New weak RSA keys

Abderrahmane Nitaj Laboratoire de Mathmatiques Nicolas Oresme
Universit de Caen, France

nitaj@math.unicaen.fr

http://www.math.unicaen.fr/~nitaj

Abstract

Let $N = pq$ be an RSA modulus with $q < p < 2q$. In this paper, we analyze the security of RSA with the class of the exponents e satisfying an equation $eX - NY = ap + bq + Z$ with

$$|a| < q, \quad b = \left\lfloor \frac{ap}{q} \right\rfloor, \quad X < \frac{N}{3|ap+bq|} \quad \text{and} \quad |Z| < \frac{|ap-bq|}{3|ap+bq|} N^{\frac{1}{4}},$$

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x. Using the continued fraction algorithm and Coppersmith's lattice reduction method for solving polynomial equations, we show that such exponents lead to the factorization of N in polynomial time. Additionally, we show that the class of such weak exponents is large, namely that their number is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon > 0$ is a small constant depending only on N.

1 Introduction

1.1 Background

The RSA cryptosystem was invented by Rivest, Shamir, and Adleman [12] in 1978. It is currently the most widely known and widely used public key cryptosystem. RSA can be described by the modulus N which is the product of two large unknown primes p and q, and by the public exponent e and the private exponent d. The exponents e and d are related by $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N) = (p-1)(q-1)$ is Euler's totient function. In a normal RSA system, p and q have approximately the same number of bits. Thus, throughout this paper, we assume that $q < p < 2q$. In some applications of RSA, to reduce the decryption execution time (or signature-generation time), it is desirable to have a short secret exponent d. Unfortunately, based on the convergents of the continued fraction expansion of $\frac{e}{N}$, Wiener [15] showed in 1990 that the RSA system can be totally broken if $d < \frac{1}{3}N^{\frac{1}{4}}$. Wiener's attack is very efficient and the number of exponents for which this attack applies can be estimated as $N^{\frac{1}{4}-\varepsilon}$ where $\varepsilon > 0$ is arbitrary small for suitably large N. Since then, many generalizations of Wiener's attack have been proposed. In 1999, based on Coppersmith's lattice basis reduction method [4], Boneh and Durfee [3] improved Wiener's bound up to $d < N^{0.292}$. Similarly, the number of exponents for which this attack applies can be estimated as $N^{0.292-\varepsilon}$. Wiener's attack as well as its generalization by Boneh and Durfee are based on the RSA key equation

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

where k is a positive integer. In 2004, Blömer and May [2] proposed another generalization of Wiener's attack using the RSA variant equation

$$ex - k\phi(N) = y.$$

Applying the continued fraction algorithm and Coppersmith's method [4], they showed that the RSA modulus can be factored in polynomial time if the parameters x and y satisfy

$$x < \frac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad |y| = \mathcal{O}\left(N^{-\frac{3}{4}}ex\right).$$

Additionaly, Blömer and May proved that the number of such weak exponents is at least $N^{\frac{3}{4}-\varepsilon}$. At Africacrypt'2008, Nitaj [10] proposed another generalization of Wiener's attack by solving the RSA variant equation

$$eX - (p-u)(q-v)Y = 1,$$

with $1 \leq Y \leq X < 2^{-\frac{1}{4}}N^{\frac{1}{4}}$, $|u| < N^{\frac{1}{4}}$, $v = \left[-\frac{qu}{p-u}\right]$ ($[x]$ means the nearest integer to to the real number x) and such that the prime factors of $p-u$ or $q-v$ are less than 10^{50}. Applying successively the continued fraction algorithm, the Elliptic Curve Method of factorization (ECM [7]) and Coppersmith's method, he showed that such exponents are weak and that their number can be estimated as $N^{\frac{1}{2}-\varepsilon}$. In a similar direction, Maitra and Sarkar [8], studied the equation

