RSA AND A HIGHER DEGREE DIOPHANTINE EQUATION

Abderrahmane Nitaj

Département de mathématiques
Université de Caen
Boulevard Maréchal Juin
14032 Caen Cedex, France
E-mail address: nitaj@math.unicaen.fr

February 28, 2006

Abstract. Let $N = pq$ be an RSA modulus where p, q are large primes of the same bitsize. We study the class of the public exponents e for which there exist an integer m with $1 \leq m \leq \frac{\log N}{\log 32}$ and small integers u, X, Y and Z satisfying

$$(e+u)Y^m - \psi(N)X^m = Z,$$

where $\psi(N) = (p+1)(q-1)$. First we show that these exponents are of improper use in RSA cryptosystems. Next we show that their number is at least $O\left(mN^{\frac{1}{2}+\frac{\alpha}{m}-\alpha-\varepsilon}\right)$ where α is defined by $N^{1-\alpha} = \psi(N)$.

1 Introduction

Let $N = pq$ be an RSA modulus, i.e the product of two large primes p and q. Without loss of generality, we assume that $q < p$. Morever, throughout this paper we assume that the primes p and q are balanced, in other words, that the bitsizes of the primes are equal so that $q < p < 2q$.

Let e, d be the public and secret exponents satisfying $ed \equiv 1 \pmod{\phi(n)}$ where $\phi(n) = (p-1)(q-1)$ is the Euler totient function. To speed up the RSA decryption of some devices with limited computing power such as smart card, one might be tempted to use short secret exponents d. In 1990, Wiener [11] showed that if $d < \frac{1}{3}N^{\frac{1}{4}}$, then RSA was insecure. Wiener's method is based on approximations using continued fractions. Verheul and van

---

2000 *Mathematics Subject Classification.* 94A60, 11Y05.
Key words and phrases. RSA cryptosystem, Continued fractions, Coppersmith's algorithm.

Tilborg [8] and Dujella [4] proposed an extension of the results of Wiener that allows RSA to be broken when $d < N^{\frac{1}{4}+\gamma}$ using an exhaustive search for about $8 + 2\gamma \log_2 N$ bit. In 1999, Boneh and Durfee [2] improved Wiener's bound to $d < N^{0.292}$. Their attack is based on Coppersmith's technique [3] for finding small roots to polynomial equations, which in turn is based on the LLL-lattice reduction algorithm. In 2002, de Weger [9] proposed an extension of these attacks to an RSA modulus with a small difference between its prime factors. In 2004, Blömer and May [1] extended both Wiener and de Weger attacks for the RSA cryptosystems with secret exponents having the modular factorization $d \equiv -xy^{-1} \pmod{\phi(N)}$ where x and y are integers satisfying

$$1 \le x < \frac{1}{3} N^{\frac{1}{4}} \qquad \text{and} \qquad |y| < N^{-\frac{3}{4}} ex.$$

Morever, they showed that the number of such keys is at least $O\left(N^{\frac{3}{4}-\varepsilon}\right)$ where ε is a positive constant. In contrast to the attacks of Wiener and Boneh-Durfee, the secret key in the attack of Blömer-May could be large.

The starting point of the former attacks is the defining equation $ed \equiv 1 \pmod{\phi(N)}$, which means that there exists an integer k such that $ed - k\phi(N) = 1$. The main results of these attacks are based on the arithmetical properties encoded in the public exponent e and the Euler totient function $\phi(N)$. Such keys (N, e) are called *weak keys* in [1] and $\phi(N)$-*constrained keys* in [7]. Instead of focusing on the information encoded in the public exponent e reltively to $\phi(N)$, an alternative way proposed in [7] is to replace $\phi(N)$ by any function F with special properties. In that paper, an attack was proposed on the public exponents e satisfying $eY - p(q-u)X = Z$, with suitably small unknown integers u, X, Y, Z. It is shown that every public exponent with these properties yields the factorization of N in polynomial time and that the number of such keys is at least $O\left(N^{\frac{3}{4}-\varepsilon}\right)$.

In this work we consider the class of the public exponents e satisfying the diophantine equation

$$(e + u)X^m - \psi(N)Y^m = Z, \tag{1}$$

where m is an integer satisfying $1 \le m \le \frac{\log N}{\log 32}$ and

$$\psi(N) = (p + 1)(q - 1).$$

For notational convenience, we define $\alpha \in \mathbb{R}$ so that $\psi(N) = N^{1-\alpha}$. Typically, $\psi(N) \approx N$ and therefore $\alpha \approx 0$. We present a new method that finds p and q in polynomial time for every exponent e satisfying (1) with

$$Y \le \left(\frac{m e^{1-\frac{1}{m}} N^{\frac{1}{m}-\frac{1}{4}} \psi(N)}{2\left(\sqrt{3} N^{\frac{1}{4}} e + 2\psi(N)\right)} \right)^{\frac{1}{2}},$$

$$|Z| \le \min\left\{ N^{\frac{1}{4}} X^m, \frac{\sqrt{3} N^{\frac{1}{4}} e + 2\psi(N)}{2^m N^{\frac{1}{m}-\frac{1}{4}} \psi(N)^{1-\frac{1}{m}}} Y^m \right\},$$

$$0 \le u \le \frac{N^{\frac{1}{4}} X^m}{Y^m}.$$

In particular, we show that our attack works for all public exponents e with the special structure $e = \left\lfloor \psi(N)\frac{X^m}{Y^m} \right\rfloor + 1$ where X, Y are relatively prime integers satisfying

$$N^{-\frac{1}{4m}}Y \leq X \leq Y < \frac{\sqrt{2m}}{4}N^{\frac{1}{4}+\frac{\alpha}{2m}-\frac{\alpha}{2}}.$$

Morever, we show that the number of such exponents is at least $O\left(mN^{\frac{1}{2}+\frac{\alpha}{m}-\alpha-\varepsilon}\right)$ and should not be used in the design of an RSA cryptosystem. As in [1] and [7], our attack will be based on combining the theory of continued fractions and Coppersmith's technique [3].

