2-2021

Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA

Willy SUSILO

Joseph TONIEN

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

Computer Standards & Interfaces 74 (2021) 103470

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA

Willy Susilo, Joseph Tonien, Guomin Yang*

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

ARTICLE INFO

Keywords:
RSA
Wiener
Boneh–Durfee
Short key attack
Continued fractions

2010 MSC:
94A60
11Y05

ABSTRACT

RSA is a well known standard algorithm used by modern computers to encrypt and decrypt messages. In some applications, to save the decryption time, it is desirable to have a short secret key d compared to the modulus N. The first significant attack that breaks RSA with short secret key given by Wiener in 1990 is based on the continued fraction technique and it works with $d < \frac{1}{\sqrt[4]{18}} N^{.25}$. A decade later, in 2000, Boneh and Durfee presented an improved attack based on lattice technique which works with $d < N^{.292}$. Until this day, Boneh–Durfee attack remain as the best attack on RSA with short secret key. In this paper, we revisit the continued fraction technique and propose a new attack on RSA. Our main result shows that when $d < \sqrt{t\,(2\sqrt{2} + 8/3)}\; N^{.75}/\sqrt{e}$, where e is the public exponent and t is a chosen parameter, our attack can break the RSA with the running time of $O(t \log(N))$. Our attack is especially well suited for the case where e is much smaller than N. When $e \approx N$, the Boneh–Durfee attack outperforms ours. As a result, we could simultaneously run both attacks, our new attack and the classical Boneh–Durfee attack as a backup.

1. Introduction

The RSA cryptosystem is one of the most popular and de facto public-key encryption standard widely used for secure data transmission. It is among the most common ciphers used in the SSL/TLS protocol which allows sensitive information transmitted securely over the Internet.

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 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.

In some applications of RSA, it is desirable to have a short secret key d compared to the modulus N. However, it is well known that RSA is not secure if the secret key d is relatively small. The first significant attack [1] that breaks RSA with short secret key given by Wiener in 1990 is based on the continued fraction technique and it works [2,3] with $d < \frac{1}{\sqrt[4]{18}} N^{.25}$. Using an exhaustive search of about $8 + 2b$ bits, Verheul et al. [4] improved Wiener's bound to $d < 2^b N^{.25}$. Another exponential time attack similar to this is due to Dujella [5].

There are other variants of Wiener's attack but these attacks need more than just the public information (N, e). For example, the Weger attack [6] exploited the small distance between the two RSA's secret primes $|p - q|$. The Blomer attack [7] assumed a linear relation between e and $\phi(N)$: $ex + y = 0 \bmod \phi(N)$ with bounded x and y.

In 1999, Boneh and Durfee [8] showed the first significant improvement over the Wiener's result. Based on the Coppersmith technique, exploiting a non-linear equation satisfied by the secret exponent, the Boneh–Durfee method can break the RSA when $d < N^{.292}$. Using a somewhat more optimized lattice, Herrmann and May [9] also derived the same bound $d < N^{.292}$, although their proof is more elementary. This bound $d < N^{.292}$ remains as the best bound to date.

Our contributions In this paper, we will present an attack on the RSA cryptosystem. We show that if the public key e and the private key d are smaller than a certain bound then it is possible to efficiently perform the RSA number factorization and determine the private key. Our bound is different compared to Wiener's bound [1] and Boneh–Durfee's

* 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.csi.2020.103470
Received 29 April 2020; Received in revised form 1 July 2020; Accepted 7 September 2020
Available online 10 September 2020
0920-5489/

bound [8] in that it involves both the private key d and the public key e.