$$eX - (N - pu - v)Y = 1,$$

using only the idea of Boneh and Durfee [3]. They showed that such exponents form a weak class of size $N^{\frac{3}{4}-\varepsilon}$. Recently, Nitaj [11] proposed an attack on RSA when the public exponent e satisfies an RSA variant equation

$$eX - (N - (ap + bq))Y = Z,$$

where $\frac{a}{b}$ is an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ and

$$Y \leq X < \frac{\sqrt{N}}{2\sqrt{ap+bq}}, \quad \gcd(X, Y) = 1,$$

and Z depends on the size of $|ap - bq|$. Using techniques from continued fractions, the Elliptic Curve Method and Coppersmith's method, he showed that such exponents lead to the factorization of N and that their number is at least $N^{\frac{3}{4}-\varepsilon}$.

1.2 Our contribution

Let e be an exponent and a an integer satisfying $|a| < q$. Define

$$b = \left\lfloor \frac{ap}{q} \right\rfloor,$$

where $\lfloor x \rfloor$ is the integer satisfying $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. It is obvious that there exist infinitely many integers X, Y and Z satisfying the equation

$$eX - NY = ap + bq + Z. \tag{1}$$

In this paper, we study the weaknesses of RSA given a public exponent e satisfying (1) with unknown a, b,

$$X < \frac{N}{3|ap+bq|} \quad \text{and} \quad |Z| < \frac{|ap-bq|}{3|ap+bq|} N^{\frac{1}{4}}.$$

As in Wiener's method, we use the continued fraction algorithm to find X and Y among the convergents of $\frac{e}{N}$. This gives us an approximation $S = |eX - NY|$ of $|ap+bq|$ with an additive error term at most $\frac{|ap-bq|}{3|ap+bq|} N^{\frac{1}{4}}$. Using the relation

$$(ap + bq)^2 = (ap - bq)^2 + 4abN,$$

we show that the product of a and b can be found as

$$ab = \left[\frac{S^2}{4N}\right],$$

where $[x]$ is the integer satisfying $-\frac{1}{2} \leq x - [x] < \frac{1}{2}$. Therefore, we transform S into an approximation $D = \sqrt{|S^2 - 4abN|}$ of $|ap - bq|$ with an additive error term at most $N^{\frac{1}{4}}$. Combining the two approximations, we find an approximation $\frac{1}{2}(S + D)$ of $|a|p$ with an error term at most $N^{\frac{1}{4}}$. By the seminal work of Coppersmith [4], we can then find p in polynomial time and the factorization of the RSA modulus follows.

Notice that, in Section 4.1.2 of the ANSI X9.31:1998 standard for public key cryptography, it is required in particular that the primes p and q of the RSA modulus shall be different in one at least of their most significant 100 bits. For such RSA modulus, we show that the number of the exponents e satisfying (1) with parameters within the desired bounds is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon > 0$ is suitably small for large N. This proves once again the existence of a large class of weak exponents in RSA.

1.3 Organization of the Paper

The rest of this paper is organized as follows. Section 2 presents definitions and known results from continued fractions and Coppersmith's method that we use. In section 3, we state and prove some lemmas required for the attack. In section 4, we present and prove our new attack on RSA. In section 5 we give an estimation of the size of the class of the exponents for which our attack applies. Section 6 concludes the paper.

2 Preliminaries on Continued Fractions and Coppersmith's Method

2.1 Continued Fractions

Every real number x has a unique continued fraction expansion

$$x = [a_0, a_1, a_2, \cdots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_m + \cdots}}}},$$

whose terms are given recursively by

$$x_0 = x, \quad a_k = \lfloor x_k \rfloor \quad \text{and} \quad x_{k+1} = \frac{1}{x_k - a_k} \quad \text{for} \quad k \geq 0.$$