The remainder of this paper is organized as follows. In Section 2, we briefly recall well known results from continued fractions and Coppersmith's technique. In Section 3, we state some properties of the function ψ. This is useful to explain our attack. In Section 4, we present the new attack. Finally, in Section 5 we give a lower bound for the number of public exponents e with a special arithmetical structure for which our approach applies.

2 Legendre's theorem and Coppersmith's technique

In this section we briefly recall Coppersmith's lattice method and the classical Legendre's theorem on diophantine approximations.

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $f(x)$ be an univariate monic polynomial of degree δ. In [3], Coppersmith described a remarkable method that finds all integer solutions x_0 of the equation $f(x_0) \equiv 0 \pmod N$ provided that $|x_0| \leq \frac{1}{2}N^{\frac{1}{\delta}-\varepsilon}$. This method has many applications in cryptography. A key role in our attack is played by the following theorem (see [3] or [6], Theorem 10).

Theorem 2.1. (Coppersmith [3]**).** *Let $N = pq$ be an RSA modulus with $q < p < 2q$. If $\tilde{p}$ is an approximation of p satisfying*

$$|p - \tilde{p}| \leq 2N^{\frac{1}{4}},$$

then N can be factored in time polynomial in $\log N$.

Similarly to Wiener's attack, our approach is also based on the continued fraction algortithm. More precisely, we will use the following classical theorem on diophantine approximations (see Corollary 2, [1, § 2] in [5]).

Theorem 2.2. (Legendre). *Let ξ be a real number. If the coprime integers X and Y satisfy*

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

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

3 Properties and basic lemmas

In this section we state some facts that we will use throughout this paper. Let $N = pq$ be an RSA modulus where p and q are primes of equal bitsize. We begin with the following useful lemma.

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

$$N - 1 - \frac{\sqrt{2}}{2}\sqrt{N} < \psi(N) < N - 1.$$

Proof. Since $q < p < 2q$, then $q^2 < N < 2q^2$. This gives

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

On the other hand, since $p = \frac{N}{q}$, then (2) gives

$$\sqrt{N} < p < \sqrt{2}\sqrt{N}. \tag{3}$$

Combining (2) and (3), we get

$$0 < p - q < \sqrt{2}\sqrt{N} - \frac{\sqrt{2}}{2}\sqrt{N} = \frac{\sqrt{2}}{2}\sqrt{N}.$$

Rewriting $\psi(N) = (p+1)(q-1) = N - 1 - (p - q)$, we get

$$N - 1 - \frac{\sqrt{2}}{2}\sqrt{N} < N - 1 - (p - q) < N - 1,$$

which proves the lemma. ■

Notice that for prime difference $p - q \le N^{\frac{1}{4}}$ an algorithm of Fermat finds the factorization of N in polynomial time (see [9]).

Recall that throughout this paper the public exponents e have the structure that they satisfy (1). We will consider in Section 4 the continued fraction expansion of $\frac{e^{\frac{1}{m}}}{N^{\frac{1}{m}}}$. The following lemma states the error terms in approximating $\psi(N)^{\frac{1}{m}}$ by $N^{\frac{1}{m}}$.

Lemma 3.2. *Let $N = pq > 39$ with $q < p < 2q$. Let m be an integer with $1 \leq m \leq \frac{\log N}{\log 32}$. Then*

$$\frac{1}{mN^{1-\frac{1}{m}}} < N^{\frac{1}{m}} - \psi(N)^{\frac{1}{m}} < \frac{\sqrt{3}\sqrt{N}}{2m\psi(N)^{1-\frac{1}{m}}},$$

Proof. Note that

$$N - \psi(N) = \left(N^{\frac{1}{m}} - \psi(N)^{\frac{1}{m}}\right) \sum_{i=0}^{m-1} N^{\frac{m-1-i}{m}} \psi(N)^{\frac{i}{m}},$$

and

$$N^{\frac{1}{m}} - \psi(n)^{\frac{1}{m}} = \frac{N - \psi(N)}{\sum_{i=0}^{m-1} N^{\frac{m-1-i}{m}} \psi(N)^{\frac{i}{m}}}. \tag{4}$$

First, consider the denominator of (4). Since $\psi(N) < N$, then

$$\sum_{i=0}^{m-1} \psi(N)^{\frac{m-1-i}{m}} \psi(N)^{\frac{i}{m}} < \sum_{i=0}^{m-1} N^{\frac{m-1-i}{m}} \psi(N)^{\frac{i}{m}} < \sum_{i=0}^{m-1} N^{\frac{m-1-i}{m}} N^{\frac{i}{m}},$$

that is

$$m\psi(N)^{1-\frac{1}{m}} < \sum_{i=0}^{m-1} N^{\frac{m-1-i}{m}} \psi(N)^{\frac{i}{m}} < mN^{1-\frac{1}{m}}. \tag{5}$$

Next, consider the numerator of (4). By Lemma 3.1, we have $N - 1 - \frac{\sqrt{2}}{2}\sqrt{N} < \psi(N) < N - 1$. This gives for $N > 39$

$$1 < N - \psi(N) < 1 + \frac{\sqrt{2}}{2}\sqrt{N} \leq \frac{\sqrt{3}}{2}\sqrt{N}.$$

Combining this with (5) in (4), we get

$$\frac{1}{mN^{1-\frac{1}{m}}} < N^{\frac{1}{m}} - \psi(N)^{\frac{1}{m}} < \frac{\sqrt{3}\sqrt{N}}{2m\psi(N)^{1-\frac{1}{m}}},$$

which terminates the proof. ∎

The following lemma gives an estimation involving $\psi(N)^{\frac{1}{m}}$ and N.

