1/2} q^{4/9}$.

Keyword : RSA, continued fraction method, cryptograph

1 Introduction

When RSA [7] is used in communications between a smar t card and a large computer, it would be desirable for the smart card to have a short secret exponent. However, the short secret exponent can be easily discovered by Wiener's method if $d < N^{1/4}$ and $e < N$, where d, N, and e denote the secret exponent, the modulus, and the public exponent, respectively. To enhance the speed of decryption for the smart card [6], one can compute C^{d_p} mod p and C^{d_q} mod q, where C is a ciphertext, d_p = d mod (p - 1) and d_q = d mod (q - 1). These two computed values can be easil combined using the Chinese remainder theorem to obtain the original plaintext. Furthermore, one can reduce the secret exponentiation time by choosing d such that d_p and d_q are short. To be immune from Wiener's method, d must be larger than $N^{1/4}$.

Is there an attack on RSA such that short d_p or d_q can be discovered? This is just Wiener's open problem [10]. It als motivates our paper. According to short d_q, we use the continued fraction method to obtain the following result. If $e < N^{1/2}$, p < q and $d_q < (\frac{2q}{3p})^{1/2}$, then we can discovered d_q from the i^{th} convergent of the continued fraction of $\frac{e}{pq}$. Note that $\frac{q}{p} > 10^t$, where t is a small integer, to avoid Lehmamn's attack [4]. The main deference between our method and Wiener's [10] is the process of verifying the guess. Once we get the guess of denominator $d_q p$, it is eas to get prime p by computing *g.c.d.*($d_q p$, N). Furthermore, our method can attack unbalanced RSA [8] if d_q is short. In unbalanced RSA, the fraction $\frac{q}{p} \approx 2^{4000}$ is very large. Therefore, d_q will be discovered i $d_q < (\frac{2}{3})^{1/2} q^{4/9} \approx 2^{2000}$.

This paper is organized as follows. In Section 2, we revie Wiener's method. Section 3 describes our proposed method Our method can also attack unbalanced RSA. The result will be presented in Section 4. The last section gives some discussions and conclusions.

2 Wiener's Method

In RSA, the public exponent e and the secret exponent d satisfy the relationship

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

where *l.c.m.* (a, b) denotes the least common multiple of a and b. It means that

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

where K is an integer. Equation (2.2) can be rewritten as

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

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

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 get

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

$$= \frac{k}{dg}(1-\delta), \quad (2.5)$$

where $\delta = \frac{p+q-1-\frac{g}{k}}{pq}$. Because $(1+\frac{g}{k})$ is far smaller than pq, we have $\delta \approx \frac{p+q}{pq}$. Let $\frac{e}{pq}$ have a continued fraction form $[a_0; a_1, ..., a_n]$, where a_i is a positive integer, $0 \le i \le n$. According to [10], $\frac{k}{dg}$ can be probably found by constructing the rational number $\frac{r}{s}$ which is equal to

$[a_0; a_1, ..., a_i+1]$, if i is even,

and $[a_0; a_1, ..., a_i]$, if i is odd. (2.6)

Wiener [10] showed that if

$$kdg \le \frac{1}{\frac{3}{2}\delta}, \quad (2.7)$$

the constructed number $\frac{r}{s}$ can be equal to $\frac{k}{dg}$. Once we guess a certain rational number $\frac{r}{s}$, we have to check whether $\frac{r}{s}$ is equivalent to $\frac{k}{dg}$. For simplicity, assume that $ed > pq$. From Equation (2.4), we have $k > g$. Next, multiplying both sides of Equation (2.4) by g, we have

$$edg = k(p-1)(q-1) + g. \quad (2.8)$$

If $\lfloor edg/k \rfloor$ is zero, then the guesses of k and dg are not correct. Otherwise, we can calculate $\frac{p+q}{2} = \frac{pq - \lfloor edg/k \rfloor + 1}{2}$. If the value is an integer, then we compute

$$\left(\frac{p-q}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2 - pq. \quad (2.9)$$

If the guess of $\left(\frac{p-q}{2}\right)^2$ is perfect square, we know that the original guess of k and dg is correct. From Equation (2.8), we can obtain g by calculating the expression edg mod k. Therefore, the secret exponent d can be discovered by dividing dg by g.