If the continued fraction is finite, we write $x = [a_0, a_1, a_2, \cdots, a_m]$. It happens that x has one other continued fraction representation, namely

$$x = [a_0, a_1, a_2, \cdots, a_{m-1}, a_m - 1, 1],$$

but we will not use this. The rational number $r_n = [a_0, a_1, a_2, \cdots, a_n]$ is a fraction $\frac{p_n}{q_n}$ in lowest term, called the n-th *convergent* of x. It is well known that p_n and q_n satisfy various properties and can be computed using the recurrences

$$\begin{aligned} p_{-2} &= 0, \quad p_{-1} = 1, \quad p_n = a_n p_{n-1} + p_{n-2}, \; n \geq 0. \\ q_{-2} &= 1, \quad q_{-1} = 0, \quad q_n = a_n q_{n-1} + q_{n-2}, \; n \geq 0. \end{aligned}$$

As in Wiener's attack, we will use the following result (see [5], Theorem 184).

Theorem 2.1. *Let $x = [a_0, a_1, a_2, \cdots]$ be the continued fraction expansion of x. If X and Y are coprime integers such that*

$$\left| x - \frac{Y}{X} \right| < \frac{1}{2X^2},$$

then $Y = p_n$ and $X = q_n$ for some convergent $\frac{p_n}{q_n}$ of x with $n \geq 0$.

2.2 Coppersmith's Method

In 1996, Coppersmith [4] introduced methods of finding small modular solutions of univariate polynomial equations $f(x) \equiv 0 \pmod{N}$ for some composite integer N with unknown factorization, and finding small integer solutions of bivariate integer polynomial equations $f(x, y) = 0$. Since then, the methods have found many applications in cryptanalysis. As an important application of the bivariate case, Coppersmith presented a solution to the following problem: The knowledge of half of the most significant bits of p is sufficient to find the factorization of an RSA modulus $N = pq$ in polynomial time. Here, we present a generalization of this problem. Let $N = pq$ and suppose we are given an approximation $\widetilde{p}$ to kp such that $kp = \widetilde{p} + x_0$ where $|x_0| < N^{\frac{1}{4}}$ and k is an unknown integer satisfying $\gcd(k, q) = 1$. Coppersmith used his ideas to get an algorithm for finding p given $k = 1$ and $\widetilde{p}$. Coppersmith originally used the bivariate polynomial method, but simpler versions were later presented by Howgrave-Graham [6] and May (Theorem 10 of [9]).

Theorem 2.2. *Let $N = pq$ with $p > q$. Furthermore, let k be an (unknown) integer that is not a multiple of q. Suppose we know an approximation $\widetilde{p}$ of kp with*

$$|kp - \widetilde{p}| < 2N^{\frac{1}{4}}.$$

Then we can find the factorization of N in time polynomial in $\log N$.

3 Useful Lemmas

In this section, we state and prove some lemmas that we will use in the new approach.

Lemma 3.1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then*

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}.$$

Proof. Assume $q < p < 2q$. Then multiplying by p we get $N < p^2 < 2N$. This gives $\sqrt{N} < p < \sqrt{2}\sqrt{N}$. Hence, since $q = \frac{N}{p}$, then

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N},$$

which terminates the proof. □

A key role in our arguments is played by the following lemma. Recall that the integer closest to x is denoted $[x]$ and the integer floor of x is denoted $\lfloor x \rfloor$.

Lemma 3.2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and a a positive integer. Define $b = \left\lfloor \frac{ap}{q} \right\rfloor$. Let S be an approximation of $ap + bq$ such that*

$$|ap + bq - S| < \frac{|ap - bq|}{3(ap + bq)} N^{\frac{1}{4}}.$$

Then

$$ab = \left[\frac{S^2}{4N} \right],$$

and $\sqrt{|S^2 - 4abN|}$ is an approximation of $|ap - bq|$ satisfying

$$\left| |ap - bq| - \sqrt{|S^2 - 4abN|} \right| < N^{\frac{1}{4}}.$$

Proof. Set $S = ap + bq + x$ with $|x| < \frac{|ap-bq|}{3(ap+bq)} N^{\frac{1}{4}}$. Then