Lemma 3.3. *Let $N = pq > 30$ with $q < p < 2q$. Let m be an integer with $1 \le m \le \frac{\log N}{\log 32}$. Then*
$$\left(2+\sqrt{3}\right)\psi(N)^{\frac{1}{m}} > 2^m N^{\frac{1}{m}-\frac{1}{4}}.$$

Proof. Using Lemma 3.1, we get
$$\psi(N)^{\frac{1}{m}} > \left(N-1-\frac{\sqrt{2}}{2}\sqrt{N}\right)^{\frac{1}{m}}.$$

Define ε by
$$N-1-\frac{\sqrt{2}}{2}\sqrt{N} = N^{1-\varepsilon}.$$

Then for $N > 30$ we have $\varepsilon < \frac{1}{20}$. It follows that for all $m \ge 1$,
$$\left(N-1-\frac{\sqrt{2}\sqrt{N}}{2}\right)^{\frac{1}{m}} = N^{\frac{1}{m}-\frac{\varepsilon}{m}} \ge N^{\frac{1}{m}-\varepsilon} > N^{\frac{1}{m}-\frac{1}{20}} = N^{\frac{1}{m}-\frac{1}{4}}N^{\frac{1}{5}}$$

Since $m < \frac{\log N}{\log 32}$, then $\left(2+\sqrt{3}\right)N^{\frac{1}{5}} > N^{\frac{1}{5}} > 2^m$. Hence
$$\left(2+\sqrt{3}\right)N^{\frac{1}{m}-\frac{1}{4}}N^{\frac{1}{5}} > 2^m N^{\frac{1}{m}-\frac{1}{4}},$$

and finally
$$\left(2+\sqrt{3}\right)\psi(N)^{\frac{1}{m}} > 2^m N^{\frac{1}{m}-\frac{1}{4}},$$

which terminates the proof. ∎

Let e be a public exponent and u a positive integer with $u < N^{\frac{1}{4}}$. The following lemma states the error terms in the approximation of $(e+u)^{\frac{1}{m}}$ by $e^{\frac{1}{m}}$.

Lemma 3.4. *Let $N = pq$ with $q < p < 2q$. Let m be an integer with $1 \le m \le \frac{\log N}{\log 32}$. If $0 \le u \le N^{\frac{1}{4}}$, then*
$$(e+u)^{\frac{1}{m}} - e^{\frac{1}{m}} \le \frac{N^{\frac{1}{4}}}{me^{1-\frac{1}{m}}}.$$

Proof. Put $x = (e+u)^{\frac{1}{m}}$ and $y = e^{\frac{1}{m}}$. Since $u \ge 0$, then $x \ge y$ and
$$u = x^m - y^m = (x-y)\sum_{i=0}^{m-1} x^{m-1-i}y^i \ge (x-y)\sum_{i=0}^{m-1} y^{m-1-i}y^i = m(x-y)y^{m-1}.$$

This gives

$$x-y \leq \frac{u}{my^{m-1}}.$$

Assume that $u \leq N^{\frac{1}{4}}$. Then

$$(e+u)^{\frac{1}{m}} - e^{\frac{1}{m}} = x-y \leq \frac{u}{my^{m-1}} \leq \frac{N^{\frac{1}{4}}}{me^{1-\frac{1}{m}}},$$

which terminates the proof. ∎

Let us focus on the diophatine equation (1). The following lemma proves the existence of a link between the small solutions of this equation and the approximations of $\left(\frac{e}{\psi(N)}\right)^{\frac{1}{m}}$.

Lemma 3.5. *Let $N = pq$ with $q < p < 2q$. Let e be a public exponent and X, Y be relatively prime positive integers. Put $eY^m - \psi(n)X^m = Z$. Then*

$$\left|\frac{X}{Y} - \left(\frac{e}{\psi(N)}\right)^{\frac{1}{m}}\right| \leq \frac{2^{m-1}|Z|}{me^{1-\frac{1}{m}}\psi(N)^{\frac{1}{m}}Y^m}.$$

Proof. Let $\delta = \left(\frac{e}{\psi(N)}\right)^{\frac{1}{m}}$ and $\theta_k = \delta \exp\left(\frac{2k\pi i}{m}\right)$ for $k = 0, 1, \cdots, m-1$. We have

$$|\psi(N)X^m - eY^m| = \psi(N) \prod_{k=0}^{m-1} |X - \theta_k Y| = \psi(N)\,|X - \delta Y| \prod_{k=1}^{m-1} |X - \theta_k Y|.$$

Hence

$$|Z| = \psi(N)\,|X - \delta Y| \prod_{k=1}^{m-1} |X - \theta_k Y|. \tag{6}$$

Since $X > 0$, $Y > 0$ and $\delta > 0$, then $|X - \theta_k Y| \geq |X - \delta Y|$. Hence for $k \geq 1$,

$$|X - \theta_k Y| \geq \frac{1}{2}\left(|X - \theta_k Y| + |X - \delta Y|\right) \geq \frac{1}{2}\,|\delta - \theta_k|\,Y.$$

This gives

$$\prod_{k=1}^{m-1} |X - \theta_k Y| \geq \frac{Y^{m-1}}{2^{m-1}} \prod_{k=1}^{m-1} |\delta - \theta_k|. \tag{7}$$

Further, let $g(x) = \psi(N)x^m - e$. Then

$$\prod_{k=0}^{m-1} |x - \theta_k| = \frac{|g(x)|}{\psi(N)},$$

and

$$\prod_{k=1}^{m-1} |\delta - \theta_k| = \frac{|g'(\delta)|}{\psi(N)} = m\delta^{m-1}.$$

Combining this with (7), we get

$$\prod_{k=1}^{m-1} |X - \theta_k Y| \geq \frac{m\delta^{m-1}Y^{m-1}}{2^{m-1}}.$$

Using this inequality in (6), we get

$$|Z| \geq \psi(N)|X - \delta Y| \frac{m\delta^{m-1}Y^{m-1}}{2^{m-1}},$$

and finally

$$\left|\frac{X}{Y} - \delta\right| \leq \frac{2^{m-1}|Z|}{m\delta^{m-1}\psi(N)Y^m}.$$

Replacing $\delta = \left(\frac{e}{\psi(N)}\right)^{\frac{1}{m}}$, this proves the lemma. ∎

We end this section by the following simple lemma connecting any approximation of $p - q$ to an approximation of $p + q$.