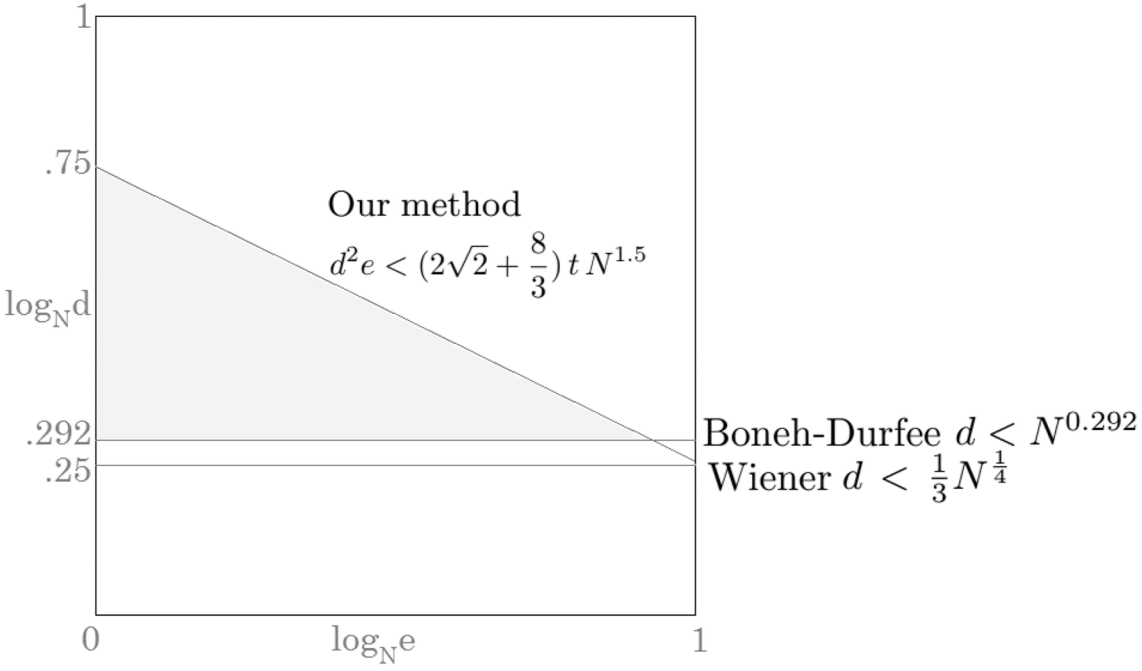
Our main result shows that when

$$d < \sqrt{t(2\sqrt{2} + 8/3)}\ N^{.75}/\sqrt{e},$$

where t is a chosen parameter, our attack can break the RSA with the running time of $O(t\log(N))$. The parameter t is an arbitrary positive integer. The larger the value of t the wider range of d can be attacked.

In some cases, our attack is weaker than the Boneh–Durfee attack, and in some cases, our attack performs better than the Boneh–Durfee one. In the following figure, the shaded part shows the area where our method is better than Wiener [1] and Boneh–Durfee[8].

As can be seen from the figure, our attack is especially well suited for the case where e is much smaller than N. When $e \approx N$, the Boneh–Durfee attack outperforms ours. As a result, we could simultaneously run both attacks, our new attack and the classical Boneh–Durfee attack as a backup.



The rest of the paper is organized as follows. In Section 2, we review some preliminary results on continued fractions. Section 3 outlines the main idea behind our new attack, namely (i) using a better approximation for $\frac{k}{d}$, and (ii) using a stronger version of the Legendre Theorem on continued fractions. Our main result is presented in Section 4. In Section 5, we show our experiment result with a 1024-bit modulus and 301-bit secret key. We conclude the paper in Section 6.

2. Preliminaries

In this section, we review the concept of continued fractions and the cryptanalysis technique based on continued fractions. The original Wiener attack[1] is based on the Legendre theorem [10]. Our new attack is based on a stronger version of the Legendre theorem which is due to Barbolosi and Jager [11].

2.1. Continued fractions

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 $\frac{1111}{2000}$.

By the Euclidean division algorithm, we have

$$\begin{aligned} 1111 &= 2000 \times \mathbf{0} + 1111 \\ 2000 &= 1111 \times \mathbf{1} + 889 \\ 1111 &= 889 \times \mathbf{1} + 222 \\ 889 &= 222 \times \mathbf{4} + 1 \\ 222 &= 1 \times \mathbf{222} \end{aligned}$$

and thus, we can see that the coefficients 0, 1, 1, 4, 222 determined by the above Euclidean division algorithm become the coefficients for the continued fraction as follows,

$$\begin{aligned} \frac{1111}{2000} &= \mathbf{0} + \frac{1111}{2000} = \mathbf{0} + \frac{1}{\frac{2000}{1111}} = \mathbf{0} + \frac{1}{\mathbf{1} + \frac{889}{1111}} = \mathbf{0} + \frac{1}{\mathbf{1} + \frac{1}{\frac{1111}{889}}} \\ &= \mathbf{0} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{1} + \frac{222}{889}}} = \mathbf{0} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{1} + \frac{1}{\frac{889}{222}}}} = \mathbf{0} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{4} + \frac{1}{\mathbf{222}}}}}. \end{aligned}$$