(2)$S^2 - 4abN = (ap + bq + x)^2 - 4abN = (ap - bq)^2 + 2(ap + bq)x + x^2$

Next, suppose $b = \left\lfloor \frac{ap}{q} \right\rfloor$. Then $bq \le ap < bq + q$ and, using Lemma 3.1, this gives $0 \le ap - bq < q < \sqrt{N}$. Thus, using the bounds $|x| < \frac{|ap-bq|}{3(ap+bq)} N^{\frac{1}{4}} < N^{\frac{1}{4}}$, the right side of (2) satisfies

$$\begin{aligned}
\left| (ap - bq)^2 + 2(ap + bq)x + x^2 \right| &\le (ap - bq)^2 + 2(ap + bq)|x| + x^2 \\
&\le N + 2(ap + bq) \frac{|ap - bq|}{3(ap + bq)} N^{\frac{1}{4}} + N^{\frac{1}{2}} \\
&< N + \frac{2}{3} N^{\frac{3}{4}} + N^{\frac{1}{2}} \\
&< 2N.
\end{aligned}$$

It follows that the left side of (2) satisfies $|S^2 - 4abN| < 2N$. Thus

$$\left| \frac{S^2}{4N} - ab \right| = \frac{|S^2 - 4abN|}{4N} < \frac{2N}{4N} = \frac{1}{2},$$

which implies that $ab = \left[\frac{S^2}{4N} \right]$. To prove the second statement of the lemma, observe that

$$\left| (ap - bq)^2 - \left| S^2 - 4abN \right| \right| \le \left| (ap - bq)^2 - \left(S^2 - 4abN \right) \right| = \left| (ap + bq)^2 - S^2 \right|.$$

This implies that

$$\begin{aligned}\left||ap-bq|-\sqrt{|S^2-4abN|}\right| &= \frac{|(ap+bq)^2-S^2|}{|ap-bq|+\sqrt{|S^2-4abN|}}\\ &\leq \frac{|ap+bq-S|\,(ap+bq+S)}{|ap-bq|}.\end{aligned}$$

By assumption, we have $|ap+bq-S| < \frac{|ap-bq|}{3(ap+bq)}N^{\frac{1}{4}}$. This implies

$$ap+bq+S < 2(ap+bq)+\frac{|ap-bq|}{3(ap+bq)}N^{\frac{1}{4}} < 3(ap+bq),$$

and leads to

$$\frac{|ap+bq-S|\,(ap+bq+S)}{|ap-bq|} < \frac{3(ap+bq)|ap-bq|N^{\frac{1}{4}}}{3(ap+bq)|ap-bq|} = N^{\frac{1}{4}}.$$

Hence, we deduce

$$\left||ap-bq|-\sqrt{|S^2-4abN|}\right| < N^{\frac{1}{4}},$$

which terminates the proof. □

For counting the exponents for which our attack applies, we need the following result.

Lemma 3.3. *Let m and n be positive integers. Then*

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{m} 1 > \frac{cm}{(\log\log n)^2},$$

where c is a positive constant.

Proof. For a positive integer d, we denote by $\mu(d)$ be the Möbius function. This function is defined by

$$\mu(d)=\begin{cases}1, & \text{if } d=1,\\ (-1)^{\omega(d)}, & \text{if } d \text{ is square free},\\ 0, & \text{otherwise,}\end{cases}$$

where, for an integer $d \geq 2$, $\omega(d)$ is the number of distinct prime factors of d. Using the Legendre formula, we get

$$\begin{aligned}
\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{m} 1 &= \sum_{d|n} \mu(d) \left\lfloor \frac{m}{d} \right\rfloor \\
&= \sum_{\substack{d|n\\ \mu(d)=1}} \left\lfloor \frac{m}{d} \right\rfloor - \sum_{\substack{d|n\\ \mu(d)=-1}} \left\lfloor \frac{m}{d} \right\rfloor \\
&\geq \sum_{\substack{d|n\\ \mu(d)=1}} \left(\frac{m}{d} - 1 \right) - \sum_{\substack{d|n\\ \mu(d)=-1}} \frac{m}{d} \\
&= \sum_{d|n} \mu(d) \frac{m}{d} - \sum_{\substack{d|n\\ \mu(d)=1}} 1.
\end{aligned}$$