Lemma 3.6. *Let $N = pq$ with $q < p < 2q$. Let $T > 0$ and $S = \sqrt{T^2 + 4n}$. We have*

$$|S - (p + q)| < |T - (p - q)|.$$

Proof. Using the identity $(p + q)^2 - 4n = (p - q)^2$, we get

$$\begin{aligned}
|S - (p + q)| &= \frac{\left|S^2 - (p + q)^2\right|}{S + p + q} \\
&= \frac{\left|T^2 + 4n - (p + q)^2\right|}{S + p + q} \\
&= \frac{\left|T^2 - (p - q)^2\right|}{S + p + q} \\
&= \frac{|T - (p - q)|\,(T + p - q)}{S + p + q}.
\end{aligned}$$

Since $T < S$ and $p - q < p + q$, then $T + p - q < S + p + q$. This gives

$$|S - (p + q)| < |T - (p - q)|,$$

which concludes the lemma. ∎

4 The attack algorithm

In this section we present the attack on the public exponents e verifying (1) that we have considered. Both continued fraction and Coppersmith's method techniques will be applied. We begin by linking the small solutions of the diophantine equation (1) to the diophantine approximations of $\left(\frac{e+u}{N}\right)^{\frac{1}{m}}$ for any positive integer u with $u \leq N^{\frac{1}{4}}$.

Theorem 4.1. *Let $N = pq$ with $q < p < 2q$. Let e be a public key and $m \geq 1$ be an integer. Suppose that e satisfies the equation $eY^m - \psi(N)X^m = Z$ with*

$$|Z| \leq \frac{\sqrt{3}N^{\frac{1}{4}}e + 2\psi(N)}{2^m N^{\frac{1}{m}-\frac{1}{4}}\psi(N)^{1-\frac{1}{m}}}Y^m, \tag{8}$$

and

$$Y \leq \left(\frac{me^{1-\frac{1}{m}}N^{\frac{1}{m}-\frac{1}{4}}\psi(N)}{2\left(\sqrt{3}N^{\frac{1}{4}}e + 2\psi(N)\right)}\right)^{\frac{1}{2}}. \tag{9}$$

Then for all positive integers $u \leq N^{\frac{1}{4}}$, $\dfrac{X}{Y}$ is a convergent of $\left(\dfrac{e+u}{N}\right)^{\frac{1}{m}}$.

Proof. We have

$$\left|\frac{(e+u)^{\frac{1}{m}}}{N^{\frac{1}{m}}} - \frac{X}{Y}\right| \leq \left|\frac{(e+u)^{\frac{1}{m}}}{N^{\frac{1}{m}}} - \frac{e^{\frac{1}{m}}}{N^{\frac{1}{m}}}\right| + \left|\frac{e^{\frac{1}{m}}}{\psi(N)^{\frac{1}{m}}} - \frac{e^{\frac{1}{m}}}{N^{\frac{1}{m}}}\right| + \left|\frac{e^{\frac{1}{m}}}{\psi(N)^{\frac{1}{m}}} - \frac{X}{Y}\right|. \tag{10}$$

Using Lemma 3.4, we get

$$\left|\frac{(e+u)^{\frac{1}{m}}}{N^{\frac{1}{m}}} - \frac{e^{\frac{1}{m}}}{N^{\frac{1}{m}}}\right| = \frac{\left|(e+u)^{\frac{1}{m}} - e^{\frac{1}{m}}\right|}{N^{\frac{1}{m}}} \leq \frac{N^{\frac{1}{4}-\frac{1}{m}}}{me^{1-\frac{1}{m}}}. \tag{11}$$

On the other hand, applying Lemma 3.2, we get

$$\left|\frac{e^{\frac{1}{m}}}{\psi(N)^{\frac{1}{m}}} - \frac{e^{\frac{1}{m}}}{N^{\frac{1}{m}}}\right| = \frac{e^{\frac{1}{m}}\left|N^{\frac{1}{m}} - \psi(N)^{\frac{1}{m}}\right|}{\psi(N)^{\frac{1}{m}}N^{\frac{1}{m}}} < \frac{\sqrt{3}N^{\frac{1}{2}-\frac{1}{m}}e^{\frac{1}{m}}}{2m\psi(N)}. \tag{12}$$

Finally, by Lemma 3.5, we have

$$\left|\frac{e^{\frac{1}{m}}}{\psi(N)^{\frac{1}{m}}} - \frac{X}{Y}\right| \leq \frac{2^{m-1}|Z|}{me^{1-\frac{1}{m}}\psi(N)^{\frac{1}{m}}Y^m}. \tag{13}$$

