A generalised bound for the Wiener attack on RSA

Willy SUSILO

Joseph TONIEN

Guomin YANG
Singapore Management University, gmyang@smu.edu.sg

Journal of Information Security and Applications 53 (2020) 102531

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A generalised bound for the Wiener attack on RSA

Willy Susilo*, Joseph Tonien, Guomin Yang

Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Australia

ARTICLE INFO

Article history:
Available online 16 May 2020

MSC:
94A60
11Y05
11Y65

Keywords:
RSA
Continued fractions
Wiener technique
Small secret exponent

ABSTRACT

Since Wiener pointed out that the RSA can be broken if the private exponent d is relatively small compared to the modulus N, it has been a general belief that the Wiener attack works for $d < N^{\frac{1}{4}}$. On the contrary, in [1], it was shown that the bound $d < N^{\frac{1}{4}}$ is not accurate as it has been thought of. Specifically, for the standard assumption of the two primes p and q that $q < p < 2q$, the Wiener continued fraction technique is proven to work for $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}$. In this paper, we consider a general condition on the RSA primes, namely $q < p < \alpha q$, and we give the corresponding bound for the Wiener attack to work, which is $d \leq \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha+1)}} N^{\frac{1}{4}}$. In a special case when $\alpha = 2$, this general bound agrees with the result of [1].

1. Introduction

The RSA cryptosystem is among the most common ciphers used in the SSL/TLS protocol which allows sensitive information transmitted securely over the Internet. It is one of the most popular and de facto public-key systems used in practice today. A simplified version of the RSA encryption algorithm works as follows. Two large primes of the same size p and q are selected to form a product $N = pq$ – which is called the *RSA modulus*. Two integers e and d are chosen so that

$$ed = 1 \pmod{\phi(N)},$$

where $\phi(N) = (p-1)(q-1)$ is the order of the multiplicative group $\mathbb{Z}_N^*$. The number e is called the *encryption exponent* and d is called the *decryption exponent*. This is because to encrypt a message $m \in \mathbb{Z}_N^*$, one calculates the exponentiation $c = m^e \pmod{N}$, and to decrypt a ciphertext $c \in \mathbb{Z}_N^*$, one performs the exponentiation $m = c^d \pmod{N}$. The pair (N, e) is called the *public key* and so that anyone can encrypt, whereas d is called the *private key* and only the owner of d can perform the decryption operation.

Since the modular exponentiation $m = c^d \pmod{N}$ takes $\mathcal{O}(\log d)$ time, to reduce decryption time, one may wish to use a relatively small value of d. However, in 1991, Wiener [2] showed that if the bit-length of d is *approximately one-quarter* of that of the modulus N, then it is possible to determine the private exponent d from the public-key (N, e), hence, a total break of the cryptosystem. In research literature, there have been two different bounds reported for this attack, one is $d < N^{\frac{1}{4}}$ (for example, in [3–6]) and another one is $d < \frac{1}{3} N^{\frac{1}{4}}$ (for example, in [7–11]). The second bound is due to Boneh [7].

However, in [1], it was showed that the first bound $d < N^{\frac{1}{4}}$ is not accurate by a counterexample. The counterexample gives a concrete value of $d = \lfloor \frac{1}{2} N^{\frac{1}{4}} \rfloor + 1 < N^{\frac{1}{4}}$ and shows that the Wiener attack fails with this value of d. Also shown in [1] that it is possible to improve Boneh's bound from $d < \frac{1}{3} N^{\frac{1}{4}}$ to $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}$.

The new bound $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}$ comes partly from the condition on the two primes p and q having the same bit length. In this paper, we consider a general condition on the RSA primes, namely $q < p < \alpha q$, and we give the corresponding bound for the Wiener attack to work, which is $d \leq \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha+1)}} N^{\frac{1}{4}}$. In a special case when $\alpha = 2$, this general bound agrees with the result of [1].

