The Wiener attack on RSA revisited: A quest for the exact bound

Willy SUSILO
University of Wollongong

Joseph TONIEN
University of Wollongong

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

The Wiener Attack on RSA Revisited: A Quest for the Exact Bound

Willy Susilo, Joseph Tonien(✉), and Guomin Yang

Institute of Cybersecurity and Cryptology,
School of Computing and Information Technology,
University of Wollongong, Wollongong, Australia
{willy.susilo,joseph.tonien,guomin.yang}@uow.edu.au

Abstract. Since Wiener pointed out that the RSA can be broken if the private exponent d is relatively small compared to the modulus N (using the continued fraction technique), it has been a general belief that the Wiener attack works for $d < N^{\frac{1}{4}}$. On the contrary, in this work, we give an example where the Wiener attack fails with $d = \left\lfloor \frac{1}{2} N^{\frac{1}{4}} \right\rfloor + 1$, thus, showing that the bound $d < N^{\frac{1}{4}}$ is not accurate as it has been thought of. By using the classical Legendre Theorem on continued fractions, in 1999 Boneh provided the first rigorous proof which showed that the Wiener attack works for $d < \frac{1}{3} N^{\frac{1}{4}}$. However, the question remains whether $\frac{1}{3} N^{\frac{1}{4}}$ is the best bound for the Wiener attack. Additionally, the question whether another rigorous proof for a better bound exists remains an elusive research problem. In this paper, we attempt to answer the aforementioned problems by improving Boneh's bound after the two decades of research. By a new proof, we show that the Wiener continued fraction technique works for a wider range, namely, for $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} = \frac{1}{2.06\ldots} N^{\frac{1}{4}}$. Our new analysis is supported by an experimental result where it is shown that the Wiener attack can successfully perform the factorization on the RSA modulus N and determine a private key d where $d = \left\lfloor \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} \right\rfloor$.

Keywords: RSA · Continued fractions · Wiener technique · Small secret exponent

1 Introduction

The RSA cryptosystem is one of the most popular and de facto public-key systems used in practice today. It is among the most common ciphers used in the SSL/TLS protocol which allows sensitive information transmitted securely over the Internet.

J. Jang-Jaccard and F. Guo (Eds.): ACISP 2019, LNCS 11547, pp. 381–398, 2019.
https://doi.org/10.1007/978-3-030-21548-4_21

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 [20] 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. Wiener's attack is based on continued fractions and the idea is as follows. Since $ed = 1 \pmod{\phi(N)}$, we have $ed - k\phi(N) = 1$ for some integer k, and thus,

$$\frac{k}{d} \approx \frac{e}{\phi(N)} \approx \frac{e}{N}.$$

Now one knows that the *convergents* of the continued fraction expansion of a number provide *rational approximations* to the number, so it is natural to search for the private fraction $\frac{k}{d}$ among the convergents of the public fraction $\frac{e}{N}$. Given Wiener's approximation analysis [20], it has been a general belief that the Wiener attack works for $d < N^{\frac{1}{4}}$ (see [1,4,13,17]). On the converse, in 2005, Steinfeld-Contini-Wang-Pieprzyk [17] showed that for any positive number ϵ, with an overwhelming probability, Wiener's attack will fail for a random choice $d \approx N^{\frac{1}{4}+\epsilon}$. Thus, the bound $d < N^{\frac{1}{4}}$ has since been believed to be the optimal bound for the Wiener attack.

There are other variants of Wiener's attack [8,10,11,18] that allow the RSA cryptosystem to be broken when d is a few bits longer than $N^{\frac{1}{4}}$. In 1997, Verheul and van Tilborg [18] proposed a method that works for $d < DN^{\frac{1}{4}}$ using an exhaustive search of about $2\log D + 8$ bits. This method was later improved by Dujella [10,11]. In the Verheul and van Tilborg attack [18], the secret exponent is of the form $d = rb_{m+1} + sb_m$, where the b_i are the denominators of the convergents of the continued fraction. Calculation of the convergents needs a complexity of $O(\log N)$, and so searching through all possible pairs (r, s) at each convergent makes the running time increased by a factor of $O(D^2A^2)$, where A is the maximum of the partial quotients $x_{m+1}, x_{m+2}, x_{m+3}$ of the continued fraction. The first Dujella method [10] improved this extra running time factor to $O(D^2 \log A)$ and $O(D^2 \log D)$, and the second Dujella method [11] improved it further to $O(D \log D)$ (with the space complexity of $O(D)$). In 2017, Bunder and Tonien [8] proposed another variant of Wiener's attack. Instead of considering the continued fraction of $\frac{e}{N}$ as in the original Wiener's attack, the Bunder and Tonien method uses the continued fraction of $\frac{e}{N'}$, where N' is a number depending on N. This new attack works for $d < 2^{(n+3-t)/2}N^{\frac{1}{4}}$ where $n = \log N$, $t = \log e$, and the running time is $O(\log N)$.