Combining (11), (12) and (13) in (10), we get

$$\begin{aligned}\left|\frac{(e+u)^{\frac{1}{m}}}{N^{\frac{1}{m}}}-\frac{X}{Y}\right| &< \frac{N^{\frac{1}{4}-\frac{1}{m}}}{me^{1-\frac{1}{m}}}+\frac{\sqrt{3}N^{\frac{1}{2}-\frac{1}{m}}e^{\frac{1}{m}}}{2m\psi(N)}+\frac{2^{m-1}|Z|}{me^{1-\frac{1}{m}}\psi(N)^{\frac{1}{m}}Y^m}\\ &= \frac{\sqrt{3}N^{\frac{1}{4}}e+2\psi(N)}{2me^{1-\frac{1}{m}}N^{\frac{1}{m}-\frac{1}{4}}\psi(N)}+\frac{2^{m-1}|Z|}{me^{1-\frac{1}{m}}\psi(N)^{\frac{1}{m}}Y^m}.\end{aligned}$$

Assume that Z satisfies (8). Then

$$\left|\frac{(e+u)^{\frac{1}{m}}}{N^{\frac{1}{m}}}-\frac{X}{Y}\right| < \frac{\sqrt{3}N^{\frac{1}{4}}e+2\psi(N)}{me^{1-\frac{1}{m}}N^{\frac{1}{m}-\frac{1}{4}}\psi(N)}.$$

Similarly, assume that Y satisfies (9). Then

$$\left|\frac{(e+u)^{\frac{1}{m}}}{N^{\frac{1}{m}}}-\frac{X}{Y}\right| < \frac{1}{2Y^2}$$

which means, by Theorem 2.2, that $\frac{X}{Y}$ is a convergent of $\left(\frac{e+u}{N}\right)^{\frac{1}{m}}$. ∎

The next theorem ensures that the modulus N can be factored if e has a more special structure.

Theorem 4.2. *Let $N = pq$ with $q < p < 2q$. Let e be a public exponent. Let m, X, Y be positive integers. If $eY^m - \psi(N)X^m = Z$ with $|Z| < 2N^{\frac{1}{4}}X^m$, then N can be factored in polynomial time.*

Proof. From $eY^m - \psi(N)X^m = Z$ with $\psi(N) = (p+1)(q-1) = N-1-(p-q)$, we get

$$p-q = N-1-\frac{eY^m}{X^m}+\frac{Z}{X^m}.$$

Let $T = \left|N-1-\frac{eY^m}{X^m}\right|$ and suppose that $|Z| < 2N^{\frac{1}{4}}X^m$. We have

$$|T-(p-q)| \le \left|\frac{Z}{X^m}\right| = \frac{|Z|}{X^m} \le 2N^{\frac{1}{4}}.$$

This means that T is an approximation of $p-q$ with an error term less than $2N^{\frac{1}{4}}$. Next, put $S = \sqrt{T^2+4N}$ and $\tilde{P} = \frac{S+T}{2}$. Applying Lemma 3.6, we get

$$|S-(p+q)| < |T-(p-q)| < 2N^{\frac{1}{4}}.$$

Hence

$$\begin{aligned}
|\tilde{P}-p| &= \frac{1}{2}|S+T-2p| \\
&= \frac{1}{2}\left|S-(p+q)+(T-(p-q))\right| \\
&\leq \frac{1}{2}\left|S-(p+q)\right|+\frac{1}{2}\left|T-(p-q)\right| \\
&< 2N^{\frac{1}{4}}.
\end{aligned}$$

It follows that $\tilde{P}$ is an approximation of p up to an error term bounded by $2N^{\frac{1}{4}}$. We can then apply Theorem 2.1 to find p and the factorization of N. ■

Let us briefly summarize the new attack. Recall that the input is a public exponent e such that $(e+u)Y^m-\psi(N)X^m=Z$ with unknown integers X, Y Z, u satisfying $0\leq u\leq N^{\frac{1}{4}}$, $|Z|<N^{\frac{1}{4}}X^m$ and the inequalities (8), (9). Notice that, since $0<e<N$, the right hand side of (9) satisfies

$$\left(\frac{me^{1-\frac{1}{m}}N^{\frac{1}{m}-\frac{1}{4}}\psi(N)}{2\left(\sqrt{3}N^{\frac{1}{4}}e+2\psi(N)\right)}\right)^{\frac{1}{2}}\leq\left(\frac{mN^{1-\frac{1}{m}}N^{\frac{1}{m}-\frac{1}{4}}\psi(N)}{4\psi(N)}\right)^{\frac{1}{2}}=\left(\frac{mN^{\frac{3}{4}}}{4}\right)^{\frac{1}{2}}=\frac{\sqrt{m}N^{\frac{3}{8}}}{2}.$$

Algorithm 4.3.

INPUT N, e.
1. $m=1$.
2. Compute $Y_0(m)=\frac{\sqrt{m}N^{\frac{3}{8}}}{2}$.
3. Compute the continued fraction expansion of $\left(\frac{e}{N}\right)^{\frac{1}{m}}$.
4. For every convergent $\frac{X}{Y}$ with $Y<Y_0$.
   i. Compute $T=\left|N-1-\frac{eY^m}{X^m}\right|$, $S=\sqrt{T^2+4N}$, $\tilde{P}=\frac{S+T}{2}$.
   ii. Apply Coppersmith's algorithm to $\tilde{P}$. If the prime factor p is found, then stop.
5. $m=m+1$. Return to Step 2 if $m\leq\frac{\log N}{\log 32}$.

OUTPUT p.

Since for every m with $1\leq m\leq\frac{\log N}{\log 32}$ there are $O(\log Y_0(m))=O(\log N)$ convergents and each step in the algortithm can be done in polynomial time in $\log N$, we can factor N in polynomial time.

5 The number of ψ-constrained keys

In Section 4, we showed that every exponent e that satisfies (1) with the inequalities of Theorem 4.1 and Theorem 4.2 yields the factorization of N. In this section, we restrict these exponents to the case where there exist small coprime positive integers X, Y such that $e = \left\lfloor \psi(N)\frac{X^m}{Y^m} \right\rfloor + 1$. We give an estimation of the number of such exponents. We begin by a corollarly of Lemma 3.3 which states a property of these exponents.