This leads to

$$\begin{aligned}
\omega(n) \sum_{\substack{k=1\\ \gcd(k,n)=1}}^{m} 1 &\geq \sum_{\substack{k=1\\ \gcd(k,n)=1}}^{m} 1 + \sum_{\substack{d|n\\ \mu(d)=1}} 1 \\
&\geq \sum_{d|n} \mu(d) \frac{m}{d} \\
&= m \sum_{d|n} \frac{\mu(d)}{d}.
\end{aligned}$$

For $n > 1$, we recall that $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\phi(n)}{n}$ (see 16.3.1 of [5]). Hence

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{m} 1 > \frac{m\phi(n)}{n\omega(n)}.$$

On the other hand, it is well known that $\frac{\phi(n)}{n} > \frac{c_1}{\log\log n}$ (see Theorem 328 of [5] or [14]) and $\omega(n) = c_2 \log\log n$ (Theorems 430-431 of [5]) where c_1, c_2

are positive constants. It follows that

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{m} 1 > \frac{c_1 m}{c_2(\log\log n)^2} = \frac{cm}{(\log\log n)^2},$$

where $c = \frac{c_1}{c_2}$ and the lemma follows. □

4 The New Attack on RSA

Let e be an exponent satisfying an equation $eX - NY = ap + bq + Z$. In this section, under certain constraints on a, b, X and Z, we show that, using e and N, one can find the factorization of N in polynomial time. The following lemma enables us to find X and Y among the convergents of the continued fraction expansion of $\frac{e}{N}$.

Lemma 4.1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that e is an exponent satisfying an equation*

$$eX - NY = ap + bq + Z,$$

with $\gcd(X, Y) = 1$ *and*

$$X < \frac{N}{3|ap + bq|} \quad \text{and} \quad |Z| < \frac{|ap - bq|}{3|ap + bq|} N^{\frac{1}{4}}.$$

Then $\frac{Y}{X}$ is a convergent of $\frac{e}{N}$.

Proof. Assume that $|Z| < \frac{|ap-bq|}{3(ap+bq)} N^{\frac{1}{4}}$. Then $|Z| < N^{\frac{1}{4}}$. Assume additionally that $X < \frac{N}{3|ap+bq|}$. Starting with the equation $eX - NY = ap + bq + Z$, we get

$$\left| \frac{e}{N} - \frac{Y}{X} \right| = \frac{|ap + bq + Z|}{NX} \leq \frac{|ap + bq| + |Z|}{NX} \leq \frac{|ap + bq| + N^{\frac{1}{4}}}{NX}.$$

So if the condition $\frac{|ap+bq|+N^{\frac{1}{4}}}{NX} < \frac{1}{2X^2}$ holds, then by Theorem 2.1, we conclude that $\frac{Y}{X}$ is one of the convergents of the continued fraction expansion of $\frac{e}{N}$. This is equivalent to

$$X < \frac{N}{2\left(|ap + bq| + N^{\frac{1}{4}}\right)},$$

which is satisfied if $X < \frac{N}{3|ap+bq|}$. □

Notice that the continued fraction algorithm is polynomial time and that the number of convergents of $\frac{e}{N}$ is at most $\mathcal{O}(\log N)$. Thus, the method of Lemma 4.1 is very efficient to find the parameters X and Y in the equation $eX - NY = ap + bq + Z$. The following result shows how to solve completely the equation and proves the new attack on RSA.

Theorem 4.2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that e is an exponent satisfying an equation*

$$eX - NY = ap + bq + Z,$$

with $|a| < q$, $\gcd(X, Y) = 1$ and

$$X < \frac{N}{3|ap + bq|} \quad \text{and} \quad |Z| < \frac{|ap - bq|}{3|ap + bq|} N^{\frac{1}{4}},$$

where $b = \left\lfloor \frac{ap}{q} \right\rfloor$. Then N can be factored in polynomial time.