The rest of this paper is organized as follows. The next section gives a brief introduction to the continued fractions. In Section 3, we give a summary of the result of [1] which shows that the Wiener continued fraction technique works for $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}$ when $q < p < 2q$. In Section 4, we consider the case $q < p < \alpha q$ and show that the bound for the Wiener attack to work is $d \leq \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha+1)}} N^{\frac{1}{4}}$. Our new bound is verified experimentally in Section 5, where we show an example with $\alpha = 8$, q is a 1024-bit prime, p is a 1027-bit prime and that the Wiener attack works for $d = \lfloor \frac{\sqrt[4]{2}}{3} N^{\frac{1}{4}} \rfloor$.

* Corresponding author.
E-mail addresses: willy.susilo@uow.edu.au (W. Susilo), joseph.tonien@uow.edu.au (J. Tonien), guomin.yang@uow.edu.au (G. Yang).

https://doi.org/10.1016/j.jisa.2020.102531
2214-2126/

2. Preliminaries

In this section, we list several well-known results about continued fractions which can be found in [12,13].

A continued fraction expansion of a rational number $\frac{u}{v}$ is an expression of the form

$$\frac{u}{v} = x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots + \cfrac{1}{x_n}}},$$

where the coefficient x_0 is an integer and all the other coefficients x_i for $i \geq 1$ are positive integers. The coefficients x_i are called the partial quotients of the continued fraction. Continued fraction expansion also exists for irrational numbers although it runs infinitely. In cryptography, finite continued fraction for rational numbers suffices our purpose.

There is a standard way to generate a unique continued fraction from any rational number. By the Euclidean division algorithm, one can efficiently determine all the coefficients $x_0, x_1, \dots, x_n$ of the continued fraction.

Given the above continued fraction of $\frac{u}{v}$, by truncating the coefficients, we obtain $(n+1)$ approximations of $\frac{u}{v}$:

$$c_0 = x_0, \quad c_1 = x_0 + \frac{1}{x_1}, \quad c_2 = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2}}, \dots,$$

$$c_n = x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots + \cfrac{1}{x_n}}}.$$

The number c_j is called the jth *convergent* of the continued fraction and these convergents provide good approximations for $\frac{u}{v}$. To write the continued fraction expansion for a number $\frac{u}{v}$, we use the Euclidean division algorithm, which terminates in $O(\log(\max(u, v)))$ steps. As a result, there are $O(\log(\max(u, v)))$ number of convergents of $\frac{u}{v}$. Thus, the Wiener continued fraction technique runs very efficiently.

The convergents $c_0, c_1, \dots, c_n$ of the continued fraction of $\frac{u}{v}$ give good approximation to $\frac{u}{v}$, however, an approximation to $\frac{u}{v}$ is not always a convergent. The following classical theorem due to Legendre gives a sufficient condition for a rational number $\frac{a}{b}$ to be a convergent for the continued fraction of $\frac{u}{v}$.

Theorem 1 (The Legendre Theorem [14]). *Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$ such that*

$$\left| \frac{u}{v} - \frac{a}{b} \right| < \frac{1}{2b^2}.$$

Then $\frac{a}{b}$ is equal to a convergent of the continued fraction of $\frac{u}{v}$.

The following Euler–Wallis Theorem gives us the recursive formulas to calculate the convergent sequence $\{c_i\}$ efficiently based on the coefficients $x_0, x_1, \dots, x_n$.

Theorem 2 (The Euler–Wallis Theorem [12]). *For any $j \geq 0$, the jth convergent can be determined as $c_j = \frac{a_j}{b_j}$, where the numerator and the denominator sequences $\{a_i\}$ and $\{b_i\}$ are calculated as follows:*

$$a_{-2} = 0, \quad a_{-1} = 1, \quad a_i = x_i\, a_{i-1} + a_{i-2}, \quad \forall i \geq 0,$$
$$b_{-2} = 1, \quad b_{-1} = 0, \quad b_i = x_i\, b_{i-1} + b_{i-2}, \quad \forall i \geq 0.$$

Based on the Euler–Wallis Theorem, the following identity involving the numerator a_i and the denominator b_i of the convergent c_i can be easily obtained by mathematical induction.