Corollarly 5.1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and m an integer with $1 \leq m \leq \frac{\log N}{\log 32}$. Let X, Y be coprime positive integers satisfying*

$$N^{-\frac{1}{4m}} Y < X < Y.$$

If $e = \left\lfloor \psi(N)\frac{X^m}{Y^m} \right\rfloor + 1$, then

$$\frac{\sqrt{3}N^{\frac{1}{4}}e + 2\psi(N)}{2^m N^{\frac{1}{m}-\frac{1}{4}}\psi(N)^{1-\frac{1}{m}}} > 1.$$

Proof. Since $e = \left\lfloor \psi(N)\frac{X^m}{Y^m} \right\rfloor + 1$, then

$$e \leq \psi(N)\frac{X^m}{Y^m} + 1 < e + 1. \tag{14}$$

Combining this with $N^{-\frac{1}{4m}} Y < X$ we get

$$e > \psi(N)\frac{X^m}{Y^m} > \frac{\psi(N)}{N^{\frac{1}{4}}}.$$

This gives

$$\sqrt{3}N^{\frac{1}{4}}e + 2\psi(N) > \sqrt{3}\psi(N) + 2\psi(N) = \left(2+\sqrt{3}\right)\psi(N)$$

On the other hand, by Lemma 3.3, we have

$$\left(2+\sqrt{3}\right)\psi(N)^{\frac{1}{m}} > 2^m N^{\frac{1}{m}-\frac{1}{4}}.$$

Multilpying this by $\psi(N)^{1-\frac{1}{m}}$ we get

$$\left(2+\sqrt{3}\right)\psi(N) > 2^m N^{\frac{1}{m}-\frac{1}{4}}\psi(N)^{1-\frac{1}{m}}.$$

Hence

$$\sqrt{3}N^{\frac{1}{4}}e + 2\psi(N) > 2^m N^{\frac{1}{m}-\frac{1}{4}}\psi(N)^{1-\frac{1}{m}},$$

and the corollarly follows. ∎

Another property of the exponents defined by $e = \left\lfloor \psi(N)\frac{X^m}{Y^m} \right\rfloor + 1$ is the following.

Lemma 5.2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and m an integer with $1 \leq m \leq \frac{\log N}{\log 32}$. Let X, Y be coprime positive integers satisfying*

$$N^{-\frac{1}{4m}} Y < X < Y.$$

If $e = \left\lfloor \psi(N)\frac{X^m}{Y^m} \right\rfloor + 1$, then

$$\frac{me^{1-\frac{1}{m}} N^{\frac{1}{m}-\frac{1}{4}} \psi(N)}{\sqrt{3}N^{\frac{1}{4}} e + 2\psi(N)} \geq \frac{m}{4} N^{\frac{1}{2}+\frac{\alpha}{m}-\alpha}.$$

Proof. Assume that $N^{-\frac{1}{4m}} Y < X < Y$. Then $1 < N^{\frac{1}{4}} \frac{X^m}{Y^m}$. Combining this with (14), we get

$$\begin{aligned}
\sqrt{3}N^{\frac{1}{4}} e + 2\psi(N) &\leq \sqrt{3}N^{\frac{1}{4}} \left(\psi(N)\frac{X^m}{Y^m} + 1 \right) + 2\psi(N) \\
&\leq 2N^{\frac{1}{4}} \psi(N)\frac{X^m}{Y^m} + 2\psi(N) \\
&= 2\psi(N) \left(N^{\frac{1}{4}} \frac{X^m}{Y^m} + 1 \right) \\
&< 4N^{\frac{1}{4}} \psi(N)\frac{X^m}{Y^m}.
\end{aligned}$$

Combinig this with (14) again, it follows that

$$\begin{aligned}
\frac{me^{1-\frac{1}{m}} N^{\frac{1}{m}-\frac{1}{4}} \psi(N)}{\sqrt{3}N^{\frac{1}{4}} e + 2\psi(N)} &> \frac{m\left(\psi(N)\frac{X^m}{Y^m} \right)^{1-\frac{1}{m}} N^{\frac{1}{m}-\frac{1}{4}} \psi(N)}{4N^{\frac{1}{4}} \psi(N)\frac{X^m}{Y^m}} \\
&= \frac{mN^{\frac{1}{m}-\frac{1}{2}} \psi(N)^{1-\frac{1}{m}} Y}{4X} \\
&> \frac{m}{4} N^{\frac{1}{m}-\frac{1}{2}} \psi(N)^{1-\frac{1}{m}} \\
&= \frac{m}{4} N^{\frac{1}{m}-\frac{1}{2}} N^{(1-\alpha)\left(1-\frac{1}{m}\right)} \\
&= \frac{m}{4} N^{\frac{1}{2}+\frac{\alpha}{m}-\alpha}.
\end{aligned}$$

and the Lemma follows. ∎

Let us show that the public exponents e defined by $e = \left\lfloor \psi(N)\frac{X^m}{Y^m} \right\rfloor + 1$ where X and Y are small positive integers should not be used in the design of an RSA cryptosystem.

Theorem 5.3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let X, Y be coprime positive integers satisfying*

$$N^{-\frac{1}{4m}}Y < X < Y < \frac{\sqrt{2m}}{4}N^{\frac{1}{4}+\frac{\alpha}{2m}-\frac{\alpha}{2}}.$$

If $e = \left\lfloor \psi(N)\frac{X}{Y} \right\rfloor + 1$, then for all u with $0 \le u \le N^{\frac{1}{4}}\left(\frac{X}{Y}\right)^m$, $\frac{X}{Y}$ is a convergent of $\left(\frac{e+u}{N}\right)^{\frac{1}{m}}$ and N can be factored in polynomial time.