Next, let us discuss the restriction on the secret exponent d. Since $\delta \approx \frac{p+q}{pq}$, in Equation (2.7), we substitute $\frac{p+q}{pq}$ 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

$$d^2 < \frac{pq}{\frac{3}{2}(p+q)} \approx N^{1/2}, \quad (2.11)$$

where $N = pq$. This implies that

$$d < N^{1/4}. \quad (2.12)$$

3 Our Method

In this section, we first describe an attack on the short exponent d_q. Next, according to [1], we present another attack on the large exponent d_q.

3.1 Attack on the Short Exponent d_q

To avoid Wiener's method and speed up decryption time, the smart card should choose a large secret exponent d such that the corresponding

$$d_p = d \bmod (p-1) \quad (3.1.1)$$

$$\text{and } d_q = d \bmod (q-1) \quad (3.1.2)$$

are very short. Because d is large, we expect that e is small. Here, we assume that $e < N^{1/2}$. Without lose of generality, we assume that $p < q$. Furthermore, according to [4], p and q should differ in length by a few digits. Thus, we have $\frac{q}{p} > 10^t$, where *t* is a small integer.

From Equation (3.1.2), there must exist an integer i such that

$$d = i(q-1) + d_q. \qquad (3.1.3)$$

Then, we use Equation (3.1.3) to substitute for d in Equation (2.2) and get

$$e(i(q-1) + d_q) = K(l.c.m.(p-1, q-1)) + 1. \qquad (3.1.4)$$

Furthermore, we have

$$ed_q = k(q-1) + 1, \qquad (3.1.5)$$

where k is an integer. Because $e < N^{1/2}$ and d_q is short, we have $k < d_q$. Dividing both sides of Equation (3.1.5) b $d_q pq$, we have

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

$$= \frac{k}{d_q p}\left(1 - \frac{1 - \frac{1}{k}}{q}\right). \qquad (3.1.6)$$

Let $\theta = \frac{1 - \frac{1}{k}}{q}$. Then, Equation (3.1.6) can be rewritten as

$$\frac{e}{pq} = \frac{k}{d_q p}(1 - \theta). \qquad (3.1.7)$$

Comparing Equation (3.1.7) with Equation (2.5), $\frac{k}{d_q p}$ can be discovered by using Formula (2.6) if

$$\theta < \frac{1}{\frac{3}{2} k d_q p}. \qquad (3.1.8)$$

Once we have the guess of $\frac{k}{d_q p}$, we compute *g.c.d.*($d_q p$, N). If *g.c.d.*($d_q p$, N)≠1 or N, we obtain p = *g.c.d.*($d_q p$, N). *Otherwise, we must try another guess of* $\frac{k}{d_q p}$.

Now, let us discuss the restriction on d_q. Since $\theta = \frac{1 - \frac{1}{k}}{q} \approx \frac{1}{q}$, in Equation (3.1.8), we use $\frac{1}{q}$ to substitute for θ, we have

$$kd_q < \frac{2q}{3p}. \qquad (3.1.9)$$

Because $k < d_q$, we view k as d_q and get

$$d_q < \left(\frac{2q}{3p}\right)^{1/2} \qquad (3.1.10)$$

According to the assumption $\frac{q}{p} > 10^t$, we have restriction

$$d_q < \left(\frac{2 * (10)^t}{3}\right)^{1/2} \qquad (3.1.11)$$

for a small integer t.

For the sake of clarity, as shown in Table 1, we can recover the secret exponent $d_q = 5$ using the continued fraction of $\frac{e}{N}$, where e = 2221 and N = 655819. It is worth noting that Wiener's method is in vain because $d > N^{1/4}$.