There are yet other variants of Wiener's attack that utilise more than just the public information (N, e). For example, the Weger attack [19] exploited the small distance between the two RSA's secret primes: if $|p - q| = N^{\beta}$ and $d = N^{\delta}$ then d can be recovered if $2 - 4\beta < \delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ or $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$. The Blömer and May attack [2] assumed a linear relation between e and $\phi(N)$: $ex + y = 0 \mod \phi(N)$ with either $0 < x < \frac{1}{3}N^{\frac{1}{4}}$ and $y = \mathcal{O}(N^{-\frac{3}{4}}ex)$ or $x < \frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}}$ and $|y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$. The Nassr et al. attack [15] required an approximation $p_o \geq \sqrt{N}$ of the prime p.

In 1999, Boneh and Durfee [4] showed the first significant improvement over the Wiener's result. Based on the Coppersmith technique [9], exploiting a non-linear equation satisfied by the secret exponent, the Boneh-Durfee method can break the RSA when $d < N^{0.292}$. Using a somewhat more optimized lattice, Herrmann and May [13] also derived the same bound $d < N^{0.292}$, although their proof is more elementary. This bound $d < N^{0.292}$ remains as the best bound to date.

Our Contributions. In this paper, we revisit Wiener's original attack based on continued fraction technique. In research literature, there have been two different bounds reported for this attack, one is $d < N^{\frac{1}{4}}$ (for example, in [1,4,13,17]) and another one is $d < \frac{1}{3}N^{\frac{1}{4}}$ (for example, in [3,5–8]). The second bound is due to Boneh [3]. Our main contributions in this paper are twofold: on one hand, we show that the first bound $d < N^{\frac{1}{4}}$ is not accurate, and on the other hand, we can improve the Boneh bound from $d < \frac{1}{3}N^{\frac{1}{4}}$ to $d \leq \frac{1}{2.06...}N^{\frac{1}{4}}$. Since many attacks on RSA based on the original Wiener attack, it is important to revisit this attack and provide an accurate analysis.

Our First Contribution. Based on the implementation of the Wiener algorithm and its execution, we have discovered that the Wiener attack fails for many values of $d < N^{\frac{1}{4}}$. This contradicts to the general belief about the Wiener attack where it has been reported that the Wiener attack works for all $d < N^{\frac{1}{4}}$ (see [1,4,13,17]). Obviously, to disprove this bound $d < N^{\frac{1}{4}}$, *one only needs to show one counterexample, i.e. a value of $d < N^{\frac{1}{4}}$ where the Wiener attack fails.* We do that in Sect. 4, where it is shown that the Wiener attack fails for a certain value of N and d with

$$d = \left\lfloor \frac{1}{2}N^{\frac{1}{4}} \right\rfloor + 1 < N^{\frac{1}{4}}.$$

Therefore, the bound $d < N^{\frac{1}{4}}$ for the Wiener attack *is not accurate* as it has been believed to date. At least, we can see that it fails at the halfway point of the range. This raises a natural question: *what is the correct bound for the Wiener attack?* And this comes to our second contribution.

Our Second Contribution. Boneh [3] provided the first and only rigorous proof which showed that the Wiener attack works for

$$d < \frac{1}{3}N^{\frac{1}{4}}.$$

The remaining question is whether this bound is the best bound for the Wiener attack. Additionally, we are wondering whether there exists another rigorous proof for a better bound. As the second contribution of this paper, we answer this question affirmatively by improving Boneh's bound.

Boneh's result does not say anything about the case $d \geq \frac{1}{3}N^{\frac{1}{4}}$. So the Wiener attack may work or it may fail for $d \geq \frac{1}{3}N^{\frac{1}{4}}$. Our first result already shows an instance where the Wiener attack fails at $d = \left\lfloor \frac{1}{2}N^{\frac{1}{4}} \right\rfloor + 1 \simeq \frac{1}{2}N^{\frac{1}{4}}$. This raises an open question: *does the Wiener attack work or fail in the following interval*

$$\frac{1}{3}N^{\frac{1}{4}} \leq d < \frac{1}{2}N^{\frac{1}{4}} \ ?$$

As the second contribution of this paper, using exactly the same setting as that of Boneh [3], we prove that the Wiener attack is always successful for all values of d in the larger interval

$$d \leq \frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}} = \frac{1}{2.06...}N^{\frac{1}{4}}.$$