Proof. Put $Z = eY^m - \psi(N)Y^m$. Since $e = \left\lfloor \psi(N)\frac{X^m}{Y^m} \right\rfloor + 1$, then using (14), we get

$$0 < e - \psi(N)\frac{X^m}{Y^m} \le 1.$$

Multiplying by Y^m, we get $0 < Z \le Y^m$. Combining this and Corollary 5.1, we get

$$0 < Z \le Y^m < \frac{\sqrt{3}N^{\frac{1}{4}}e + 2\psi(N)}{2^m N^{\frac{1}{m}-\frac{1}{4}}\psi(N)^{1-\frac{1}{m}}}Y^m.$$

Hence the inequality (8) of Theorem 4.1 is satisfied. On the other hand, by assumption $Y < \frac{\sqrt{2m}}{4}N^{\frac{1}{4}+\frac{\alpha}{2m}-\frac{\alpha}{2}}$. Then applying Lemma 5.2, we get

$$Y < \frac{\sqrt{2m}}{4}N^{\frac{1}{4}+\frac{\alpha}{2m}-\frac{\alpha}{2}} = \left(\frac{m}{8}N^{\frac{1}{2}+\frac{\alpha}{m}-\alpha}\right)^{\frac{1}{2}} \le \left(\frac{me^{1-\frac{1}{m}}N^{\frac{1}{m}-\frac{1}{4}}\psi(N)}{2\left(\sqrt{3}N^{\frac{1}{4}}e + 2\psi(N)\right)}\right)^{\frac{1}{2}}.$$

Hence the inequality (9) of Theorem 4.1 is also satisfied. Consequently, by Theorem 4.1, for all u with $0 \le u \le N^{\frac{1}{4}}$, $\frac{X}{Y}$ is a convergent of $\left(\frac{e+u}{N}\right)^{\frac{1}{m}}$. Next, put

$$Z_u = (e+u)Y^m - \psi(N)X^m = Z + uY^m.$$

Since $0 < Z \le Y^m$, $N^{-\frac{1}{4m}}Y < X$ and $0 \le u \le N^{\frac{1}{4}}\left(\frac{X}{Y}\right)^m$, we get

$$|Z_u| \le Z + |u|Y^m \le Y^m + N^{\frac{1}{4}}X^m < 2N^{\frac{1}{4}}X^m.$$

Applying Theorem 4.2, we conclude that N can be factored in polynomial time. ∎

The following lemma shows that different tuples (X, Y) lead to different exponents e with $e = \left\lfloor \psi(N)\left(\frac{X}{Y}\right)^m \right\rfloor + 1$.

Lemma 5.4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let X, Y, U, V be coprime positive integers with*

$$N^{-\frac{1}{4m}}Y < X < Y < \frac{\sqrt{2m}}{4}N^{\frac{1}{4}-\frac{\alpha}{2}+\frac{\alpha}{2m}} \quad \text{and} \quad N^{-\frac{1}{4m}}V < U < V < \frac{\sqrt{2m}}{4}N^{\frac{1}{4}-\frac{\alpha}{2}+\frac{\alpha}{2m}}.$$

Let $e = \left\lfloor \psi(N)\left(\frac{X}{Y}\right)^m \right\rfloor + 1$ and $e' = \left\lfloor \psi(N)\left(\frac{U}{V}\right)^m \right\rfloor + 1$. If $e+u = e'+u'$ for some positive integers u and u' with $0 \le u, u' \le N^{\frac{1}{4}}$ then $e = e'$.

Proof. Since $e = \left\lfloor \psi(N)\left(\frac{X}{Y}\right)^m \right\rfloor + 1$, then using (14), we get

$$u < e + u - \psi(N)\left(\frac{X}{Y}\right)^m \le 1 + u.$$

Similarly, we have

$$u' < e' + u' - \psi(N)\left(\frac{U}{V}\right)^m \le 1 + u'.$$

Combining these inequalities, we get

$$u' - u - 1 < (e' + u') - (e + u) + \psi(N)\left(\left(\frac{X}{Y}\right)^m - \left(\frac{U}{V}\right)^m\right) < u' - u + 1.$$

Suppose that $e + u = e' + u'$ with $u, u' < N^{\frac{1}{4}}$. Then

$$\psi(N)\left|\left(\frac{X}{Y}\right)^m - \left(\frac{U}{V}\right)^m\right| \le \max(|u' - u - 1|, |u' - u + 1| \le N^{\frac{1}{4}},$$

which gives

$$\psi(N)\left|(XV)^m - (YU)^m\right| \le N^{\frac{1}{4}}(YV)^m,$$

and

$$|XV - YU| \le \frac{N^{\frac{1}{4}}(YV)^m}{\psi(N)\sum_{i=0}^{m-1}(XV)^{m-1-i}(YU)^i}. \tag{15}$$

Since $X > N^{-\frac{1}{4m}}Y$ and $U > N^{-\frac{1}{4m}}V$, then

$$\begin{aligned}
\sum_{i=0}^{m-1}(XV)^{m-1-i}(YU)^i &\ge \sum_{i=0}^{m-1} N^{-\frac{m-1-i}{4m}}(YV)^{m-1-i}N^{-\frac{i}{4m}}(YV)^i \\
&= \sum_{i=0}^{m-1} N^{-\frac{m-1}{4m}}(YV)^{m-1} \\
&= mN^{-\frac{m-1}{4m}}(YV)^{m-1}.
\end{aligned}$$

Combining this with (15) we get

$$|XV - YU| \leq \frac{N^{\frac{1}{4}}(YV)^m}{m\psi(N)N^{-\frac{m-1}{4m}}(YV)^{m-1}} = \frac{N^{\frac{1}{2}-\frac{1}{4m}}YV}{m\psi(N)}.$$

