New vulnerabilities in RSA

Abderrahmane Nitaj

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, France
nitaj@math.unicaen.fr
http://www.math.unicaen.fr/~nitaj

Abstract. Let $N = pq$ be the product of two large unknown primes of equal bit-size. Wiener's famous attack on RSA shows that using a public key (N, e) satisfying $ed - k(N + 1 - (p + q)) = 1$ with $d < \frac{1}{3}N^{1/4}$ makes RSA completely insecure. The number of such weak keys can be estimated as $N^{\frac{1}{4}-\varepsilon}$. In this paper, we present a generalization of Wiener's attack. We study two new classes of exponents satisfying an equation

$$eX - \left(N - \left(up \pm \frac{q}{u}\right)\right) Y = Z,$$

where X, Y are suitably small integers, u is an integer with $|u| < \frac{1}{2}q$ and Z is a small rational. Using a combination of the continued fraction algorithm and Coppersmith's lattice based technique for solving polynomial equations, we show that every exponent e in these classes yields the factorization of N. Moreover, we show that the number of such exponents is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for large N when p and q satisfy $|p - q| = \Omega\left(\sqrt{N}\right)$.

KEYWORDS: RSA, Cryptanalysis, Factorization, Continued Fraction, Coppersmith's method

1 Introduction

The RSA algorithm [14] was invented by Rivest, Shamir and Adleman in 1977 and has withstood years of extensive cryptanalysis (see e.g. [3]). It is still the most widely deployed and used public-key cryptosystem. Let $N = pq$ be the product of two large primes p, q of the same bit-size and let e and d be positive integers satisfying $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N) = (p - 1)(q - 1)$ is Euler's totient function. Thus, e and d satisfy the RSA key equation $ed - k\phi(N) = 1$, where k is some positive integer. The integer N is called the RSA modulus, e is the public (encrypting) exponent and d is the private (decrypting) exponent.

The security of RSA is based on the hardness of factoring the modulus N and computing roots modulo N. A survey on the attacks on RSA before the year 2000 is available in [3]. Many attacks tried to solve the key equation $ed - k\phi(N) = 1$. Indeed, trying to break RSA by finding d, the decryption key, or computing $\phi(N)$ amounts to factoring N in the end. In 1990, using information obtained from the continued fraction expansion of $\frac{e}{N}$, Wiener [15] showed how to efficiently factor the modulus $N = pq$ for any instance of RSA with private exponent d satisfying $d < \frac{1}{3}N^{\frac{1}{4}}$. The number of such weak exponents can be estimated as $N^{\frac{1}{4}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for large N. At Eurocrypt'99, Boneh and Durfee [4] improved the bound, by showing that p and q can be recovered in polynomial time if $d < N^{0.292}$. The attack is based on the lattice-based work by Coppersmith [5] on finding small roots to modular polynomial equations. The number of the exponents for which this method works can be estimated as $N^{0.292-\varepsilon}$.

Other cryptanalytic ideas have been based on some variants of the RSA key equation. In 2004, Blömer and May [2] showed that p, q can be found in polynomial time for every (N, e) satisfying $ex + y = k\phi(N)$ with $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| = \mathcal{O}\left(N^{-\frac{3}{4}}ex\right)$. This attack is based on the continued fraction algorithm and on Coppersmith's method [5] for finding small roots of modular polynomial equations. The number of such weak exponents is estimated as $N^{\frac{3}{4}-\varepsilon}$ when p and q satisfy $|p - q| = \Omega\left(\sqrt{N}\right)$. Another attack was presented by Maitra and Sarkar [10] in 2008. The attack applies the continued fraction algorithm to various $\frac{e}{\phi'(N)}$ where $\phi'(N)$ is an approximation of $\phi(N)$. Recently, Nitaj [12] proposed another attack on RSA using the equation $eX + \phi(N)Y = NZ$. He showed that it is possible to find X and $Z - Y$ using the continued fraction algorithm if $XY < \frac{\sqrt{2}}{6}N^{\frac{1}{2}}$. Then Y and Z can be found using Coppersmith's technique [5] if $p-q < N^{\frac{3}{8}}$ and this leads to the factorization of N. The number of the exponents for which this method works is estimated as $N^{\frac{1}{2}-\varepsilon}$. Very recently, Nitaj [13] studied the equation $eX - (N - (ap + bq))Y = Z$ where $\frac{a}{b}$ is an unknown convergent of the continued fraction expansion of $\frac{q}{p}$. Using similar techniques and the Elliptic Curve Method of factorization (ECM) [8], he showed that N can be factored efficiently if $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ where α is defined by $|ap + bq| = N^{\frac{1}{2}+\alpha}$. He showed that the number of the exponents for which this attack applies is at least $N^{\frac{3}{4}-\varepsilon}$.

In this paper, we introduce two new attacks on RSA. The first attack works for all exponents satisfying an equation

$$eX - \left(N - \left(pu + \frac{q}{u}\right)\right)Y = Z,$$

with $1 \leq |u| < \frac{1}{2}q$ and

$$\gcd(X, Y) = 1, \quad XY < \frac{N}{4\left|pu + \frac{q}{u}\right|}, \quad |Z| < \frac{p-q}{3(p+q)}Y.$$

Observe that, when $u = 1$, the equation becomes

$$eX - (N - (p+q))\,Y = Z,$$

or equivalently $eX + Y - Z = Y\phi(N)$, with suitably small integers X, Y and $|Z - Y|$ which is similar to the equation studied by Blömer and May [2]. Hence, our new attack is an extension of the attack of Blömer and May, and consequently a generalization of Wiener's attack [15]. Our new attack is based on the continued fraction algorithm and Coppersmith's technique. We show that for integers X, Y and Z within the given bounds, the attack yields the factorization of the RSA modulus $N = pq$.