3.2 Attack on the Large Exponent d_q

Chen et al. [1] showed that the large secret exponent d will be discovered if $|d - l.c.m.(p-1, q-1)| < N^{1/4}$. Like [1], we assume that d_q is large such that

$$|(q-1) - d_q| < \left(\frac{2q}{3p}\right)^{1/2}. \qquad (3.2.1)$$

Without loss of generality, let $d_q < (q-1)$. Then, we compute $d_q' = (q-1) - d_q$, which satisfies

$$d_q' < \left(\frac{2q}{3p}\right)^{1/2}. \qquad (3.2.2)$$

Now, we rewrite Equation(3.1.5) as

$$e((q-1) - d_q') = k(q-1) + 1. \qquad (3.2.3)$$

It implies that

$$e d_q' = k'(q-1) - 1, \qquad (3.2.4)$$

where k' is an integer. According to the assumption of Section 3.1, we know that $e < N^{1/2}$ and d_q' is short, we have $k' < d'_q$. Dividing both sides of Equation (3.2.4) by $d'_q pq$, we have

$$\frac{e}{pq} = \frac{k'}{d'_q p}(1-\frac{1}{q}) - \frac{1}{d'_q pq}$$

$$= \frac{k'}{d'_q p}(1-\frac{1+\frac{1}{k'}}{q}) \quad . \qquad (3.2.5)$$

Let $\theta = \frac{1+\frac{1}{k'}}{q}$. Then, Equation (3.2.5) can be rewritten as

$$\frac{e}{pq} = \frac{k'}{d'_q p}(1-\theta) \quad . \qquad (3.2.6)$$

Due to Equation (3.2.2), we can compute $\frac{k'}{d'_q p}$ from the continued fraction of $\frac{e}{pq}$. Then, we discover p *g.c.d.*($d'_q p$, N). Once we get p, d'_q can be discovered by $d'_q p$ /p and another RSA prime q can also be computed b N/p. Therefore, the original d_q is recovered by (q-1) - d'_q. For the sake of clarity, as shown in Table 2, we ca n recover the large d_q using the continued fraction of $\frac{e}{N}$, where e 957 and N = 655819.

4. Attack on unbalanced RSA

The security of RSA depends on the difficulty of factoring large numbers. Therefore, a larger RSA modulus is chosen for further security. However, a larger computational effort is required for encryption and decryption. To resist against the best factorization algorithm [5] and not increase the decryption time, Shamir [8] presented the concept of unbalanced RSA. In unbalanced RSA, q is much larger than p, where q is of 4500 bits and p of 500 bits. The security of unbalanced RSA has been discussed in [2, 3]. Here we cryptanalyze it from the viewpoint of Section 3. According to [8], we know that

$$\frac{q}{p} \approx \frac{2^{4500}}{2^{500}} = 2^{4000} \qquad (4.1)$$

Like the assumption of Section 3, we have $k < d_q$. From Equation (3.1.10), we substitute 2^{4000} for $\frac{q}{p}$ and get

$$d_q < (\frac{2}{3} 2^{4000})^{1/2} \qquad (4.2)$$

Because $q \approx 2^{4500}$, the relationship between d_q and q is

$$d_q < (\frac{2}{3})^{1/2} q^{4/9} \qquad (4.3)$$

Therefore, we find that if $d_q < (\frac{2}{3})^{1/2} q^{4/9}$, we can recover d_q and further compute the secret exponent d.

5. Discussions and Conclusions

From Inequality (3.1.11), the limit of d_q is very small. For example, the limit of d_q is about 26 when t = 3. To enhance the limit of d_q, we use the Verheul and van Tilborg scheme [9]. The secret exponent d_q can be found by exhaustively searching for about 2r + 8 bit workload if $d_q < 2^r (\frac{2*(10)^t}{3})^{1/2}$, where r is an integer.