Since $Y, V < \frac{\sqrt{2m}}{4}N^{\frac{1}{4}-\frac{\alpha}{2}+\frac{\alpha}{2m}}$ and $\psi(N) = N^{1-\alpha}$ with $\alpha < \frac{1}{4}$, we get

$$\frac{N^{\frac{1}{2}-\frac{1}{4m}}YV}{m\psi(N)} \leq \frac{1}{8}\frac{N^{\frac{1}{2}-\frac{1}{4m}}N^{\frac{1}{2}-\alpha+\frac{\alpha}{m}}}{N^{1-\alpha}} = \frac{1}{8}N^{\frac{4\alpha-1}{4m}} < \frac{1}{8}.$$

Summarizing, we find that

$$|XV - YU| < \frac{1}{8}.$$

Since $XV - YU$ is an integer and $\gcd(X, Y) = \gcd(U, V) = 1$, then $XV = YU$ and $X = U$, $Y = V$ implying $e = e'$. ∎

Finally, we derive a lower bound for the number of public exponents with the special atructure $e = \left\lfloor \psi(N) \left(\frac{X}{Y}\right)^m \right\rfloor + 1$ where X, Y are small positive integers.

Theorem 5.5. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. The number of $\psi(N)$-constrained exponents is at least*

$$O\left(mN^{\frac{1}{2}+\frac{\alpha}{2}-\alpha-\varepsilon}\right).$$

Proof. We will give a lower bound for the number of exponents e satisfying Theorem 5.3. Let X and Y be relatively prime integers satisfying

$$N^{-\frac{1}{4m}}Y < X < Y < \frac{\sqrt{2m}}{4}N^{\frac{1}{4}-\frac{\alpha}{2}+\frac{\alpha}{2m}}.$$

Let u be an integer with $0 \leq u \leq N^{\frac{1}{4}}\frac{X^m}{Y^m}$. Let e be defined by $e = \left\lfloor \psi(N) \left(\frac{X}{Y}\right)^m \right\rfloor + 1$. The uniqueness of e is assured by Lemma 5.4. Put

$$X_0 = \left\lceil N^{-\frac{1}{4m}}Y \right\rceil \qquad \text{and} \qquad Y_0 = \left\lfloor \frac{\sqrt{2m}}{4}N^{\frac{1}{4}-\frac{\alpha}{2}+\frac{\alpha}{2m}} \right\rfloor.$$

The number of the exponents $e + u$ defined before is

$$\Omega = \sum_{Y=1}^{Y_0} \sum_{\substack{X=X_0 \\ \gcd(X,Y)=1}}^{Y-1} N^{\frac{1}{4}}\frac{X^m}{Y^m}.$$

Since $N^{-\frac{1}{4m}}Y < X$, then trivially $N^{\frac{1}{4}}\frac{X^m}{Y^m} > 1$. Hence

$$\Omega > \sum_{Y=1}^{Y_0} \sum_{\substack{X=X_0 \\ \gcd(X,Y)=1}}^{Y-1} 1 = \sum_{Y=1}^{Y_0} \frac{Y-X_0}{Y}\phi(Y) = \left(1 - N^{-\frac{1}{4m}}\right) \sum_{Y=1}^{Y_0} \phi(Y).$$

Recall that $\phi(Y)$ is the Euler totient function and satisfies (see [10])

$$\phi(Y) \geq \frac{e^{-\lambda}Y}{9\log\log(Y)} \geq \frac{Y}{\log\log(N)} = N^{-\varepsilon}Y,$$

where γ is the Euler-Mascheroni constant and ε is a small positive constant. We get finally

$$\begin{aligned}\Omega &> \left(1 - N^{-\frac{1}{4m}}\right) N^{-\varepsilon} \sum_{Y=1}^{Y_0} Y \\ &= \left(1 - N^{-\frac{1}{4m}}\right) N^{-\varepsilon} \frac{Y_0(Y_0+1)}{2} \\ &\geq \frac{m}{16}\left(1 - N^{-\frac{1}{4m}}\right) N^{-\varepsilon} N^{\frac{1}{2}+\frac{\alpha}{m}-\alpha}.\end{aligned}$$

Since $m \leq \frac{\log N}{\log 32}$, then $1 - N^{-\frac{1}{4m}} \geq \frac{1}{2}$, which concludes the proof. ■

References

1. J. Blömer, A. May, *A generalized Wiener attack on RSA*, In Practice and Theory in Public Key Cryptography (PKC 2004), Lecture Notes in Computer Science, Springer-Verlag **2947** (2004), 1–13.
2. D. Boneh, G. Durfee, *Cryptanalysis of RSA with private key d less than* $N^{0.292}$, IEEE Transactions on Information Theory **46** (2000), 1339–1349.
3. D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, Journal of Cryptology **10 (4)** (1997), 223–260.
4. A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29** (2004), 101–112.
5. S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley Pub. Co,, 1966.
6. A. May, *New RSA Vulnerabilities Using Lattice Reduction Methods*, PhD thesis, University of Paderborn, (2003), `http://wwwcs.upb.de/cs/ag-bloemer/personen/alex/publikationen/`.
7. A. Nitaj, *Cryptanalysis of RSA with constrained keys*, Appl. Algebra Eng. Commun. Comput., Submitted.
8. E. R. Verheul, H. C. A. van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Appl. Algebra Eng. Commun. Comput. **8** (1997), 425–435.
9. B. de Weger, *Cryptanalysis of RSA with small prime difference*, Appl. Algebra Eng. Commun. Comput. **13** (2002), 17–28.
10. E. W. Weisstein, *Totient Function*, From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/TotientFunction.html`.
11. M. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory **36** (1990), 553-558.