Let $[x]$ denote the nearest integer to x. For every integer u with $|u| < \frac{1}{2}q$, we show that the class of the exponents e with the structure

$$e = \left[\frac{\left(N - \left(pu + \frac{q}{u}\right)\right) Y}{X} \right] + z,$$

and

$$\gcd(X, Y) = 1, \quad X \leq Y < \frac{\sqrt{N}}{2\sqrt{\left|pu + \frac{q}{u}\right|}}, \quad |z| < \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} - \frac{1}{2},$$

is vulnerable by our attack. When p and q satisfy $|p-q| = \Omega\left(\sqrt{N}\right)$, we also show that the number of such exponents is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for large N which is large comparatively to the number of weak exponents in Wiener's attack.

In a similar direction, the second attack works for all exponents e satisfying an equation

$$eX - \left(N - \left(pu - \frac{q}{u}\right)\right) Y = Z,$$

with

$$\gcd(X, Y) = 1, \quad XY < \frac{N}{4\left|pu - \frac{q}{u}\right|}, \quad |Z| < N^{\frac{1}{4}} Y.$$

We show that such exponents yield the factorization of $N = pq$. As an application, we show that the exponents with the structure

$$e = \left[\left(N - \left(pu - \frac{q}{u}\right)\right) \frac{Y}{X} \right] + z,$$

where $|u| < \frac{1}{2}q$ and

$$\gcd(X, Y) = 1, \quad X < Y < \frac{\sqrt{N}}{2\sqrt{\left|pu - \frac{q}{u}\right|}}, \quad |z| < N^{\frac{1}{4}},$$

are weak and that the number of such exponents is at least $N^{\frac{3}{4}-\varepsilon}$.

The new attacks work as follows. We use the continued fraction algorithm to recover X and Y among the convergents of $\frac{e}{N}$. Using X and Y, we show that $N - \frac{eX}{Y}$ is an approximation of $pu + \frac{p}{u}$ (respectively $pu - \frac{p}{u}$). Then we find an approximation of $pu - \frac{p}{u}$ (respectively $pu + \frac{p}{u}$) and therefore an approximation of pu. The approximations are up to additive terms at most $N^{\frac{1}{4}}$. Afterwards, we find

p and q using Coppersmith's lattice based method. This yields the factorization of N.

The remainder of this paper is organized as follows. In Section 2, we begin with some notations and a brief review of basic facts about the continued fraction algorithm and Coppersmith's method. In Section 3, we present some useful lemmas needed for the attack. In Section 4 we present our first attack on RSA and estimate the size of the exponents that are weak for this attack. Similarly, in Section 5 we present our second attack and estimate the size of the weak exponents. Finally, we conclude in Section 6.

2 Preliminaries

We first introduce some notation. We use the notation $[x]$ to denote the integer closest to the real number x and $\lfloor x \rfloor$ to denote the largest integer less than or equal to x.

2.1 The Continued Fraction Algorithm

Let $x \neq 0$ be a real number. Put

$$x_0 = x, \quad a_0 = \lfloor x_0 \rfloor.$$

Thus $x_0 = a_0 + (x_0 - a_0)$ with $0 \leq x_0 - a_0 < 1$. For $n \geq 1$, if $x_{n-1} \neq a_{n-1}$, define the double recurrence

$$x_n = \frac{1}{x_{n-1} - a_{n-1}}, \quad a_n = \lfloor x_n \rfloor.$$

This process, which associates to a real number x the sequence of integers $a_0, a_1, a_2, \ldots$, is called the continued fraction algorithm. Also, the continued fraction expansion of x is

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

The quantities a_n are called partial quotients where a_0 is an integer and $a_1, a_2, \cdots$ are positive integers. If the number of terms is finite, we write $x = [a_0, a_1, a_2, \cdots, a_m]$. Truncating at the k-th place (with $k < m$ in the finite case), we get the rational number

$$\frac{p_k}{q_k} = [a_0, a_1, \cdots, a_k].$$

This number is called the k-th convergent of x.

The convergents of a continued fraction have nice properties and applications in number theory. As in Wiener's attack, a key role in our attacks is played by the following theorem on good rational approximations (see Theorem 184 of [6]).

Theorem 1. *Let x be a real number. If X and Y are coprime integers such that*

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

then $\frac{Y}{X}$ is a convergent of x.

2.2 Coppersmith's Method

An important application of lattice basis reduction is finding small solutions to modular univariate polynomial equations

$$f(x) = \sum_i a_i x^i \equiv 0 \pmod N, \quad a_i \in \mathbb{Z}/N\mathbb{Z},$$

and small roots of bivariate polynomial equations

$$g(x,y) = \sum_{i,j} a_{i,j} x^i y^j = 0, \quad a_{i,j} \in \mathbb{Z}.$$

In 1996, Coppersmith introduced a method for solving the two equations using the LLL-algorithm [9]. He showed that for any modulus N, all the solutions $f(x_0) \equiv 0 \pmod N$ with $|x_0| < N^{1/\delta}$ may be found in time polynomial in $\log N$ and δ where δ is the degree of f. Similarly, he showed that if $g(x,y)$ has maximum degree d in each variable separately, then one can find all integer pairs (x_0, y_0) satisfying $|x_0| < X$, $|y_0| < Y$ and $g(x_0, y_0) = 0$ in time polynomial in $\log W$ and 2^d if X and Y satisfy

$$XY < W^{2/(3d)-\varepsilon},$$

for some $\varepsilon > 0$ where $W = \max_{i,j} \left|a_{i,j} X^i Y^j\right|$.