Theorem 3 [12]. *The numerator a_i and the denominator b_i of the convergent c_i satisfy the following identity*

$$b_i a_{i-1} - a_i b_{i-1} = (-1)^i, \quad \forall i \geq 0. \tag{1}$$

3. Wiener attack for equal size primes

By using the classical Legendre Theorem on continued fractions, Boneh provided the first rigorous proof [7] which showed that the Wiener attack works for $d < \frac{1}{3}N^{\frac{1}{4}}$. In [1], this bound is improved to

$$d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}.$$

Theorem 4 [7]. *If the following conditions are satisfied*

(i) $q < p < 2q$
(ii) $0 < e < \phi(N)$
(iii) $ed - k\phi(N) = 1$
(iv) $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}$

then $\frac{k}{d}$ is equal to a convergent of the continued fraction of $\frac{e}{N}$. Thus, the secret information p, q, d, k can be recovered from public information (e, N) in $O(\log(N))$ time complexity.

Remark. Since $ed - k\phi(N) = 1$, we have $\gcd(k, d) = 1$. By the identity (1) in Theorem 3, we also have $\gcd(a_i, b_i) = 1$. Therefore, if $\frac{k}{d}$ is equal to a convergent of the continued fraction of $\frac{e}{N}$,

$$\frac{k}{d} = c_i = \frac{a_i}{b_i},$$

then we must have $k = a_i$ and $d = b_i$. In that case, using the equation $ed - k\phi(N) = 1$, we have $eb_i - a_i\phi(N) = 1$, and $\phi(N) = \frac{eb_i - 1}{a_i}$.

From here, we obtain

$$S = p + q = N - \phi(N) + 1,$$

and with $N = pq$, we can solve for p and q from the quadratic equation

$$x^2 - Sx + N = 0.$$

In the Algorithm 1, we can see that if $\frac{k}{d}$ is equal to a convergent of the continued fraction of $\frac{e}{N}$ as asserted in Theorem 4, then the secret information p, q, d, k can be recovered from the public information (e, N). By the Euclidean division algorithm, we obtain $O(\log(N))$ number of convergents of the continued fraction of $\frac{e}{N}$, so the Wiener algorithm will succeed to factor N and output p, q, d, k in $O(\log(N))$ time complexity.

4. A general bound on the Wiener attack for arbitrary size primes

The coefficient $\frac{1}{\sqrt[4]{18}}$ in Theorem 4 comes partly from the condition on the two primes p and q having the same bit length. In this paper, we consider a general condition $q < p < \alpha q$ and we show that the corresponding bound for the Wiener attack to work is

$$d \leq \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha + 1)}} N^{\frac{1}{4}}.$$

When $\alpha = 2$, this agrees with the bound in Theorem 4.

Theorem 5. *If the following conditions are satisfied*

(i) $q < p < \alpha q$
(ii) $0 < e < \phi(N)$
(iii) $ed - k\phi(N) = 1$
(iv) $d \leq \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha+1)}} N^{\frac{1}{4}}$

Algorithm 1 Factorisation Algorithm Based on Continued Fraction.

Input: e, N
Output: (d, p, q) or $\perp$

Run the Euclidean division algorithm on input $(e, N)$to obtain the coefficients $x_0, x_1, \ldots, x_n$ of the continued fraction of $\frac{e}{N}$.
Use the Euler–Wallis Theorem to calculatethe convergents

$$c_0 = \frac{a_0}{b_0}, c_1 = \frac{a_1}{b_1}, \ldots, c_n = \frac{a_n}{b_n}.$$

for $0 \le i \le n$ **do**
  if $a_i | (eb_i - 1)$ **then**
    $\lambda_i = \dfrac{eb_i - 1}{a_i}$ $\triangleright$ $\lambda_i = \phi(N)$ if $\frac{a_i}{b_i} = \frac{k}{d}$
    $S = N - \lambda_i + 1$ $\triangleright$ $S = p + q$ if $\lambda_i = \phi(N)$
    Find the two roots p' and q' by solving the quadratic equation

$$x^2 - Sx + N = 0$$

    if p' and q' are prime numbers **then**
      return $(d = b_i, p = p', q = q')$ $\triangleright$ Successfully factorise N
    end if
  end if
end for
return $\perp$ $\triangleright$ Fail to factorise N

then $\frac{k}{d}$ is equal to a convergent of the continued fraction of $\frac{e}{N}$. Thus, the secret information p, q, d, k can be recovered from public information (e, N) in $O(\log(N))$ time complexity.