With this improvement of Boneh's bound from $d < \frac{1}{3}N^{\frac{1}{4}}$ to $d \leq \frac{1}{2.06...}N^{\frac{1}{4}}$, we show that the Wiener attack works for all value of d in the interval

$$\frac{1}{3}N^{\frac{1}{4}} \leq d \leq \frac{1}{2.06...}N^{\frac{1}{4}}.$$

Thus, the undecided interval has been narrowed down to

$$\frac{1}{2.06...}N^{\frac{1}{4}} < d < \frac{1}{2}N^{\frac{1}{4}}$$

and it is unknown if the Wiener attack fails or succeeds in this narrow interval. Nevertheless, we conjecture that our new bound $\frac{1}{2.06...}N^{\frac{1}{4}}$ is indeed *the best bound* for the Wiener attack. We conjecture that, for any $\frac{1}{2.06...} < \alpha \leq \frac{1}{2}$, there is always a value of d in the interval $\frac{1}{2.06...}N^{\frac{1}{4}} < d < \alpha N^{\frac{1}{4}}$ that makes the Wiener attack fail.

Our Experimental Results. In this paper, we show two experimental results. In Sect. 4, we show an example where *the Wiener attack fails* with

$$d = \left\lfloor \frac{1}{2}N^{\frac{1}{4}} \right\rfloor + 1 < N^{\frac{1}{4}},$$

this is *a counterexample* to disprove the first bound $d < N^{\frac{1}{4}}$. In Sect. 6, we show an example that *the Wiener attack works* with

$$d = \left\lfloor \frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}} \right\rfloor = \left\lfloor \frac{1}{2.06...}N^{\frac{1}{4}} \right\rfloor,$$

this is *an illustration* to our new improved bound $d \leq \frac{1}{2.06...}N^{\frac{1}{4}}$.

Roadmap. The rest of this paper is organized as follows. The next section gives a brief introduction to the continued fractions. We revisit Boneh's version of Wiener's attack in Sect. 3 for clarity and completeness. In Sect. 4, we demonstrate our first experimental result showing an example that the Wiener attack fails at $d = \left\lfloor \frac{1}{2} N^{\frac{1}{4}} \right\rfloor + 1$. In Sect. 5, we give a new rigorous proof which shows that the Wiener continued fraction technique works for $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} = \frac{1}{2.06...} N^{\frac{1}{4}}$. Our new bound is verified experimentally in Sect. 6, where we show an example that the Wiener attack works with $d = \left\lfloor \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} \right\rfloor$. Finally, we conclude our paper and discuss open problems in Sect. 7.

2 Preliminaries

In this section, we list several well-known results about continued fractions which can be found in [12,16].

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 $x_0, x_1, \ldots, x_n$ of the continued fraction. For clarity, we present the following example to show how to construct the continued fraction for $\frac{2000}{2019}$.

By the Euclidean division algorithm, we have

$$\begin{aligned} 2000 &= 2019 \times \mathbf{0} + 2000 \\ 2019 &= 2000 \times \mathbf{1} + 19 \\ 2000 &= 19 \times \mathbf{105} + 5 \\ 19 &= 5 \times \mathbf{3} + 4 \\ 5 &= 4 \times \mathbf{1} + 1 \\ 4 &= 1 \times \mathbf{4} \end{aligned}$$

and thus, we can see that the coefficients $0, 1, 105, 3, 1, 4$ determined by the above Euclidean division algorithm become the coefficients for the continued fraction as follows,

$$\frac{2000}{2019} = \mathbf{0} + \frac{2000}{2019} = \mathbf{0} + \frac{1}{\frac{2019}{2000}} = \mathbf{0} + \cfrac{1}{\mathbf{1} + \cfrac{19}{2000}} = \mathbf{0} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\frac{2000}{19}}}$$

$$= \mathbf{0} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{105} + \cfrac{5}{19}}} = \mathbf{0} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{105} + \cfrac{1}{\frac{19}{5}}}}$$

$$= \mathbf{0} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{105} + \cfrac{1}{\mathbf{3} + \cfrac{4}{5}}}} = \mathbf{0} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{105} + \cfrac{1}{\mathbf{3} + \cfrac{1}{\frac{5}{4}}}}}$$

$$= \mathbf{0} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{105} + \cfrac{1}{\mathbf{3} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{4}}}}}}.$$

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

$$c_0 = x_0, \quad c_1 = x_0 + \frac{1}{x_1}, \quad c_2 = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2}}, \ldots, \quad c_n = x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots + \cfrac{1}{x_n}}}.$$

The number c_j is called the j^{th} *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 $c_0, c_1, \ldots, c_n$ 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, $x_1, \ldots, x_n$.

Theorem 2 (The Euler-Wallis Theorem [12]). *For any $j \geq 0$, the j^{th} 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:*

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

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 Boneh's Version of the Wiener Attack

In this section, for clarity and completeness, we recall here Boneh's version of the Wiener attack result [3]. Boneh provided the first and only rigorous proof which showed that the Wiener attack works for

$$d < \frac{1}{3} N^{\frac{1}{4}}.$$

Theorem 4 (The Wiener-Boneh Theorem [3]). *If the following conditions are satisfied*

(i) $q < p < 2q$
(ii) $0 < e < \phi(N)$
(iii) $ed - k\phi(N) = 1$
(iv) $d < \frac{1}{3} N^{\frac{1}{4}}$

then $\frac{k}{d}$ is equal to a convergent of the continued fraction of $\frac{e}{N}$.