Since then, Coppersmith's method has found many different applications in the area of public key cryptography, specifically in cryptanalysis of some instances of RSA (see [3]). As an important application of the bivariate case, Coppersmith showed in 1996 that 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. Later, Howgrave-Graham [7] and May [11] showed that the univariate modular approach suffices. Our attacks make use of the following generalization of Coppersmith's result (see [11], Theorem 10).

Theorem 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose we know an approximation $\tilde{P}$ of pu with $|\tilde{P} - pu| < 2N^{\frac{1}{4}}$ where u is an unknown integer that is not a multiple of q. 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 useful lemmas. The first is about the size of the balanced prime factors p, q of an RSA modulus $N = pq$.

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then*

$$2^{-\frac{1}{2}} N^{\frac{1}{2}} < q < N^{\frac{1}{2}} < p < 2^{\frac{1}{2}} N^{\frac{1}{2}}.$$

Proof. Assume $q < p < 2q$. Then multiplying by p we get $N < p^2 < 2N$. This gives $N^{\frac{1}{2}} < p < 2^{\frac{1}{2}} N^{\frac{1}{2}}$. Similarly, multiplying $q < p < 2q$ by q we get $q^2 < N < 2q^2$ which leads to $2^{-\frac{1}{2}} N^{\frac{1}{2}} < q < N^{\frac{1}{2}}$ and the lemma follows.

The following lemma shows how to find an approximation of $\left|pu - \frac{q}{u}\right|$ using an approximation of $\left|pu + \frac{q}{u}\right|$.

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and u an integer. If S is a positive integer such that*

$$\left|S - \left|pu + \frac{q}{u}\right|\right| < \frac{p-q}{3(p+q)} N^{\frac{1}{4}},$$

then

$$\left|D - \left|pu - \frac{q}{u}\right|\right| < N^{\frac{1}{4}},$$

where $D = \sqrt{|S^2 - 4N|}$.

Proof. Let u be an integer. Suppose that S satisfies $\left|S - \left|pu + \frac{q}{u}\right|\right| < \frac{p-q}{3(p+q)} N^{\frac{1}{4}}$. Define $D = \sqrt{|S^2 - 4N|}$. Then

$$\begin{aligned}
\left|D^2 - \left(pu - \frac{q}{u}\right)^2\right| &= \left|\left|S^2 - 4N\right| - \left(pu - \frac{q}{u}\right)^2\right| \\
&\leq \left|S^2 - 4N - \left(pu - \frac{q}{u}\right)^2\right| \\
&= \left|S^2 - \left(pu + \frac{q}{u}\right)^2\right| \\
&= \left(S + \left|pu + \frac{q}{u}\right|\right)\left|S - \left|pu + \frac{q}{u}\right|\right| \\
&\leq \left(S + \left|pu + \frac{q}{u}\right|\right) \times \frac{p-q}{3(p+q)} N^{\frac{1}{4}}.
\end{aligned}$$

Dividing by $D + \left|pu - \frac{q}{u}\right|$, we get

$$\left|D - \left|pu - \frac{q}{u}\right|\right| \leq \frac{S + \left|pu + \frac{q}{u}\right|}{D + \left|pu - \frac{q}{u}\right|} \times \frac{p-q}{3(p+q)} N^{\frac{1}{4}}. \tag{1}$$

Let us find an upper bound for $\frac{S + \left|pu + \frac{q}{u}\right|}{D + \left|pu - \frac{q}{u}\right|}$ in terms of p and q. We have

$$\frac{S + \left|pu + \frac{q}{u}\right|}{D + \left|pu - \frac{q}{u}\right|} < \frac{2\left|pu + \frac{q}{u}\right| + \frac{p-q}{3(p+q)} N^{\frac{1}{4}}}{\left|pu - \frac{q}{u}\right|} < \frac{3\left|pu + \frac{q}{u}\right|}{\left|pu - \frac{q}{u}\right|} \leq \frac{3(p+q)}{p-q}.$$

Plugging this in (1), we get

$$\left|D-\left|pu-\frac{q}{u}\right|\right| \le \frac{3(p+q)}{p-q}\times\frac{p-q}{3(p+q)}N^{\frac{1}{4}}=N^{\frac{1}{4}}.$$

This terminates the proof.

Similarly, the following lemma shows how to find an approximation of $\left|pu+\frac{q}{u}\right|$ using an approximation of $\left|pu-\frac{q}{u}\right|$.

Lemma 3. *Let $N=pq$ be an RSA modulus with $q<p<2q$ and u an integer. If D is a positive integer such that*

$$\left|D-\left|pu-\frac{q}{u}\right|\right| < N^{\frac{1}{4}},$$

then

$$\left|S-\left|pu+\frac{q}{u}\right|\right| < N^{\frac{1}{4}},$$

where $S=\sqrt{D^2+4N}$.