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

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

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 $c_0, c_1, \ldots, c_n$ 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 [10]*). *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 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:*

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

The following example shows how to calculate the convergents of the continued fraction of $\frac{1111}{2000}$. As previously shown, by the Euclidean division algorithm, we have the continued fraction

$$\frac{1111}{2000} = \mathbf{=0} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{4} + \frac{1}{\mathbf{222}}}}}.$$

with coefficients

$$x_0 = 0, \quad x_1 = 1, \quad x_2 = 1, \quad x_3 = 4, \quad x_4 = 222.$$

By using the Euler-Wallis Theorem, we calculate the numerator and the denominator sequences $\{a_i\}$ and $\{b_i\}$:

i	2	1	0	1	2	3	4
x_i			**0**	**1**	**1**	**4**	**222**
a_i	0	1	0	1	1	5	1111
b_i	1	0	1	1	2	9	2000

and obtain the following 5 convergents:

$$c_0 = \frac{a_0}{b_0} = \frac{0}{1}, \ c_1 = \frac{a_1}{b_1} = \frac{1}{1}, \ c_2 = \frac{a_2}{b_2} = \frac{1}{2}, \ c_3 = \frac{a_3}{b_3} = \frac{5}{9}, \ c_4 = \frac{a_4}{b_4} = \frac{1111}{2000}.$$

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

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

2.2. A stronger version of Legendre theorem

In 1994, Barbolosi and Jager [11] proved a stronger version of the Legendre Theorem which requires an additional constraint on the signature of $\frac{a}{b}$ with respect to $\frac{u}{v}$, which is defined as follows.

Definition 1. If

$$\frac{a}{b} = \alpha_0 + \frac{1}{\alpha_1 + \frac{1}{\ddots + \frac{1}{\alpha_m}}},$$

then we define

$$\ell\left(\frac{a}{b}\right) = (-1)^m$$

and

$$\epsilon\left(x, \frac{a}{b}\right) = \begin{cases} 1, & \text{for } x > \frac{a}{b} \\ 0, & \text{for } x = \frac{a}{b} \\ -1, & \text{for } x < \frac{a}{b} \end{cases}.$$

The signature of a rational number $\frac{a}{b}$ with respect to x is defined by

$$\delta\left(x, \frac{a}{b}\right) = \ell\left(\frac{a}{b}\right)\epsilon\left(x, \frac{a}{b}\right).$$

The following theorem due to Barbolosi and Jager [11] gives a stronger version of the Legendre Theorem which requires an additional constraint on the signature of $\frac{a}{b}$ with respect to $\frac{u}{v}$.

Theorem 4. *Barbolosi and Jager [11] Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$ such that*

$$\left|\frac{u}{v} - \frac{a}{b}\right| < \frac{2}{3b^2}$$

and $\delta(\frac{u}{v}, \frac{a}{b}) = 1$, then $\frac{a}{b}$ is equal to a convergent of the continued fraction of $\frac{u}{v}$.

The following observation is useful for our attack.

Theorem 5. *If*

$$\phi_0 < \frac{a}{b} < \phi_1$$

then

$$\delta\left(\phi_0, \frac{a}{b}\right) = 1 \ \text{ or } \ \delta\left(\phi_1, \frac{a}{b}\right) = 1,$$

i.e., the signature of $\frac{a}{b}$ with respect to either ϕ_0 or ϕ_1 is 1.