Proof. Suppose e satisfies an equation $eX - NY = ap + bq + Z$ and X and Z satisfy the conditions of Lemma 4.1, then $\frac{Y}{X}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$. Using X and Y, define $S = eX - NY$. Then S is an approximation of $ap + bq$ satisfying

$$|ap + bq - S| = |Z| < \frac{|ap - bq|}{3|ap + bq|} N^{\frac{1}{4}}.$$

Then Lemma 3.2 implies that $ab = \left[\frac{S^2}{4N}\right]$, and $D = \sqrt{|S^2 - 4abN|}$ is an approximation of $|ap - bq|$ with $||ap - bq| - D| < N^{\frac{1}{4}}$. Using S and D we get

$$\left| ap - \frac{S \pm D}{2} \right| < N^{\frac{1}{4}}.$$

Then Coppersmith's Theorem 2.2 with one of the values $\frac{S+D}{2}$ and $\frac{S-D}{2}$ will find p in polynomial time and the factorization of N follows. □

Now we summarize the factorization algorithm.

Algorithm 1 : The factorization algorithm

```
Input: An RSA modulus $N = pq$ with $q < p < 2q$ and a public exponent $e$
    satisfying $eX - NY = ap + bq + Z$ with $|a| < q$, $b = \left\lfloor \frac{ap}{q} \right\rfloor$, $X < \frac{N}{3|ap+bq|}$
    and $|Z| < \frac{|ap-bq|}{3|ap+bq|} N^{\frac{1}{4}}$.
Output: The prime factors $p$ and $q$.
Compute the continued fraction expansion of $\frac{e}{N}$.
For every convergent $\frac{Y}{X}$ of $\frac{e}{N}$ do
    If $X < \frac{1}{3} N^{\frac{1}{2}}$ then
        Compute $S = eX - NY$, $k = \left[\frac{S^2}{4N}\right]$ and $D = \sqrt{|S^2 - 4kN|}$.
        Apply Coppersmith's algorithm (Theorem 2.2) with $\frac{S+D}{2}$ and $\frac{S-D}{2}$.
        If Coppersmith's algorithm succeeds then
            Outputs the factors $p$ and $q$.
            Stop.
        End if
    End if
End for
```

5 Estimation of the Weak Exponents

In this section, we give an estimation of the number of the exponents $e < N$ for which our approach applies. We begin by showing, that for a fixed a with $|a| < q$, an exponent $e < N$ satisfies at most one equation $eX - NY = ap + bq + Z$ where the parameters X, Y and Z satisfy the conditions of Theorem 4.2.

Lemma 5.1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that e is an exponent satisfying two equations*

$$eX - NY = ap + bq + Z \qquad \text{and} \qquad eX' - NY' = ap + bq + Z',$$

with $|a| < q$,

$$X, X' < \frac{N}{3|ap + bq|}, \quad \text{and} \quad |Z|, |Z'| < \frac{|ap - bq|}{3|ap + bq|} N^{\frac{1}{4}},$$

where $b = \left\lfloor \frac{ap}{q} \right\rfloor$. Then $X = X'$, $Y = Y'$ and $Z = Z'$.

Proof. Assume that $eX - NY = ap + bq + Z$ and $eX' - NY' = ap + bq + Z'$. Then eliminating e, we get

$$\frac{NY + ap + bq + Z}{X} = \frac{NY' + ap + bq + Z'}{X'},$$

which is equivalent to

$$(ap + bq)(X' - X) + ZX' - Z'X = N(XY' - X'Y). \tag{3}$$

Next, assume $X, X' < \frac{N}{3|ap+bq|}$ and $|Z|, |Z'| < \frac{|ap-bq|}{3|ap+bq|} N^{\frac{1}{4}}$. Then