Proof. Let u be an integer. Suppose that D satisfies $\left|D-\left|pu-\frac{q}{u}\right|\right| < N^{\frac{1}{4}}$. Define $S=\sqrt{D^2+4N}$. We have

$$\begin{aligned}
\left|S^2-\left(pu+\frac{q}{u}\right)^2\right| &= \left|D^2+4N-\left(pu+\frac{q}{u}\right)^2\right| \\
&= \left|D^2-\left(pu-\frac{q}{u}\right)^2\right| \\
&= \left(D+\left|pu-\frac{q}{u}\right|\right)\left|D-\left|pu-\frac{q}{u}\right|\right| \\
&\le \left(D+\left|pu-\frac{q}{u}\right|\right)N^{\frac{1}{4}}.
\end{aligned}$$

Dividing by $S+\left|pu+\frac{q}{u}\right|$, we get

$$\left|S-\left|pu-\frac{q}{u}\right|\right| \le \frac{D+\left|pu-\frac{q}{u}\right|}{S+\left|pu+\frac{q}{u}\right|}N^{\frac{1}{4}}.$$

Since $D<S$ and $\left|pu-\frac{q}{u}\right|<\left|pu+\frac{q}{u}\right|$, then

$$\left|S-\left|pu+\frac{q}{u}\right|\right| < N^{\frac{1}{4}}.$$

This terminates the proof.

4 The Exponents Satisfying $eX-\left(N-\left(pu+\frac{q}{u}\right)\right)Y=Z$

In this section, we consider the class of the exponents e satisfying an equation

$$eX-\left(N-\left(pu+\frac{q}{u}\right)\right)Y=Z,$$

where X and Y are suitably small integers satisfying $\gcd(X,Y)=1$ and Z is a suitable rational.

4.1 The Attack

We begin with a useful lemma connecting the parameters X and Y to the convergents of $\frac{e}{N}$.

Lemma 4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be an exponent satisfying an equation*

$$eX - \left(N - \left(pu + \frac{q}{u}\right)\right) Y = Z,$$

for some $u \in \mathbb{N}$. If

$$\gcd(X, Y) = 1, \quad XY < \frac{N}{4\left|pu + \frac{q}{u}\right|}, \quad |Z| < \frac{p-q}{3(p+q)} N^{\frac{1}{4}} Y,$$

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

Proof. Suppose that e satisfies an equation

$$eX - \left(N - \left(pu + \frac{q}{u}\right)\right) Y = Z,$$

with $|Z| < \frac{p-q}{3(p+q)} N^{\frac{1}{4}} Y$. Then, since $p > \sqrt{N}$, we have $|Z| < \left|pu + \frac{q}{u}\right| Y$ and we get

$$\begin{aligned}
\left|\frac{e}{N} - \frac{Y}{X}\right| &= \frac{|eX - NY|}{NX} \\
&= \frac{\left|Z - \left(pu + \frac{q}{u}\right) Y\right|}{NX} \\
&\leq \frac{|Z|}{NX} + \frac{\left|pu + \frac{q}{u}\right| Y}{NX} \\
&\leq \frac{2\left|pu + \frac{q}{u}\right| Y}{NX}.
\end{aligned}$$

In order to apply Theorem 1, we need $\frac{2\left|pu+\frac{q}{u}\right|Y}{NX} < \frac{1}{2X^2}$. Solving for XY, we get

$$XY < \frac{N}{4\left|pu + \frac{q}{u}\right|}.$$

Under this condition, $\frac{Y}{X}$ is then a convergent of $\frac{e}{N}$.

We now present the first attack.

Theorem 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be an exponent satisfying an equation*

$$eX - \left(N - \left(pu + \frac{q}{u}\right)\right) Y = Z,$$

for some $u \in \mathbb{N}$. If

$$\gcd(X, Y) = 1, \quad XY < \frac{N}{4\left|pu + \frac{q}{u}\right|}, \quad |Z| < \frac{p-q}{3(p+q)} N^{\frac{1}{4}} Y.$$

Then N can be factored in polynomial time.

Proof. Let u be an integer. Suppose that e is an exponent satisfying an equation

$$eX - \left(N - \left(pu + \frac{q}{u}\right)\right) Y = Z,$$

with

$$\gcd(X,Y) = 1, \quad XY < \frac{N}{4\left|pu + \frac{q}{u}\right|}, \quad |Z| < \frac{p-q}{3(p+q)} N^{\frac{1}{4}} Y.$$

Then, by Lemma 4, $\frac{Y}{X}$ appears among the convergents of the continued fraction expansion of $\frac{e}{N}$. Using X and Y, define

$$S = \left|N - \frac{eX}{Y}\right|, \quad D = \sqrt{|S^2 - 4N|}.$$

Then S is an approximation of $\left|pu + \frac{q}{u}\right|$ satisfying

$$\left|S - \left|pu + \frac{q}{u}\right|\right| \leq \left|N - \frac{eX}{Y} - \left(pu + \frac{q}{u}\right)\right| = \frac{|Z|}{Y} < \frac{p-q}{3(p+q)} N^{\frac{1}{4}}. \tag{2}$$

By Lemma 2, it follows that D is an approximation of $\left|pu - \frac{q}{u}\right|$ satisfying

$$\left|D - \left|pu - \frac{q}{u}\right|\right| < N^{\frac{1}{4}}.$$

Combining this with (2), we get

$$\begin{aligned}
\left|p|u| - \frac{S+D}{2}\right| &= \frac{1}{2}\left|2p|u| - (S+D)\right| \\
&= \frac{1}{2}\left|\left(p|u| + \frac{q}{|u|} - S\right) + \left(p|u| - \frac{q}{|u|} - D\right)\right| \\
&\leq \frac{1}{2}\left|p|u| + \frac{q}{|u|} - S\right| + \frac{1}{2}\left|p|u| - \frac{q}{|u|} - D\right| \\
&= \frac{1}{2}\left|\left|pu + \frac{q}{u}\right| - S\right| + \frac{1}{2}\left|\left|pu - \frac{q}{u}\right| - D\right| \\
&< \frac{1}{2} \times \frac{p-q}{3(p+q)} N^{\frac{1}{4}} + \frac{1}{2} N^{\frac{1}{4}} \\
&< N^{\frac{1}{4}}.
\end{aligned}$$

This implies that $\frac{S+D}{2}$ is an approximation of $p|u|$ with an additive error term at most $N^{\frac{1}{4}}$. Hence, using Coppersmith's technique (Theorem 2), this leads to the factorization of N. Since the number of convergents of $\frac{e}{N}$ is bounded by $\mathcal{O}(\log N)$ and the continued fraction algorithm and Coppersmith's method are polynomial time algorithms, then N can be factored in polynomial time.