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

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

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 $x_0, x_1, \dots, x_n$ of the continued fraction of $\frac{e}{N}$.
Use the Euler-Wallis Theorem to calculate the convergents
    $c_0 = \frac{a_0}{b_0}, c_1 = \frac{a_1}{b_1}, \dots, c_n = \frac{a_n}{b_n}$.
for $0 \le i \le n$ do
    if $a_i | (eb_i - 1)$ then
        $\lambda_i = \frac{eb_i - 1}{a_i}$                    ▷ $\lambda_i = \phi(N)$ if $\frac{a_i}{b_i} = \frac{k}{d}$
        $S = N - \lambda_i + 1$                              ▷ $S = p + q$ 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 $(d = b_i, p = p', q = q')$               ▷ Successfully factorise N
        end if
    end if
end for
return $\perp$                                               ▷ Fail to factorise N
```

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.

Our experiments confirm that the Wiener algorithm runs very efficiently. In Sects. 4 and 5, we use 1024-bit primes p and q, and with the Euclidean division algorithm, the continued fractions of $\frac{e}{N}$ give us less than 2000 convergents c_i.

4 An Experimental Result

In this section, we give an example where the Wiener attack fails with

$$d = \left\lfloor \frac{1}{2} N^{\frac{1}{4}} \right\rfloor + 1,$$

thus, showing that the bound $d < N^{\frac{1}{4}}$ is not accurate as it has been generally believed [1,4,13,17].

This result came as a total surprise to us. As we implemented the Wiener algorithm and run it, we found out that the Wiener attack failed for many values of $d < N^{\frac{1}{4}}$. The example here clearly shows that it fails at the halfway point of the range. This raises a natural question: what is the correct bound for the Wiener attack? Attempting to answer this question has been the motivation of this work, and hence *the quest for the exact bound.*

Below, we choose 1024-bit primes p and q which give 2047-bit modulus N. We set the private key

$$d = \left\lfloor \frac{1}{2} N^{\frac{1}{4}} \right\rfloor + 1$$

which is a 511-bit number and the corresponding public key e is 2047-bit. Using the Euclidean division algorithm, we determine the continued fraction expansion of $\frac{e}{N}$. This continued fraction has 1179 convergents: $c_0, c_1, \ldots, c_{1178}$. Using the Algorithm 1 to search through these 1179 convergents, we found no factorization of N, so the Wiener algorithm failed in this case.

Here are the experimental values:

$$\begin{aligned} p = {} & 1491527899\ 5477760590\ 2728010071\ 6980981660\ 1258222662 \\ & 2431819289\ 1225141694\ 5753993233\ 4134597092\ 2789813803 \\ & 2123071118\ 7456841568\ 6244681095\ 6494959013\ 6209617496 \\ & 4856101327\ 5715997217\ 9803365696\ 1960828527\ 8759316539 \\ & 7375676105\ 8838761560\ 3738626761\ 6351893514\ 2444493175 \\ & 0194503087\ 8223260165\ 3356278700\ 2338989328\ 5059210806 \\ & 959842047 \text{ (1024 bits)} \end{aligned}$$

$$\begin{aligned} q = {} & 9111167064\ 7390707425\ 7779057216\ 8580155934\ 8047103723 \\ & 9509013689\ 9393941503\ 6663226117\ 3483046733\ 6435253791 \\ & 0245424858\ 8231334271\ 0003745035\ 1560880167\ 0686028666 \\ & 9368653851\ 4065809046\ 6070550773\ 1596277357\ 7225073326 \\ & 8667388642\ 6946395521\ 3055868264\ 9615090699\ 8451255847 \\ & 8563387800\ 1084724118\ 4269448761\ 8873870285\ 9133249777 \\ & 21380459 \text{ (1024 bits)} \end{aligned}$$

N =1358955987 4499142355 7513414060 3539768425 5014057126
0741075421 2867822612 0805968144 4708819214 5518842119
9958881804 7937878622 4112295347 5325559673 5996725202
8633553360 3757756220 1871004594 8076611030 2567765384
0026153784 2770613729 4329327237 0569653405 5424667619
2238028495 4841783632 6958663905 5958512318 1193434612
0315768395 7219446440 1318651117 5563726203 4345904525
9443782456 6436078112 6077167607 7739231458 9205427377