$$\begin{aligned} |(ap + bq)(X' - X) + ZX' - Z'X| &\leq |ap + bq|(|X| + |X'|) + |ZX'| + |Z'X| \\ &< \frac{2N}{3} + \frac{2|ap - bq|N^{\frac{5}{4}}}{9|ap + bq|^2} \\ &< \frac{2N}{3} + \frac{2N^{\frac{3}{4}}}{3} \\ &< N, \end{aligned}$$

where we used $|ap + bq| > p > N^{\frac{1}{2}}$ and $|ap - bq| < |ap + bq|$. Plugging this in (3), we get $XY' = X'Y$ and $(ap + bq)(X' - X) + ZX' - Z'X = 0$. Since $\gcd(X, Y) = 1$ and $\gcd(X', Y') = 1$, this leads to $X = X'$, $Y = Y'$ and finally $Z = Z'$. □

Now we give an estimation of the size of the class of the exponents for which our approach applies.

Theorem 5.2. *Let $N = pq$ be a normal RSA modulus with $q < p < 2q$ and $p - q > 2^{-100}\sqrt{N}$. The number of the exponents $e < N$ satisfying an equation $eX - NY = ap + bq + Z$ with* $\gcd(X, Y) = 1$*, $|a| < q$ and*

$$b = \left\lfloor \frac{ap}{q} \right\rfloor, \qquad X < \frac{N}{3|ap + bq|} \quad \text{and} \quad |Z| < \frac{|ap - bq|}{3|ap + bq|} N^{\frac{1}{4}},$$

is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon > 0$ is arbitrary small for suitably large N.

Proof. Suppose that the exponent e satisfies an equation $eX - NY = ap + bq + Z$ with $\gcd(X, Y) = 1$ and $X < \frac{N}{3|ap+bq|}$. Then, since $X < \frac{1}{3}N^{\frac{1}{2}}$, we have $X < q$ and $\gcd(X, N) = 1$. Hence we can express e as

$$e \equiv \frac{ap + bq + Z}{X} \pmod{N}.$$

Additionally, if $e < N$, then this representation is unique. This implies that the number of such exponents is

$$\mathcal{N}(a) = \sum_{|Z|=1}^{B_1} \sum_{\substack{X=1 \\ \gcd(X,ap+bq+Z)=1}}^{B_2} 1, \tag{4}$$

where

$$B_1 = \left\lfloor \frac{|ap-bq|}{3|ap+bq|} N^{\frac{1}{4}} \right\rfloor \quad \text{and} \quad B_2 = \left\lfloor \frac{N}{3|ap+bq|} \right\rfloor .$$

Using Lemma 3.3 with $m = B_2$ and $n = ap + bq + Z$, we get

$$\sum_{\substack{X=1 \\ \gcd(X,ap+bq+Z)=1}}^{B_2} 1 > \frac{cB_2}{(\log\log|ap+bq+Z|)^2} > \frac{cB_2}{(\log\log N)^2} = B_2 N^{-\varepsilon_1},$$

where $c > 0$ is a constant and $\varepsilon_1 > 0$ is arbitrary small for suitably large N. Plugging this in (4), we deduce

$$\mathcal{N}(a) > \sum_{|Z|=1}^{B_1} B_2 N^{-\varepsilon_1} = 2B_2B_1N^{-\varepsilon_1} = 2\left\lfloor \frac{|ap-bq|}{3|ap+bq|} N^{\frac{1}{4}} \right\rfloor \left\lfloor \frac{N}{3|ap+bq|} \right\rfloor N^{-\varepsilon_1}.$$