Proof. Since $1 < \sqrt{\frac{p}{q}} < \sqrt{\alpha}$, we have

$$\frac{p+q}{N^{\frac{1}{2}}} = \sqrt{\frac{p}{q}} + \sqrt{\frac{q}{p}} < \sqrt{\alpha} + \frac{1}{\sqrt{\alpha}} = \frac{\alpha+1}{\sqrt{\alpha}}.$$

Therefore,

$$p + q < \frac{\alpha+1}{\sqrt{\alpha}} N^{\frac{1}{2}}. \quad (2)$$

From the proof of Theorem 4,

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{p+q}{N},$$

and hence,

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

The condition $d \le \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha+1)}} N^{\frac{1}{4}}$, implies

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

and thus by the Legendre Theorem (Theorem 1), $\frac{k}{d}$ is equal to a convergent of the continued fraction of $\frac{e}{N}$ and the theorem is proved. □

5. An experimental result

In this section, we provide an experimental result to support our new bound. We select a 2051-bit modulus N and choose a private key

$$d = \left\lfloor \frac{\sqrt[4]{2}}{3} N^{\frac{1}{4}} \right\rfloor = \left\lfloor \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha+1)}} N^{\frac{1}{4}} \right\rfloor,$$

where $\alpha = 8$. The corresponding public key e is 2050-bit.

Using the Euclidean division algorithm, we determine the continued fraction expansion of $\frac{e}{N}$. This continued fraction has 1181 convergents: $c_0, c_1, \ldots, c_{1180}$. We run the Wiener algorithm through these 1181 convergents. At the 299th convergent $c_{299} = \frac{a_{299}}{b_{299}}$, we found the correct factorization of the modulus N into an 1027-bit primes p and an 1024-bit prime q. Hence, the Wiener algorithm is successful in this case which confirms our new bound.

Here are the experimental values:

$p =$ 9232360486 8932164714 9596507440 1035192029
1450809606 9566597723 8021105629 7503091019
9701404738 5807354016 3477738671 1283516912
2326923882 8750557797 0328512830 5397195543
6001628828 0368936267 6942772368 7624789705
4189248270 7903254141 8663345402 4152171374
6214923541 1392484937 8054438553 5032332198
1411866929 4194786979 525811431 (1027 bits)

$q =$ 1414690807 3406269503 3464531560 9070289526
7868521210 6382410266 7979088203 2254621850
8341886709 8719117017 5226857360 9463580013
9726042440 3423970519 3265769414 1980229445
2471842998 6490503157 0345973482 4307189649
7718367405 2896673601 2231616340 8382614148
5236962773 9987832473 8481583381 9570119849
5002627825 9886486977 705010641 (1024 bits)

$N =$ 1306093551 0862668129 9268368196 7673831028
1532856930 8290865914 7951674406 8279244280
9259952291 6182244038 7869678308 8459730618
7486890661 8456214323 5953806292 5623458437
0139268819 9848874679 9567521741 8264705335
9155783046 6484420789 5843142416 5876756784
2927515368 2364108842 7277174151 6795647859
5589300540 4081264070 5667843853 6230692499
0283849149 5134082178 7333492889 2630914169
8588678650 2174843707 3873090487 5180597934
2847006449 1342392087 9050136004 5777912483
5085903845 9463546555 3420085249 8203251335
2934838732 3760708152 0943106354 4338777875
0658112157 1154693712 9237649198 0850505236
1100891099 4357100250 8492693466 7775060445
2331802800 14437271 (2051 bits)

$e =$ 6901406503 6860039081 4956132264 1440541732
9628244881 3775820642 1051700600 0321191142
7858519759 6894841336 9045947780 8452677407
7646066962 6675830846 3747833979 8644470531
2299175228 3003210592 0196537748 6011696964
3969608108 0460635232 3629065531 8105403615
4232675072 5052749363 0002338510 8403090838
6468736364 0548523349 2036059034 5907417817
4266397821 8129295747 4393859327 9011867656
4011369005 7784548163 9157308004 2180541499