In this paper, we improve Wiener's method to discover the short secret exponent d_q when $d_q < (\frac{2q}{3p})^{1/2}$, $e < N^{1/2}$ and p < q. We then make use of the technique of [1] to discover d_q which is close to (q-1). Furthermore, we attack unbalanced RSA such that it will be insecure if $d_q < (\frac{2}{3})^{1/2} q^{4/9} \approx 2^{2000}$

NSC 89-2213-E-214-002

References

[1] C. Y. Chen, C. C. Chang, and W. P. Yang, "Cryptanalysis of the Secret Exponent of the RSA Scheme," Journal of Information Science and Engineering, Vol. 12, pp. 277-290, 1996.

[2] H. Gilbert, D. Gupta, A. Odlyzko and J. -J. Quisquater, "Attacks on Shamir's 'RSA for Paranoids'," Information Processing Letters, Vol. 68, pp. 197-199, 1998.

[3] M. Joye, J. J. Quisquater, S. M. Yen, and M. Yung, "Security Paradoxes: How improving a cryptosystem may weaken it," Proceedings of The Ninth National Conference on Information Security, TaiChung County, Taiwan, pp. 27-32, May 14-15, 1999.

[4] S. Lehmann, "Factoring Large Integers," Math. Comp., Vol. 28, pp.637-646, 1974.

[5] A. Odlyzko, "The Future of Integer Factorization," CRYPTOBYTES, Vol. 1, No. 2, pp. 5-12, 1995.

[6] J.-J. Quisquater and C. Couvreu, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem," Electronics Letters, Vol. 18, pp. 905-907, 1982.

[7] R. L. Rivest, A. Shamir, and L. Adleman, " A Method for Obtaining Digital Signatures and Public -Key Cryptosystems," Comm. of the ACM, Vol.21, pp 120-126, 1978.

[8] A. Shamir, "RSA for Paranoids," CRYPTOBYTES, Vol 1, No. 3, pp. 1-4, 1995.

[9] E. R. Verheul and H. C. A. van Tilborg, "Cryptanalysis of 'Less Short' RSA Secret Exponents," Applicabl Algebra in Engineering, Communication an Computing, Vol.8, pp.425-435, 1997.

[10] M. J. Wiener, "Cryptanalysis of Short RSA Secret Exponents," IEEE Trans. on Information Theory, V ol. IT-36, pp. 553-558, 1990.

Table 1. The process of our method when d_q is small.

$N = (137\times4787) = 655819$, $e = 3829$

Calculated Quantit	How It is Derived	i=0	i=1	i=2
a_i	continued fraction of $\frac{e}{N}$	0	171	3
$\frac{r_i}{s_i} = [a_0; a_1, ...a_i]$	See [10]	$\frac{0}{1}$	$\frac{1}{171}$	$\frac{3}{514}$
The guess of $\frac{k}{d_q p}$	$[a_0; a_1, ...a_i+1]$ (i even) $[a_0; a_1, ...a_i]$ (i odd)	$\frac{1}{1}$	$\frac{1}{171}$	$\frac{4}{685}$
The guess of p	$p = g.c.d.(d_q p, N)$	1	1	137
d_q	$d_q = d_q p/p$			5
q	$q = N/p$			4787
Secret exponent d	ed = 1 mod l.c.m.(p-1, q-1)			76581

Table 2. the process of our method when d_q is large

$N = (137\times4787) = 655819$, $e = 957$

Calculated Quantit	How It is Derived	i=0	i=1
a_i	continued fraction of $\frac{e}{N}$	0	685
$\frac{r_i}{s_i} = [a_0; a_1, ...a_i]$	See [10]	$\frac{0}{1}$	$\frac{1}{685}$
The guess of $\frac{k'}{d'_q p}$	$[a_0; a_1, ...a_i+1]$ (i even) $[a_0; a_1, ...a_i]$ (i odd)	$\frac{1}{1}$	$\frac{1}{685}$
The guess of p	$p = g.c.d.(d'_q p, N)$	1	137
d'_q	$d'_q = d'_q p / p$		5
q	$q = N/p$		4787
d_q	$d_q = (q-1) - d'_q$		4781