Proof. Since $\phi_0 < \frac{a}{b} < \phi_1$, we have

$$\epsilon\left(\phi_0, \frac{a}{b}\right) = -1 \ \text{ and } \ \epsilon\left(\phi_1, \frac{a}{b}\right) = 1.$$

Since $\ell\left(\frac{a}{b}\right)$ is 1 or -1, the two products

$$\delta\left(\phi_0, \frac{a}{b}\right) = \ell\left(\frac{a}{b}\right)\epsilon\left(\phi_0, \frac{a}{b}\right) \ \text{ and } \ \delta\left(\phi_1, \frac{a}{b}\right) = \ell\left(\frac{a}{b}\right)\epsilon\left(\phi_1, \frac{a}{b}\right)$$

have opposite signs, so one of the signatures $\delta\left(\phi_0, \frac{a}{b}\right)$ and $\delta\left(\phi_1, \frac{a}{b}\right)$ must be equal to 1. □

3. "Divide and capture" algorithm

In this section, we present a new technique of "divide and capture" to break RSA with short secret key. Our algorithm is an improvement of the Wiener attack.

Let us first recall the idea behind the original Wiener attack [1]. Since

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

we have

$ed - k\phi(N) = 1$

for some integer k, i.e. $ed \approx k\phi(N)$ 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 good *rational approximations* to the number, so in the Wiener attack, we search for $\frac{k}{d}$ among the convergents of the continued fraction of $\frac{e}{N}$. The Legendre Theorem is used to give a sufficient condition for $\frac{k}{d}$ to be a convergent of $\frac{e}{N}$, which is $d < \frac{1}{\sqrt[4]{18}}N^{.25}$.

Our new attack improves upon the Wiener attack by two ingredients. The first ingredient is that we use a better approximation for $\frac{k}{d}$, and the second ingredient is that we use a stronger version of the Legendre Theorem which is due to Barbolosi and Jager [11]. The two ingredients are employed in the following two steps of our algorithm: the "divide" step and the "capture" step.

The "divide" step Instead of using $\frac{e}{N}$ as an approximation for $\frac{k}{d}$ as in the original Wiener attack, we will use a better approximation. We show that we can narrow down the intervals for $\phi(N)$ and $\frac{k}{d}$ as follows:

$\phi(N) \in [\phi_{\min}, \phi_{\max}]$,

and

$$\frac{k}{d} \in \left[\frac{e}{\phi_{\max}}, \frac{e}{\phi_{\min}}\right],$$

where

$$\phi_{\min} = \left\lceil N - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} + 1 \right\rceil, \phi_{\max} = \lfloor N - 2N^{\frac{1}{2}} + 2 \rfloor.$$

Thus, if we **divide** the interval $\left[\frac{e}{\phi_{\max}}, \frac{e}{\phi_{\min}}\right]$ into t equal sub-intervals

$$\left[\frac{e}{\phi_{\max}}, \frac{e}{\phi_{\min}}\right] = [X_0, X_1] \cup [X_1, X_2] \cup ...\cup[X_{t-1}, X_t]$$

then $\frac{k}{d}$ must be in one of these intervals. By dividing the interval, those sub-interval end-points X_j are better approximations for $\frac{k}{d}$, and the larger value of t, the finer approximation it gets. The parameter t is chosen by our algorithm and our run-time depend linearly on t. Our main theorem shows that a larger value of t enable us to break a wider range of secret key d.

The "capture" step Similar to the Wiener attack, where we search for $\frac{k}{d}$ among the convergents of $\frac{e}{N}$. In our algorithm, by searching among the convergents of the sub-interval end-points X_j we **"capture"** $\frac{k}{d}$. We use a stronger version of the Legendre Theorem [11] to work out a sufficient condition for $\frac{k}{d}$ to be a convergent of X_j.

If $\frac{k}{d}$ is equal to a convergent $\frac{a_i}{b_i}$ of X_j. Then since $ed - k\phi(N) = 1$, we have

$\gcd(k, d) = 1$,

and by the identity (1) in Theorem 3, we also have

$\gcd(a_i, b_i) = 1$.

Therefore, if $\frac{k}{d} = \frac{a_i}{b_i}$, 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 X_j, 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 X_j, so for each $0 \le j \le t$, the run-time is $O(\log(N))$. Therefore, if $\frac{k}{d}$ is indeed equal to a convergent of the continued fraction of X_j as asserted by our main Theorem 7, then our algorithm will succeed to factor N and output p, q, d, k in $O(t\log(N))$ time complexity.