2268437286 4735492393 2750716520 2984412539 2729934943
9305127634 2706564766 5583235029 4396813965 7917910935
3031271720 0339494884 0018966371 3447510835 9275849868
6562766142 9910164397 0677468356 5904851307 0086539066
0235916943 2359573 (2047 bits)

e =1330419030 5540874988 5376069329 7084174518 7260177538
5866925366 2997366672 3493599969 0390276038 0919368940
1864701342 9310242427 8833742509 7494436400 5403659294
0555161192 1972457828 7339053358 7614588496 6324498356
6363071098 8205134167 5000847275 0988164806 4636099774
1181379056 1319572282 3672568352 1298430680 1201814131
9604052114 8335594185 3173571813 7624310228 5349453986
0737412659 9608417423 2546667689 2033178326 5130304082
6314383724 2740893126 4550856662 5119551763 4091295935
2191957179 9876282943 3381372125 9047810743 6224521388
6861509236 7407065451 7584476965 4348997529 8178870165
9669410312 1497394053 8763499800 1901681249 3233425747
4891365832 5046931 (2047 bits)

$d = \left\lfloor \frac{1}{2}N^{\frac{1}{4}} \right\rfloor + 1$ =5398478203 0311651626 6068367829 8945738486 9044874575
7958435010 7981488386 1130096080 6180756651 2262828961
6340636130 6706635548 8922382801 5381181990 9555989039
3235 (511 bits)

k =5285114605 3829091397 9620556948 0145234187 5641719964
7496242061 4986547849 9915220055 9741796430 2523466970
5824394524 5600033207 6486525013 4460390163 5991230680
7438 (511 bits)

In the Algorithm 1, the continued fraction of $\frac{e}{N}$ has 1179 convergents c_i, so

$$n = 1178.$$

In line 4 of the Algorithm 1, there are only 2 values of i that $a_i \mid (eb_i - 1)$:

$$i = 1, \quad a_1 = 1, \quad b_1 = 1,$$

and

$$i = 3, \quad a_3 = 47, \quad b_3 = 48.$$

With these two cases: $i = 1$ and $i = 3$, the quadratic equation in line 7 of the Algorithm 1 does not produce prime number roots. So the Wiener algorithm fails in this example.

We can explain the reason for the Wiener algorithm fails in this example. This is because among 1179 convergents of the continued fraction of $\frac{e}{N}$, none of them is equal to $\frac{k}{d}$ as required in Theorem 4.

5 Improving Boneh's Bound on the Wiener Attack

By using the classical Legendre Theorem on continued fractions, Boneh provided the first rigorous proof [3] which showed that the Wiener attack works for

$$d < \frac{1}{3} N^{\frac{1}{4}}.$$

In this section, we establish an improved bound on the Wiener's attack. We extend the well-known Boneh's bound and show that the Wiener continued fraction technique works for a wider range, namely, for

$$d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} = \frac{1}{2.06...} N^{\frac{1}{4}}.$$

Below is our new theorem which is an improvement of the Wiener-Boneh Theorem (i.e., Theorem 4). Additionally, our new proof is also based on the Legendre Theorem.

Theorem 5. *If the following conditions are satisfied*

(i) $q < p < 2q$
(ii) $0 < e < \phi(N)$
(iii) $ed - k\phi(N) = 1$
(iv) $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} = \frac{1}{2.06...} N^{\frac{1}{4}}$

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.*

Proof. As we want to use the Legendre Theorem (Theorem 1) to prove that $\frac{k}{d}$ is equal to a convergent of the continued fraction of $\frac{e}{N}$, we consider the following inequality

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \frac{|kN - ed|}{Nd} = \frac{|k(N - \phi(N)) - (ed - k\phi(N))|}{Nd}$$
$$= \frac{k(p+q-1) - 1}{Nd} < \frac{k(p+q)}{Nd}.$$

Since $ed - k\phi(N) = 1$ and $e < \phi(N)$, we have $k < d$. Therefore,

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

It follows from $q < p < 2q$ that $1 < \sqrt{\frac{p}{q}} < \sqrt{2}$, and since the function $f(x) = x + \frac{1}{x}$ is increasing on $[1, +\infty)$, we have

$$\frac{p+q}{N^{\frac{1}{2}}} = \sqrt{\frac{p}{q}} + \sqrt{\frac{q}{p}} < \sqrt{2} + \frac{1}{\sqrt{2}} = \frac{3}{\sqrt{2}}.$$

Thus,

$$p + q < \frac{3}{\sqrt{2}} N^{\frac{1}{2}}. \tag{2}$$