Let us consider the case with $a = 1$. Since $q < p < 2q$, then $b = \left\lfloor \frac{ap}{q} \right\rfloor = 1$. We also consider the case where the primes p and q satisfy $p - q > 2^{-100}\sqrt{N}$, as required by the the ANSI X9.31 standard [1] (see also [13]). This results in the following lower bound for $\mathcal{N}(1)$

$$\begin{aligned}
\mathcal{N}(1) &> 2\left\lfloor \frac{|p-q|}{3|p+q|} N^{\frac{1}{4}} \right\rfloor \left\lfloor \frac{N}{3(p+q)} \right\rfloor N^{-\varepsilon_1} \\
&> 2\left\lfloor \frac{2^{-100}\sqrt{N}N^{\frac{1}{4}}}{6\sqrt{2}\sqrt{N}} \right\rfloor \left\lfloor \frac{N}{6\sqrt{2}\sqrt{N}} \right\rfloor N^{-\varepsilon_1} \\
&> \frac{2^{-100}N^{\frac{1}{4}}}{6\sqrt{2}} \times \frac{\sqrt{N}}{6\sqrt{2}} \times N^{-\varepsilon_1} \\
&= N^{\frac{3}{4}-\varepsilon},
\end{aligned}$$

where we used $p+q < 2p < 2\sqrt{2}\sqrt{N}$ and $\varepsilon > 0$ is arbitrary small for suitably large N. This terminates the proof. □

6 Conclusion

Based on the equation $ed - k\phi(N) = 1$, Wiener's famous attack on RSA with $d < \frac{1}{3}N^{\frac{1}{4}}$ shows that using a small private exponent d for an efficient decryption (or signature-generation) process makes RSA completely insecure. In this paper, we studied the class of the exponents e satisfying an equation $eX - NY = ap + bq + Z$ where a is an unknown integer satisfying $|a| < q$ and $b = \left\lfloor \frac{ap}{b} \right\rfloor$ and where X and Z are suitably small parameters. Using the continued fraction algorithm and Coppersmith's method, we showed that such exponents are weak as they enable us to break the RSA system. Additionally, we showed that they form a class of size $N^{\frac{3}{4}-\varepsilon}$ which is approximately $\sqrt{N}$ times more larger than Wiener's class of weak exponents. This shows that instances of RSA, even with large private exponents, can be insecure as they can efficiently be recovered.

References

[1] ANSI Standard X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).

[2] J. Blömer and A. May, A generalized Wiener attack on RSA, In Public Key Cryptography – PKC 2004, volume 2947 of Lecture Notes in Computer Science, pp. 1–13. Springer-Verlag (2004)

[3] D. Boneh and G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology – Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, 1–11 (1999)

[4] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *Journal of Cryptology*, 10(4), 233–260 (1997)

[5] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, London (1965)

[6] N. Howgrave–Graham, Approximate integer common divisors, Cryptography and Lattices, CaLC 2001 (J.H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 51–66.

[7] H.W. Lenstra, Factoring integers with elliptic curves, *Annals of Mathematics*, vol. 126, 649–673 (1987)

[8] S. Maitra and S. Sarkar, A New Class of Weak Encryption Exponents in RSA, In: D.R. Chowdhury and V. Rijmen (eds.) INDOCRYPT 2008, LNCS, vol. 5365, pp. 337–349. Springer–Verlag Berlin Heidelberg 2008

[9] A. May, New RSA Vulnerabilities Using Lattice Reduction Methods, Ph.D. thesis, Paderborn, 2003, `http://www.informatik.tu-darmstadt.de/KP/publications/03/bp.ps`

[10] A. Nitaj, Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 174–190. Springer–Verlag Berlin Heidelberg 2008

[11] A. Nitaj, Cryptanalysis of RSA using the ratio of the primes, In: B. Preneel (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 98–115. Springer–Verlag Berlin Heidelberg 2009

[12] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, Vol. 21 (2), 120–126 (1978)

[13] R.D. Silverman, Fast generation of random, strong RSA primes, *CryptoBytes*, Vol. 3, No. 1 (1997) pp. 9–13.

[14] E.W. Weisstein, Totient Function, From MathWorld - AWolframWeb Resource. `http://mathworld.wolfram.com/TotientFunction.html`

[15] M. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Transactions on Information Theory*, Vol. 36, 553–558 (1990)