5964028825 9501600786 0676676732 4466256054
2014289463 8396713525 3155751963 4944481015
8004248560 3019492084 1695596931 0021145182
2623738481 5485792618 9841916250 7915115308
4060884377 3804491205 2136691114 9676578043
1890478318 7987207 (2050 bits)

$d =$ 7535807837 8717456677 9927946434 3898734878
0802942755 8983797188 5585141967 2560171569
4204242926 2236041073 3763539081 6820136725
4144656852 3406101419 2764542263 5543 (512 bits)

$k =$ 3981925581 0245516299 2117516495 4114612257
9625753325 9553027437 6979640067 9757747796
9661867743 8623208508 4033535480 0473441502
2269818889 4116170989 9344273972 1467 (511 bits)

In the Algorithm 1, the continued fraction of $\frac{e}{N}$ has 1181 convergents c_i, and the 299th convergent c_{299} produces the correct factorization of the modulus N.

6. Conclusion

In this paper, we extend the result of [1] and show that for the two RSA primes which satisfy the condition $q < p < \alpha q$, the Wiener attack based on continued fractions works for secret key $d \leq \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha+1)}} N^{\frac{1}{4}}$. In a special case when $\alpha = 2$, this general bound agrees with the result of [1]. Steinfeld-Contini-Wang-Pieprzyk [4] showed that Wiener's attack fails with an overwhelming probability for a random choice $d \approx N^{\frac{1}{4}+\epsilon}$. It is an open problem to extend this negative result to check in the case $q < p < \alpha q$ if the Wiener attack will fail for $d > \frac{\sqrt[4]{\alpha}}{\sqrt{2(\alpha+1)}} N^{\frac{1}{4}}$ with an overwhelming probability or not.

Declaration of Competing Interest

We have no conflict of interest in this work.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jisa.2020.102531

CRediT authorship contribution statement

Willy Susilo: Writing - original draft. **Joseph Tonien:** Formal analysis, Data curation. **Guomin Yang:** Writing - review & editing, Investigation.

References

[1] Susilo W, Tonien J, Yang G. The Wiener attack on RSA revisited: a quest for the exact bound. In: Proceedings of the 24th Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science 11547; 2019. p. 381–98.
[2] Wiener M. Cryptanalysis of short RSA secret exponents. IEEE Trans Inf Theory 1990;36:553–8.
[3] Boneh D, Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans Inf Theory 2000;46:1339–49.
[4] Steinfeld R, Contini S, Pieprzyk J, Wang H. Converse results to the Wiener attack on RSA. In: Lecture Notes in Computer Science 3386; 2005. p. 184–98.
[5] Bleichenbacher D, May A. New attacks on RSA with small secret CRT-exponents. In: Lecture Notes in Computer Science 3958; 2006. p. 1–13.
[6] Herrmann M, May A. Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Public Key Cryptography 2010, Lecture Notes in Computer Science 6056; 2010. p. 53–69.
[7] Boneh D. Twenty years of attacks on the RSA cryptosystem. Not Am Math Soc 1999;46:203–13.
[8] Bunder M, Nitaj A, Susilo W, Tonien J. A new attack on three variants of the RSA cryptosystem. In: Proceedings of the 21st Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science 9723; 2016. p. 258–68.
[9] Bunder M, Tonien J. A new attack on the RSA cryptosystem based on continued fractions. Malaysian J Math Sci 2017;11:45–57.
[10] Bunder M, Nitaj A, Susilo W, Tonien J. A generalized attack on RSA type cryptosystems. Theor Comput Sci 2017;704:74–81.
[11] Bunder M, Nitaj A, Susilo W, Tonien J. Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves. J Inf Security Appl 2018;40:193–8.
[12] Hardy G, Wright E. An introduction to the theory of numbers. 6th. Oxford University Press; 2008.
[13] Olds CD. Continued fractions. New mathematical library: 9. Washington: Mathematical Association of America; 1963.
[14] Legendre A-M. Essai sur la théorie des nombres. Duprat, Paris, An VI; 1798.