It follows that

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{\frac{3}{\sqrt{2}} N^{\frac{1}{2}}}{N} = \frac{3}{\sqrt{2} N^{\frac{1}{2}}}$$

Finally, since $d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}$, we have

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

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. ■

6 The Second Experimental Result

In Sect. 5, we improve the Boneh bound [3]:

$$d < \frac{1}{3} N^{\frac{1}{4}}.$$

We show that the Wiener continued fraction technique works for a wider range, namely, for

$$d \leq \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} = \frac{1}{2.06...} N^{\frac{1}{4}}.$$

In this section, we provide an experimental result to support our new bound. We choose a private key $d = \left\lfloor \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} \right\rfloor$ and show that the Wiener attack indeed works, which confirms our new bound.

Here, we select a 2048-bit modulus N. We set the private key $d = \left\lfloor \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} \right\rfloor$ which is a 511-bit number. The corresponding public key e is 2048-bit.

Using the Euclidean division algorithm, we determine the continued fraction expansion of $\frac{e}{N}$. This continued fraction has 1219 convergents: $c_0, c_1, \ldots, c_{1218}$. We run the Wiener algorithm through these 1219 convergents. At the 289$^{\text{th}}$ convergent $c_{289} = \frac{a_{289}}{b_{289}}$, we found the correct factorization of the modulus N into two 1024-bit primes p and q. Hence, the Wiener algorithm is successful in this case which confirms our new bound in Theorem 5.

Here are the experimental values:

$$\begin{aligned} p =& 1753651555\ 7959285985\ 8389246962\ 5666004143\ 2631322905 \\ & 3792511376\ 1823387899\ 6863875472\ 8500338195\ 6106187059 \\ & 8979790786\ 3900938931\ 7295752778\ 9842328060\ 3224176903 \\ & 6697007530\ 6302349794\ 5882100113\ 2594934722\ 2701276857 \\ & 3702925327\ 3032617922\ 5592387182\ 1655023312\ 3781280062 \\ & 3318071860\ 0703325676\ 9316877525\ 0029640840\ 1329310468 \\ & 563365517 \text{ (1024 bits)} \end{aligned}$$

$$\begin{aligned} q =& 1302246063\ 5244450969\ 8486520987\ 6835312123\ 3825549540 \\ & 4590911663\ 0930183138\ 4524166515\ 2217429150\ 6917508540 \\ & 1229882549\ 1643140442\ 7317286012\ 5333646913\ 8593238275 \\ & 0954632799\ 2092626902\ 5564720911\ 8376898712\ 1336228332 \\ & 6412475983\ 8782926026\ 4681550732\ 7524640686\ 1898664920 \\ & 0982675880\ 5711531846\ 6818868729\ 5634599558\ 9465454245 \\ & 497973799 \text{ (1024 bits)} \end{aligned}$$

$N =$2283685835 3287668091 9203688162 8641577810 3964252589
2829513042 0474999022 9966219821 6666459658 1454018899
4842992237 6560732622 7548715380 4387435627 0300826321
1665057256 4937978011 1813943886 7926552494 0467869924
8547365003 8355720409 4262355848 3358418844 9224331698
6356990029 6911605460 6455811765 2232596722 1393273906
6967318845 7131381644 1207877832 1534284874 4792830245
0180559814 0668893320 3072001361 9079413832 5132168722
1421794347 4001731747 8227015966 3404029234 2194986951
9455164666 8806852454 0063123724 1365869202 7515557841
4144066123 2146905186 4313571125 6653677066 9381756925
3817941547 8954522854 7119685992 7901448206 0579354284
5523886372 6089083 (2048 bits)

$e =$1716081930 8904585327 7890161348 9791423576 2203050367
3463267958 5567058963 9956759654 2803490663 7374660531
6475059968 7461192166 4245059192 9370601129 3378320096
4337238276 6547546926 5356977528 0523991876 7190684796
2650929866 9049485976 1183156661 2687168184 7641670872
5889507391 9139366379 9018676640 7654053176 5577090231
6720982183 2859747419 6583443634 6658489531 6847817524
2470325739 2651850823 5172974203 8213894377 0358904660
5944230019 1228592937 2517345927 3262320732 4742303631
3243627441 4264865868 0285278401 0248376241 4082363751