4. Our new attack

In this section, we present our new attack which is an improvement over the Wiener attack. Our algorithm has one parameter t, which is an arbitrary positive integer. The larger the value of t the wider range of d can be attacked. The running time is linearly depending on t. Specifically, we show that if

$$d^2e \lesssim (2\sqrt{2} + \frac{8}{3})\, t\, N^{1.5}$$

or equivalently,

$$d \lesssim \sqrt{2\sqrt{2} + \frac{8}{3}}\ \sqrt{t}\, N^{0.75}/\sqrt{e}$$

then we can determine the secret information p, q, d, k from the public parameter (e, N) in time complexity of $O(t\log(N))$.

We first need the following lemma.

Lemma 6. *Let t be a fixed positive integer. Define*

$$\phi_{\min} = \left\lceil N - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} + 1 \right\rceil, \quad \phi_{\max} = \lfloor N - 2N^{\frac{1}{2}} + 2 \rfloor,$$

If the following conditions are satisfied

- $q < p < 2q$
- $0 < e, d < \phi(N)$
- $ed - k\phi(N) = 1$

then

$$\frac{e}{\phi_{\max}} \le \frac{k}{d} < \frac{e}{\phi_{\min}}.$$

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

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

Hence,

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

Since $\phi(N) = N + 1 - (p + q)$, we have

$$N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} < \phi(N) < N + 1 - 2N^{\frac{1}{2}},$$

and since $\phi(N)$ is an integer, it follows that

$$\left\lceil N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} \right\rceil \le \phi(N) \le \lfloor N + 1 - 2N^{\frac{1}{2}} \rfloor.$$

From the definition of $\phi_{\min}$ and $\phi_{\max}$, we have the following bound for $\phi(N)$:

$$\phi_{\min} \le \phi(N) \le \phi_{\max} - 1.$$

It follows that

$$k\phi_{\min} < 1 + k\phi(N) \le k\phi_{\max}$$

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

Calculate

$$\phi_{\min} = \left\lceil N - \frac{3}{\sqrt{2}} N^{\frac{1}{2}} + 1 \right\rceil, \phi_{\max} = \left\lfloor N - 2N^{\frac{1}{2}} + 2 \right\rfloor.$$

for $0 \le j \le t$ **do**
  Calculate

$$X_j = \frac{e}{\phi_{\max}} + \frac{j}{t}\left(\frac{e}{\phi_{\min}} - \frac{e}{\phi_{\max}}\right)$$

  Run the Euclidean division algorithm to obtain the coefficients $x_0, x_1, \ldots, x_n$ of the continued fraction of X_j.
  Use the Euler-Wallis Theorem to calculate the convergents of X_j:

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

  for $0 \le i \le n$ **do**
    if $a_i | (eb_i - 1)$ **then**
      $\lambda_i = \dfrac{eb_i - 1}{a_i}$ ▷ $\lambda_i = \phi(N)$ 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
end for
return $\perp$ ▷ Fail to factorise N

Algorithm 1. "Divide and capture" algorithm based on continued fraction.

and since $ed = 1 + k\phi(N)$, we have

$k\phi_{\min} < ed \le k\phi_{\max}$

and so we have the following bound for $\frac{k}{d}$:

$$\frac{e}{\phi_{\max}} \le \frac{k}{d} < \frac{e}{\phi_{\min}}.$$

□

In our attack, instead of using the convergents of the continued fraction of $\frac{e}{N}$ as in the Wiener's original attack, we will use the convergents of the continued fraction of X_j where X_j is a better approximation of $\frac{e}{\phi(N)}$.

In the above lemma, $\frac{k}{d} \in \left[\frac{e}{\phi_{\max}}, \frac{e}{\phi_{\min}}\right]$. By dividing the interval $\left[\frac{e}{\phi_{\max}}, \frac{e}{\phi_{\min}}\right]$ into t equal sub-intervals
$[X_0, X_1] \cup [X_1, X_2] \cup \ldots \cup [X_{t-1}, X_t]$

and we contend that $\frac{k}{d}$ must be in one of this sub-interval. This narrow-down technique gives a better approximation for $\frac{k}{d}$.