4.2 The Number of the Weak Exponents

Here, we present a class of exponents e with the structure

$$e = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right] + z,$$

with suitably small parameters X, Y and z for every $|u| < \frac{1}{2}q$. We will show that such exponents are vulnerable to our attack and will give a lower bound for their number.

Lemma 5. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that e is an exponent with the structure*

$$e = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right] + z,$$

where $|u| < \frac{1}{2}q$ and

$$\gcd(X, Y) = 1, \quad XY < \frac{N}{4\left|pu + \frac{q}{u}\right|}, \quad |z| < \frac{(p-q)N^{\frac{1}{4}}Y}{3(p+q)X} - \frac{1}{2}.$$

Then N can be factored in polynomial time.

Proof. Define

$$e_0 = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right].$$

Then using the property of the round function $[x]$, we get

$$\left|e_0 - \left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right| \leq \frac{1}{2}.$$

If $e = e_0 + z$ then e satisfies

$$\left|e - \left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right| \leq \left|e_0 - \left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right| + |z| \leq \frac{1}{2} + |z|.$$

Multiplying by X, we get

$$\left|eX - \left(N - \left(pu + \frac{q}{u}\right)\right)Y\right| \leq \left(\frac{1}{2} + |z|\right)X.$$

In order to apply Theorem 3, we have to satisfy

$$\gcd(X, Y) = 1, \quad XY < \frac{N}{4\left|pu + \frac{q}{u}\right|}.$$

We have also to satisfy

$$\left(\frac{1}{2} + |z|\right)X < \frac{p-q}{3(p+q)}N^{\frac{1}{4}}Y,$$

which is satisfied if
$$|z| < \frac{(p-q)N^{\frac{1}{4}}Y}{3(p+q)X} - \frac{1}{2}.$$
This terminates the proof.

Let u be an integer satisfying $1 \leq |u| < \frac{1}{2}q$. In the rest of this section, we define α by the equality
$$\left|pu + \frac{q}{u}\right| = N^{\frac{1}{2}+\alpha}.$$
Since $1 \leq |u| < \frac{1}{2}q$ and $p > \sqrt{N}$, then α satisfies $0 < \alpha < \frac{1}{2}$.

Now, we consider the set of the exponents with the structure
$$e = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right] + z,$$
where the parameters X, Y and z satisfy
$$\gcd(X, Y) = 1, \quad X \leq Y < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}, \quad |z| < \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} - \frac{1}{2},$$
and propose to find a lower bound for the size of the number of such exponents. Observe that, since $XY < \frac{1}{4}N^{\frac{1}{2}-\alpha} = \frac{N}{4\left|pu+\frac{q}{u}\right|}$, then, by Lemma 5, the new set of exponents is weak to our attack.

The following result shows that for a common u, different parameters X, Y define different exponents.

Lemma 6. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let u be an integer such that $|u| < \frac{1}{2}q$. For $i = 1, 2$, let e_i be two exponents satisfying*
$$e_i = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y_i}{X_i}\right] + z_i,$$
where
$$\gcd(X_i, Y_i) = 1, \quad X_i \leq Y_i < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}, \quad |z_i| < \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} - \frac{1}{2},$$
and α is defined by $\left|pu + \frac{q}{u}\right| = N^{\frac{1}{2}+\alpha}$. If $(X_1, Y_1) \neq (X_2, Y_2)$ then $e_1 \neq e_2$.

Proof. For $i = 1, 2$, suppose that the exponents e_i satisfy
$$e_i = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y_i}{X_i}\right] + z_i.$$
Then, as in the proof of Lemma 5, we have for $i = 1, 2$
$$\left|e_i - \left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y_i}{X_i}\right| < \frac{1}{2} + |z_i|.$$

Now, suppose that $e_1 = e_2$. Then

$$
\begin{aligned}
&\left(N - \left(pu + \frac{q}{u}\right)\right)\left|\frac{Y_1}{X_1} - \frac{Y_2}{X_2}\right| \\
&= \left|e_1 - \left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y_1}{X_1} - e_2 + \left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y_2}{X_2}\right| \\
&\leq \left|e_1 - \left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y_1}{X_1}\right| + \left|e_2 - \left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y_2}{X_2}\right| \\
&\leq 1 + |z_1| + |z_2|.
\end{aligned}
$$

Multiplying by X_1X_2, we get

$$\left(N - \left(pu + \frac{q}{u}\right)\right)|Y_1X_2 - Y_2X_1| \leq (1 + |z_1| + |z_2|)X_1X_2. \tag{3}$$

For $i = 1, 2$, suppose that

$$X_i \leq Y_i < \frac{1}{2}N^{\frac{1}{4} - \frac{\alpha}{2}}, \quad |z_i| < \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} - \frac{1}{2}.$$