8720861263 2105886502 3936481567 7633023698 7329249988
1142950825 6124902530 9574993383 3690395192 4035916501
5366161007 0010419 (2048 bits)

$d = \left\lfloor \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}} \right\rfloor =$5968166949 0793605552 2026899285 2191823920 0238114742
8873867437 0592596189 5174438877 8002365303 1793516493
8064621142 4818137141 6016184480 4216409734 3986334607
9123 (511 bits)

In the Algorithm 1, the continued fraction of $\frac{e}{N}$ has 1219 convergents c_i, and the 289th convergent c_{289} produces the correct factorization of the modulus N.

$$i = 289,$$

a_{289} =4484795282 8757963262 4661693174 9335120861 3264690597
1711725983 1381808371 6124351193 7219275062 5936785513
3802411458 7021923657 4897458445 0198267245 3098232091
5377

b_{289} =5968166949 0793605552 2026899285 2191823920 0238114742
8873867437 0592596189 5174438877 8002365303 1793516493
8064621142 4818137141 6016184480 4216409734 3986334607
9123

λ_{289} =2283685835 3287668091 9203688162 8641577810 3964252589
2829513042 0474999022 9966219821 6666459658 1454018899
4842992237 6560732622 7548715380 4387435627 0300826321
1665057256 4937978011 1813943886 7926552494 0467869924
8547365003 8355720409 4262355848 3358418844 9224331698
6356990029 6911605460 6455811765 2232596722 1393273906
6967318815 1541619712 0834182263 3957489849 4661203580
4493315230 2326589392 7714897548 0275215025 3355434091
9052234345 3034398192 3819078520 2100150082 4597489533
7713646790 3642819470 0565454009 6683766693 0332214401
0393547122 0606774068 2759176222 9259885575 1415357068
5823443304 8879748790 5633933631 4326822749 4155314376
6047414966 4749768

The quadratic equation in line 7 produces two correct prime roots p and q. Hence, the Wiener algorithm is successful in this example.

We can see that the Wiener algorithm works because the convergent

$$c_{289} = \frac{a_{289}}{b_{289}} = \frac{k}{d}$$

as confirmed in our Theorem 5.

7 Conclusion

In this paper, we show a certain belief about the Wiener attack on the RSA is not accurate. It has been a general belief that the Wiener attack works for $d < N^{\frac{1}{4}}$ (see [1,4,13,17]), and on the converse, Steinfeld-Contini-Wang-Pieprzyk [17] showed that Wiener's attack fails with an overwhelming probability for a random choice $d \approx N^{\frac{1}{4}+\epsilon}$ for any positive number ϵ. Thus, as depicted in Fig. 1(i),

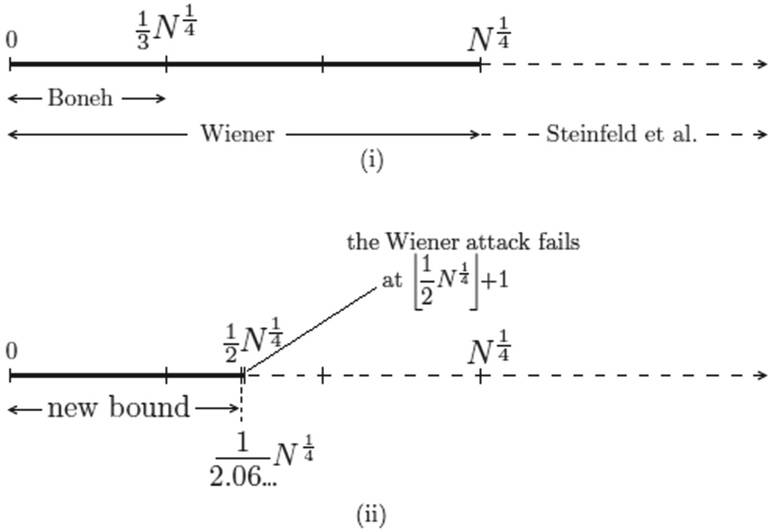
0
$\frac{1}{3}N^{\frac{1}{4}}$
$N^{\frac{1}{4}}$
Boneh
Wiener
Steinfeld et al.
(i)
the Wiener attack fails
at $\left\lfloor\frac{1}{2}N^{\frac{1}{4}}\right\rfloor+1$
0
$\frac{1}{2}N^{\frac{1}{4}}$
$N^{\frac{1}{4}}$
new bound
$\frac{1}{2.06...}N^{\frac{1}{4}}$
(ii)

Fig. 1. (i) Old belief: Wiener attack works for $d < N^{\frac{1}{4}}$. Boneh's rigorous proof covers $d < \frac{1}{3}N^{\frac{1}{4}}$. (ii) Our research shows that Wiener attack fails at $d = \lfloor \frac{1}{2}N^{\frac{1}{4}} \rfloor + 1$. Our new rigorous proof covers $d \leq \frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}} = \frac{1}{2.06...}N^{\frac{1}{4}}$.

the bound $d < N^{\frac{1}{4}}$ has since been believed to be the optimal bound for the Wiener attack.

On the contrary, in this paper, we show that the bound $d < N^{\frac{1}{4}}$ for the Wiener attack on the RSA is not accurate. We give an example where the Wiener attack fails with

$$d = \left\lfloor \frac{1}{2}N^{\frac{1}{4}} \right\rfloor + 1.$$

By using the Legendre Theorem on continued fractions, Boneh provided the first rigorous proof which showed that the Wiener attack works for

$$d < \frac{1}{3}N^{\frac{1}{4}}.$$

As depicted in Fig. 1(ii), in this paper, we improve Boneh's bound by showing that the Wiener continued fraction technique actually works for a wider range, namely, for

$$d \leq \frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}} = \frac{1}{2.06...}N^{\frac{1}{4}}.$$