This is our main theorem.

Theorem 7. *Let t be a fixed positive integer. Define*

$$\phi_{\min} = \left\lceil N - \frac{3}{\sqrt{2}} N^{\frac{1}{2}} + 1 \right\rceil, \phi_{\max} = \lfloor N - 2N^{\frac{1}{2}} + 2 \rfloor,$$

$$X_j = \frac{e}{\phi_{\max}} + \frac{j}{t}\left(\frac{e}{\phi_{\min}} - \frac{e}{\phi_{\max}}\right), 0 \le j \le t.$$

If the following conditions are satisfied

- $q < p < 2q$
- $0 < e, d < \phi(N)$
- $ed - k\phi(N) = 1$
- $d^2 e < \frac{2t\,\phi_{\min}\phi_{\max}}{3(\phi_{\max} - \phi_{\min})} \approx (2\sqrt{2} + \frac{8}{3})\, t\, N^{1.5}$

then $\frac{k}{d}$ is a convergent of X_j for some $j \in [0, t]$ and there is an algorithm with time complexity $O(t \log(N))$ that can determine the secret information p, q, d, k from the public parameter (e, N).

Proof. From the definition of X_j, we have

$$X_0 = \frac{e}{\phi_{\max}}, X_t = \frac{e}{\phi_{\min}}$$

and the interval $[X_0, X_t]$ is divided into t equal sub-intervals $[X_j, X_{j+1}]$ with $0 \le j \le t - 1$.

Since $\frac{k}{d} \in [X_0, X_t]$, it must belong to one of the sub-interval $[X_m, X_{m+1}]$. If $\frac{k}{d}$ is equal to one of the end points X_m or X_{m+1} then the theorem is proved, otherwise, we have $\frac{k}{d} \in (X_m, X_{m+1})$, and by Theorem 5,

$$\delta(X_m, \frac{k}{d}) = 1 \text{ or } \delta(X_{m+1}, \frac{k}{d}) = 1.$$

Suppose that $\delta(X_j, \frac{k}{d}) = 1$ where $j = m$ or $j = m + 1$. We also have

$$\left| X_j - \frac{k}{d} \right| < X_{m+1} - X_m = \frac{1}{t}\left(\frac{e}{\phi_{\min}} - \frac{e}{\phi_{\max}}\right) < \frac{2}{3d^2},$$

so by Theorem 4, $\frac{k}{d}$ is equal to a convergent of X_j.

Now, since $\frac{k}{d}$ is equal to a convergent of X_j, we need to go through the list of all convergents of X_j for each $0 \le j \le t$ to determine the secret information p, q, d, k. Since there are $t + 1$ such numbers X_i and each of these numbers X_i has $O(\log N)$ convergents, so the algorithm runs with time complexity $O(t \log N)$. □

5. Experiment result

In this experiment, we use a 1024-bit modulus N. With this 1024-bit modulus, the Wiener [1] upper bound $\frac{1}{3}N^{\frac{1}{4}}$ is 255-bit and the Boneh et al [8] upper bound $N^{0.292}$ is 300-bit. Here, we show an example of a 301-bit secret key d.

N= 1126684696 7960415267 9715205320 8764730377 0468843729 7602869626 8742679673 7565392691 1896720899 7817225421 9456563825 7598607299 8228483966 7277977750 0846524256 5405192174 3404715392 4111131445 2806998666 0800802542 6667428651 5822067868 3332139684 8178848647 1862041996 8307733888 2654976426 1652555778 0660037933 7429836710 469844689

e= 3546827515 0449892821 4645483994 9072354169 9917854105 3777881480 5556306506 8030441497 9123832858 1104189334 5269595865 1561530906 7787860350 8234271208 8372493244 0491567538 7082443615 0635715027 6983721999 4359528508 5507420733 6971847203 5998068636 3860035748 5766592157 1443573804 3230094162 2668134824 7084765906 3039

$\phi_{\min}$= 1126684696 7960415267 9715205320 8764730377 0468843729 7602869626 8742679673 7565392691 1896720899 7817225421 9456563825 7598607299 8228483966 7277977750 0846524256 5404967005 9338159387 5629893840 6790640806 5978949505 5190048763 1806998912 0018798869 8456552744 0343256918 0947602140 5998331016 7031165930 7924380180 5083193694 447678024