Then using Lemma 1, the right side of (3) satisfies

$$(1 + |z_1| + |z_2|)X_1X_2 < \frac{2(p-q)N^{\frac{1}{4}}}{3(p+q)} \times \frac{1}{4}N^{\frac{1}{2} - \alpha} < \frac{(p-q)N^{\frac{3}{4} - \alpha}}{6(p+q)}.$$

On the other hand, for $1 \leq |u| < \frac{1}{2}q$, the expression $N - \left(pu + \frac{1}{u}q\right)$ is minimal for $u = \frac{q}{2}$. More precisely,

$$N - \left(pu + \frac{q}{u}\right) \geq N - \left(\frac{N}{2} + 2\right) = \frac{N}{2} - 2.$$

It follows that the term $N - \left(pu + \frac{q}{u}\right)$ in the left side of (3) satisfies

$$N - \left(pu + \frac{q}{u}\right) \geq \frac{N}{2} - 2 > \frac{(p-q)N^{\frac{3}{4} - \alpha}}{6(p+q)}.$$

Consequently, the inequality (3) implies that $Y_1X_2 - Y_2X_1 = 0$, and since $\gcd(X_1, Y_1) = \gcd(X_2, Y_2) = 1$, then $X_1 = X_2$ and $Y_1 = Y_2$ which terminates the proof.

Another result needed to count the number of weak exponents is the following lemma. It shows that different parameters u define different exponents.

Lemma 7. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. For $i = 1, 2$, let e_i be two exponents satisfying*

$$e_i = \left[\left(N - \left(pu_i + \frac{q}{u_i}\right)\right)\frac{Y_i}{X_i}\right] + z_i,$$

with

$$\gcd(X_i, Y_i) = 1, \quad X_i \leq Y_i, \quad |z_i| < \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} - \frac{1}{2}.$$

If $u_1 \neq u_2$ then $e_1 \neq e_2$.

Proof. Suppose for contradiction that $u_1 \neq u_2$, and, without loss of generality that $u_1 < u_2$. Then

$$pu_1 + \frac{q}{u_1} - \left(pu_2 + \frac{q}{u_2}\right) = (u_1 - u_2)\left(p - \frac{q}{u_1 u_2}\right) \leq -\left(p - \frac{1}{2}q\right).$$

From this, we deduce

$$\left(N - \left(pu_1 + \frac{q}{u_1}\right)\right) - \left(N - \left(pu_2 + \frac{q}{u_2}\right)\right) \geq p - \frac{1}{2}q. \tag{4}$$

Now, for $i = 1, 2$, suppose that the exponents e_i satisfy

$$e_i = \left[\left(N - \left(pu_i + \frac{q}{u_i}\right)\right)\frac{Y_i}{X_i}\right] + z_i.$$

and that $e_1 = e_2 = e$. Then

$$\begin{aligned}
&\left|\left(N - \left(pu_1 + \frac{q}{u_1}\right)\right)\frac{Y_1}{X_1} - \left(N - \left(pu_2 + \frac{q}{u_2}\right)\right)\frac{Y_2}{X_2}\right| \\
&= \left|-e_1 + \left(N - \left(pu_1 + \frac{q}{u_1}\right)\right)\frac{Y_1}{X_1} + e_2 - \left(N - \left(pu_2 + \frac{q}{u_2}\right)\right)\frac{Y_2}{X_2}\right| \\
&\leq \left|e_1 - \left(N - \left(pu_1 + \frac{q}{u_1}\right)\right)\frac{Y_1}{X_1}\right| + \left|e_2 - \left(N - \left(pu_2 + \frac{q}{u_2}\right)\right)\frac{Y_2}{X_2}\right| \\
&\leq 1 + |z_1| + |z_2|.
\end{aligned}$$

Since $\frac{Y_1}{X_1}$ and $\frac{Y_2}{X_2}$ are two convergents of $\frac{e}{N}$, then $\frac{Y_1}{X_1} \approx \frac{Y_2}{X_2}$. This leads to

$$\left|\left(N - \left(pu_1 + \frac{q}{u_1}\right)\right) - \left(N - \left(pu_2 + \frac{q}{u_2}\right)\right)\right|\frac{Y_1}{X_1} < 1 + |z_1| + |z_2|.$$

Rearranging, we get

$$\left|\left(N - \left(pu_1 + \frac{q}{u_1}\right)\right) - \left(N - \left(pu_2 + \frac{q}{u_2}\right)\right)\right| < (1 + |z_1| + |z_2|)\frac{X_1}{Y_1}. \tag{5}$$

If

$$X_i \leq Y_i, \quad |z_i| < \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} - \frac{1}{2},$$

for $i = 1, 2$, then the right side of (5) satisfies

$$(1 + |z_1| + |z_2|)\frac{X_1}{Y_1} \leq 1 + |z_1| + |z_2| < \frac{2(p-q)N^{\frac{1}{4}}}{3(p+q)}.$$

This is a contradiction since, combining Lemma 1 and inequality (4), the left side of (5) satisfies

$$p - \frac{1}{2}q > \sqrt{N} - 2^{-\frac{3}{2}}\sqrt{N} > \frac{2(p-q)N^{\frac{1}{4}}}{3(p+q)}.$$

Hence $u_1 = u_2$ and applying Lemma 6, it follows that $X_1 = X_2$ and $Y_1 = Y_2$. This terminates the proof.

We are now able to prove a lower bound for the number of the exponents with the structure

$$e = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right] + z,$$

where the parameters X, Y and z satisfy the conditions of Lemma 6. We notice that the $X9.31$ standard [1] for public key cryptography requires that the primes p and q of an RSA modulus $N = pq$ satisfy

$$|p - q| > \frac{\sqrt{N}}{2^{100}}.$$

The following result is valid for such modulus.