Our new result is supported by an experimental result where it is shown that the Wiener attack succeeds with $d = \left\lfloor \frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}} \right\rfloor$.

It is an open problem to determine the exact optimal bound for the Wiener attack. Suppose that

$$d < \omega N^{\frac{1}{4}}$$

is this exact optimal bound, then by the two main results of this paper, it follows that

$$\frac{1}{\sqrt[4]{18}} \leq \omega \leq \frac{1}{2},$$

where $\sqrt[4]{18} = 2.06...$ We are yet to find the exact value of ω and we conjecture that $\omega = \frac{1}{\sqrt[4]{18}}$ (Fig. 2).

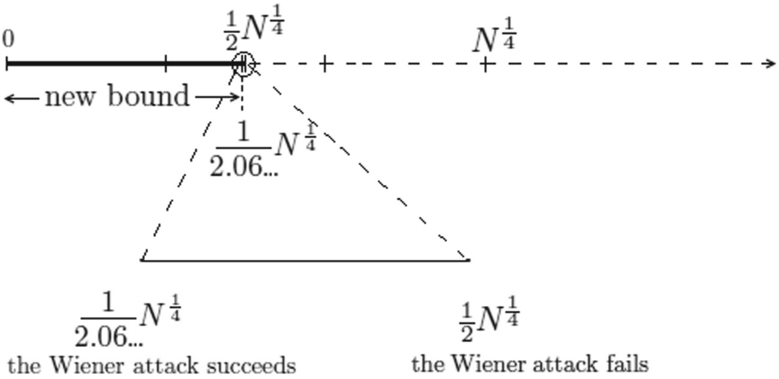
0
$\frac{1}{2}N^{\frac{1}{4}}$
$N^{\frac{1}{4}}$
← new bound →
$\frac{1}{2.06...}N^{\frac{1}{4}}$
$\frac{1}{2.06...}N^{\frac{1}{4}}$
the Wiener attack succeeds
$\frac{1}{2}N^{\frac{1}{4}}$
the Wiener attack fails

Fig. 2. Open problem. Undecided interval: it is unknown if the Wiener attack fails or succeeds in the interval $\frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}} < d \leq \frac{1}{2}N^{\frac{1}{4}}$.

References

1. Bleichenbacher, D., May, A.: New attacks on RSA with small secret CRT-exponents. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 1–13. Springer, Heidelberg (2006). https://doi.org/10.1007/11745853_1
2. Blömer, J., May, A.: A generalized wiener attack on RSA. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 1–13. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24632-9_1
3. Boneh, D.: Twenty years of attacks on the RSA cryptosystem. Not. Am. Math. Soc. **46**, 203–213 (1999)
4. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. Inf. Theor. **46**, 1339–1349 (2000)
5. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A new attack on three variants of the RSA cryptosystem. In: Liu, J.K., Steinfeld, R. (eds.) ACISP 2016. LNCS, vol. 9723, pp. 258–268. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-40367-0_16
6. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A generalized attack on RSA type cryptosystems. Theor. Comput. Sci. **704**, 74–81 (2017)
7. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves. J. Inf. Secur. Appl. **40**, 193–198 (2018)

8. Bunder, M., Tonien, J.: A new attack on the RSA cryptosystem based on continued fractions. Malays. J. Math. Sci. **11**, 45–57 (2017)
9. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptology **10**, 233–260 (1997)
10. Dujella, A.: Continued fractions and RSA with small secret exponent. Tatra Mt. Math. Publ. **29**, 101–112 (2004)
11. Dujella, A.: A variant of wiener's attack on RSA. Computing **85**, 77–83 (2009)
12. Hardy, G., Wright, E.: An Introduction to the Theory of Numbers, 6th edn. Oxford University Press, Oxford (2008)
13. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 53–69. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_4
14. Legendre, A.M.: Essai sur la théorie des nombres. Duprat, An VI, Paris (1798)
15. Nassr, D.I., Bahig, H.M., Bhery, A., Daoud, S.S.: A new RSA vulnerability using continued fractions. In: Proceedings of IEEE/ACS International Conference on Computer Systems and Applications AICCSA, 2008, pp. 694–701 (2008)
16. Olds, C.D.: Continued fractions. New Mathematical Library, vol. 9. Mathematical Association of America, Washington (1963)
17. Steinfeld, R., Contini, S., Wang, H., Pieprzyk, J.: Converse results to the wiener attack on RSA. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 184–198. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30580-4_13
18. Verheul, E., van Tilborg, H.: Cryptanalysis of 'less short' RSA secret exponents. Appl. Algebra Eng. Commun. Comput. **8**, 425–435 (1997)
19. de Weger, B.: Cryptanalysis of RSA with small prime difference. Appl. Algebra Eng. Commun. Comput. **13**, 17–28 (2002)
20. Wiener, M.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theor. **36**, 553–558 (1990)