$\phi_{\max}$= 1126684696 7960415267 9715205320 8764730377 0468843729 7602869626 8742679673 7565392691 1896720899 7817225421 9456563825 7598607299 8228483966 7277977750 0846524256 5404979883 5307980122 5008117646 2984182057 4395408755 2375219678 2506148712 8274248859 4636262332 4878439474 0682918249 5327161306 0062525305 7397996939 6556133164 889091144

We are searching for $\frac{k}{d}$ among the convergents of X_i for $i \in [0, 2^{38}]$ and found it at the convergent $c_{153} = \frac{p_{153}}{q_{153}}$ of $X_{274877906943}$:

$k = p_{153}$= 6412632807 1602446527 2583222705 5821078117 6686722401 4569475530 8687145037 898787

$d = q_{153}$= 2037035976 3344860862 6844568840 9378161061 4683903318 9250127228 0898753762 5995266734 1973464393 9

which gives the factorization of N:

p= 1501122711 0373365654 1584030677 5719063214 5686914318 2532589343 3793042208 8938766481 5306021012 5233858240 0878317771 0969396414 2598981823 7718354897 7620106814 43971

q= 7505613555 1866828270 7920153387 8595316072 8434571591 2662946716 8965211044 4693832407 6530105062 6169291200 4391588855 4846982071 2994909118 8591774488 8100534072 2459

This experiment result shows that our usage of continued fractions of X_i is *essential*. If we use continued fractions of $\frac{e}{N}$ as in Wiener's original attack then no convergent c_i is found for which $c_i = \frac{k}{d}$.

6. Conclusion

In this paper, we revisit Wiener's continued fraction technique and propose a new attack on RSA. For a parameter t, our attack can break the RSA when

$$d < \sqrt{t\,(2\sqrt{2} + 8/3)}\; N^{.75}/\sqrt{e}$$

and the running time is $O(t \log(N))$. Our attack is especially well suited for the case where e is much smaller than N. When $e \approx N$, the Boneh–Durfee attack outperforms ours. It is an open problem to extend the attack to the case $e \approx N$ that goes beyond the Boneh–Durfee's bound.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Trans. Inf. Theory 36 (1990) 553–558.
[2] W. Susilo, J. Tonien, G. Yang, The Wiener attack on RSA revisited: a quest for the exact bound, Proceedings of the 24th Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science 11547, (2019), pp. 381–398.
[3] W. Susilo, J. Tonien, G. Yang, A generalised bound for the Wiener attack on RSA, J. Inf. Secur. Appl. 53 (2020) 102531.
[4] E. Verheul, H. van Tilborg, Cryptanalysis of 'less short' RSA secret exponents, Appl. Algebra Eng. Commun. Comput. 8 (1997) 425–435.
[5] A. Dujella, Continued fractions and RSA with small secret exponent, Tatra Mountains Math. Publ. 29 (2004) 101–112.
[6] B. de Weger, Cryptanalysis of RSA with small prime difference, Appl. Algebra Eng. Commun. Comput. 13 (2002) 17–28.
[7] J. Blömer, A. May, A generalized Wiener attack on RSA, Practice and Theory in Public Key Cryptography, Proceedings of PKC 2004, Lecture Notes in Computer Science 2947, (2004), pp. 1–13.
[8] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, IEEE Trans. Inf. Theory 46 (2000) 1339–1349.
[9] M. Herrmann, A. May, Maximizing small root bounds by linearization and applications to small secret exponent RSA, Public Key Cryptography 2010, Lecture Notes in Computer Science 6056, (2010), pp. 53–69.
[10] A.-M. Legendre, Essai sur la théorie des nombres, Duprat, Paris, An VI, 1798.
[11] D. Barbolosi, H. Jager, On a theorem of Legendre in the theory of continued fractions, J. Théorie Nombres Bordeaux 6 (1) (1994) 81–94.
[12] G. Hardy, E. Wright, An Introduction to the Theory of Numbers, sixth ed., Oxford University Press, 2008.