Theorem 4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and $|p-q| > \frac{\sqrt{N}}{2^{100}}$. The number of the exponents e satisfying*

$$e = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right] + z,$$

with $|u| < \frac{1}{2}q$ and

$$\gcd(X, Y) = 1, \quad X \leq Y < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}, \quad |z| < \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} - \frac{1}{2},$$

where $\left|pu + \frac{q}{u}\right| = N^{\frac{1}{2}+\alpha}$, is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for suitably large N.

Proof. The number of the exponents satisfying

$$e = \left[\left(N - \left(pu + \frac{q}{u}\right)\right)\frac{Y}{X}\right] + z,$$

with the conditions of the theorem is

$$\mathcal{N} = \sum_{|u|=1}^{\left\lfloor \frac{1}{2}q \right\rfloor} \sum_{Y=1}^{B_1} \sum_{\substack{X=1 \\ \gcd(X,Y)=1}}^{Y-1} \sum_{|z|=1}^{B_2} 1. \tag{6}$$

where

$$B_1 = \left\lfloor \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}} \right\rfloor \quad \text{and} \quad B_2 = \left\lfloor \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} \right\rfloor.$$

We have

$$\sum_{|z|=1}^{B_2} 1 = 2B_2 > \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)}.$$

Plugging this in (6), we get

$$\mathcal{N} > \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} \sum_{|u|=1}^{\left\lfloor \frac{1}{2}q \right\rfloor} \sum_{Y=1}^{B_1} \sum_{\substack{X=1 \\ \gcd(X,Y)=1}}^{Y-1} 1. \tag{7}$$

Now, we have for $1 < Y < N$ (see [6], Theorem 328)

$$\sum_{\substack{X=1 \\ \gcd(X,Y)=1}}^{Y-1} 1 = \phi(Y) > \frac{cY}{\log\log Y} > \frac{cY}{\log\log N},$$

where $c > 0$ is a constant. Plugging in turn in (7), we get

$$\mathcal{N} > \frac{c(p-q)N^{\frac{1}{4}}}{3(p+q)\log\log N} \sum_{|u|=1}^{\left\lfloor \frac{1}{2}q \right\rfloor} \sum_{Y=1}^{B_1} Y. \tag{8}$$

Now, for $|u| < \frac{1}{2}q$, we have

$$\sum_{Y=1}^{B_1} Y = \frac{B_1(B_1+1)}{2} > \frac{1}{8}N^{\frac{1}{2}-\alpha} = \frac{N}{8\left|pu + \frac{q}{u}\right|} > \frac{N}{16p|u|} > \frac{\sqrt{N}}{16\sqrt{2}|u|},$$

where we used $\left|pu + \frac{q}{u}\right| < 2p|u|$ and $p < \sqrt{2}\sqrt{N}$. Plugging in (8), we get

$$\mathcal{N} > \frac{c(p-q)\sqrt{N}N^{\frac{1}{4}}}{48\sqrt{2}(p+q)\log\log N} \sum_{|u|=1}^{\left\lfloor \frac{1}{2}q \right\rfloor} \frac{1}{|u|}. \tag{9}$$

Using the estimation (see [6], Theorem 422)

$$\sum_{x=1}^{n} \frac{1}{x} \geq \log n,$$

we get

$$\sum_{|u|=1}^{\left\lfloor \frac{1}{2}q \right\rfloor} \frac{1}{|u|} > 2\log\left(\left\lfloor \frac{1}{2}q \right\rfloor\right) > \log(2q) > \log\left(\sqrt{2}\sqrt{N}\right),$$

where we used $q > \frac{\sqrt{2}}{2}\sqrt{N}$. Plugging in (9), we get

$$\mathcal{N} > \frac{c(p-q)N^{\frac{3}{4}}\log\left(\sqrt{2}\sqrt{N}\right)}{48(p+q)\sqrt{2}\log\log N} > \frac{c(p-q)}{96\sqrt{2}(p+q)\log\log N}N^{\frac{3}{4}}\log N. \tag{10}$$

Suppose that the primes p and q satisfy

$$|p-q| > \frac{\sqrt{N}}{2^{100}}.$$

(This is required by the $X9.31$ standard [1] for public key cryptography). Combining with Lemma 1, this implies that for a normal RSA modulus, we find

$$\frac{p-q}{p+q} > \frac{\frac{\sqrt{N}}{2^{100}}}{\left(1+\sqrt{2}\right)\sqrt{N}} = \frac{1}{2^{100}\left(1+\sqrt{2}\right)} > \frac{1}{2^{102}}.$$

Plugging in (10), we get

$$\mathcal{N} > \frac{c}{96 \times 2^{102}\sqrt{2}\log\log N} N^{\frac{3}{4}} \log N = N^{\frac{3}{4}-\varepsilon},$$

where we put $\frac{c \log N}{96 \times 2^{102}\sqrt{2}\log\log N} = N^{-\varepsilon}$ and $\varepsilon > 0$ is arbitrarily small for suitably large N. This terminates the proof.

5 The Exponents Satisfying $eX - \left(N - \left(pu - \frac{q}{u}\right)\right) Y = Z$

In this section, we consider the class of exponents e satisfying an equation

$$eX - \left(N - \left(pu - \frac{q}{u}\right)\right) Y = Z,$$

with suitably small parameters X, Y, Z and u is an integer satisfying $|u| < \frac{1}{2}q$. The following lemma shows how to find X and Y using the convergents of $\frac{e}{N}$.

Lemma 8. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be an exponent satisfying an equation*

$$eX - \left(N - \left(pu - \frac{q}{u}\right)\right) Y = Z.$$

If

$$\gcd(X,Y) = 1, \quad XY < \frac{N}{4\left|pu - \frac{q}{u}\right|} \quad \text{and} \quad |Z| < N^{\frac{1}{4}}Y,$$

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

Proof. The proof is similar to the proof of Lemma 4.

The following result presents the second attack.

Theorem 5. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be an exponent satisfying an equation*

$$eX - \left(N - \left(pu - \frac{q}{u}\right)\right) Y = Z.$$

If

$$\gcd(X,Y) = 1, \quad XY < \frac{N}{4\left|pu - \frac{q}{u}\right|} \quad \text{and} \quad |Z| < N^{\frac{1}{4}}Y.$$

Then N can be factored in polynomial time.

Proof. Suppose that e is an exponent satisfying an equation

$$eX - \left(N - \left(pu - \frac{q}{u}\right)\right) Y = Z,$$

with

$$\gcd(X,Y) = 1, \quad XY < \frac{N}{4\left|pu - \frac{q}{u}\right|} \quad \text{and} \quad |Z| < N^{\frac{1}{4}}Y.$$

Then Lemma 8 implies that $\frac{Y}{X}$ is a convergent of $\frac{e}{N}$. Next, define

$$D = \left|N - \frac{eX}{Y}\right| \quad \text{and} \quad S = \sqrt{D^2 + 4N}.$$

Then D is an approximation of $\left|pu - \frac{q}{u}\right|$ satisfying

$$\left|D - \left|pu - \frac{q}{u}\right|\right| \leq \left|N - \frac{eX}{Y} - \left(pu - \frac{q}{u}\right)\right| = \frac{|Z|}{Y} < N^{\frac{1}{4}}. \tag{11}$$

Applying Lemma 3, S is then an approximation of $\left|pu + \frac{q}{u}\right|$ which satisfies

$$\left|S - \left|pu + \frac{q}{u}\right|\right| < N^{\frac{1}{4}}.$$

Combining this with (11), we get, as in the proof of Theorem 3

$$\left|p|u| - \frac{S + D}{2}\right| < N^{\frac{1}{4}},$$

and we conclude using similar arguments.

Now, we consider the class of the exponents e with the structure

$$e = \left[\left(N - \left(pu - \frac{q}{u}\right)\right)\frac{Y}{X}\right] + z,$$

where $|u| < \frac{1}{2}q$ and

$$\gcd(X,Y) = 1, \quad X < Y < \frac{\sqrt{N}}{2\sqrt{\left|pu - \frac{q}{u}\right|}} \quad \text{and} \quad |z| < N^{\frac{1}{4}}.$$

Then using similar arguments as in Subsection 4.2, where one mainly substitutes $pu + \frac{q}{u}$ by $pu - \frac{q}{u}$, it is easy to show that such exponents are weak to our second attack and that their number is at least $N^{\frac{3}{4}-\varepsilon}$, where $\varepsilon > 0$ is arbitrarily small for suitably large N.

6 Conclusion

In this paper, we studied the set of exponents e satisfying an equation

$$eX - \left(N - \left(pu \pm \frac{q}{u}\right)\right) Y = Z.$$

where u is an integer with $|u| < \frac{1}{2}q$ and X, Y are suitably small coprime integers. We show that a combination of the continued fraction algorithm and Coppersmith's method can be efficiently applied to find the parameters X, Y and more importantly, the prime factors p and q of the modulus $N = pq$. In addition, when p and q satisfy $|p - q| = \Omega\left(\sqrt{N}\right)$, we show that the set of such weak exponents is relatively large, namely that their number is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for suitably large N. Our results illustrate once again the fact that one should be cautious in the design of RSA exponents of special forms.

References

1. ANSI Standard X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).
2. Blömer, J., May, A.: 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. Boneh, D.: Twenty years of attacks on the RSA cryptosystem. Notices of the American Mathematical Society (AMS) 46(2), 203-213 (1999)
4. Boneh, D., Durfee, G.: 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)
5. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), 233-260 (1997)
6. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, London (1975)
7. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In Cryptography and Coding, LNCS 1355, pp. 131-142, Springer-Verlag (1997)
8. Lenstra, H.W.: Factoring integers with elliptic curves, Annals of Mathematics, vol. 126, 649-673 (1987)
9. Lenstra, A.K., Lenstra, H.W., Lovasz, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, 513-534 (1982)
10. Maitra, S., Sarkar S.: Revisiting Wiener's Attack - New Weak Keys in RSA, In: T.-C.Wu et al. (Eds): ISC 2008, LNCS 5222, pp. 228–243, 2008. Springer-Verlag, Berlin Heidelberg 2008
11. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods, Ph.D. thesis, Paderborn, 2003, `http://www.informatik.tu-darmstadt.de/KP/publications/03/bp.ps`
12. Nitaj, A.: Application of ECM to a class of RSA keys, J. Discrete Math. Sci. Cryptography, vol. 12, pp. 121–137 (2009)

13. Nitaj, A.: Cryptanalysis of RSA using the ratio of the primes, In: B. Preneel (Ed.) Africacrypt 2009, LNCS 5580, pp. 98–115, 2009. Springer-Verlag, Berlin Heidelberg 2009
14. Rivest, R., Shamir A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol. 21 (2), 120-126 (1978)
15. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553-558 (1990)