Another Generalization of Wiener's Attack on RSA

Abderrahmane Nitaj

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, France
BP 5186, 14032 Caen Cedex, France
http://www.math.unicaen.fr/~nitaj
nitaj@math.unicaen.fr

Abstract. A well-known attack on RSA with low secret-exponent d was given by Wiener in 1990. Wiener showed that using the equation $ed-(p-1)(q-1)k=1$ and continued fractions, one can efficiently recover the secret-exponent d and factor $N=pq$ from the public key (N,e) as long as $d<\frac{1}{3}N^{\frac{1}{4}}$. In this paper, we present a generalization of Wiener's attack. We show that every public exponent e that satisfies $eX-(p-u)(q-v)Y=1$ with

$$1\leq Y<X<2^{-\frac{1}{4}}N^{\frac{1}{4}},\ |u|<N^{\frac{1}{4}},\ v=\left\lfloor -\frac{qu}{p-u}\right\rfloor,$$

and all prime factors of $p-u$ or $q-v$ are less than 10^{50} yields the factorization of $N=pq$. We show that the number of these exponents is at least $N^{\frac{1}{2}-\varepsilon}$.

KEYWORDS: RSA, Cryptanalysis, ECM, Coppersmith's method, Smooth numbers

1 Introduction

The RSA cryptosystem invented by Rivest, Shamir and Adleman [20] in 1978 is today's most important public-key cryptosystem. The security of RSA depends on mainly two primes p, q of the same bit-size and two integers e, d satisfying $ed\equiv 1 \pmod{(p-1)(q-1)}$. Throughout this paper, we label the primes so that $q<p<2q$. The RSA modulus is given by $N=pq$ and Euler's totient function is $\phi(N)=(p-1)(q-1)$. The integer e is called the public (or encrypting) exponent and d is called the private (or decrypting) exponent.

To reduce the decryption time or the signature-generation time, one may wish to use a short secret exponent d. This was cryptanalysed by Wiener [22] in 1990 who showed that RSA is insecure if $d<\frac{1}{3}N^{0.25}$. Wiener's method is based on continued fractions. These results were extended by Boneh and Durfee [3] in 1999 to $d<N^{0.292}$. The method of Boneh and Durfee is based on Coppersmith's results for finding small solutions of modular polynomial equations [6]. In 2004,

Blömer and May [2] presented a generalization of Wiener's attack by combining continued fractions and Coppersmith's method. They showed that RSA is insecure for every (N, e) satisfying $ex + y \equiv 0 \pmod{\phi(N)}$ with $x < \frac{1}{3}N^{1/4}$ and $|y| = O\left(N^{-3/4}ex\right)$.

In this paper, we present another generalization of Wiener's attack. Our method combines continued fractions, integer partial factorization, integer relation detection algorithms and Coppersmith's method. Let us introduce the polynomial

$$\psi(u, v) = (p - u)(q - v).$$

Observe that $\psi(1, 1) = (p - 1)(q - 1) = \phi(N)$, so ψ could be seen as a generalization of Euler's function. We describe an attack on RSA that works for all public exponents e satisfying

$$eX - \psi(u, v)Y = 1, \tag{1}$$

with integers X, Y, u, v such that

$$1 \leq Y < X < 2^{-\frac{1}{4}}N^{\frac{1}{4}}, \quad |u| < N^{\frac{1}{4}}, \quad v = \left\lfloor -\frac{qu}{p-u} \right\rceil,$$

with the extra condition that all prime factors of $p-u$ or $q-v$ are less than the Elliptic Curve Method of Factoring smoothness bound $B_{\text{ecm}} = 10^{50}$. Here and throughout this paper, we let $\lfloor x \rceil$ and $\lfloor x \rfloor$ denote the nearest integer to the real number x and the fractional part of x.

Observe that when $u = 1$, we get $v = -1$ and rewriting (1) as

$$eX - (p - 1)(q + 1)Y = 1,$$

a variant of Wiener's attack enables us to compute p and q without assuming any additional condition on the prime divisors of $p - 1$ nor $q + 1$.

Our new method works as follows: We use the Continued Fraction Algorithm (see e.g. [11], p. 134) to find the unknowns X and Y among the convergents of $\frac{e}{N}$. Then we use Lenstra's Elliptic Curve Factorization Method (ECM) [14] to partially factor $\frac{eX-1}{Y}$. Afterwards, we use an integer relation detection algorithm (notably LLL [15] or PSLQ [7]) to find the divisors of the B_{ecm}-smooth part of $\frac{eX-1}{Y}$ in a short interval. Finally, we show that a method due to Coppersmith [6] can be applied. Moreover, we show that the number of keys (N, e) for which our method works is at least $N^{\frac{1}{2}-\varepsilon}$.

Organization of the paper. Section 2 presents well known results from number theory that we use. After presenting some useful lemmas in Section 3, and some properties of ψ in Section 4, we present our attack in Section 5 and in Section 6, we show that the number of keys (N, e) for which our method works is lower bounded by $N^{\frac{1}{2}-\varepsilon}$. We briefly conclude the paper in Section 7.

2 Preliminaries

2.1 Continued fractions and Wiener's attack

The continued fraction expansion of a real number ξ is an expression of the form

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N} - \{0\}$ for $i \geq 1$. The numbers $a_0, a_1, a_2, \cdots$ are called the partial quotients. As usual, we adopt the notation $\xi = [a_0, a_1, a_2, \cdots]$. For $i \geq 0$, the rationals $\frac{r_i}{s_i} = [a_0, a_1, a_2, \cdots, a_i]$ are called the convergents of the continued fraction expansion of ξ. If $\xi = \frac{a}{b}$ is rational with $\gcd(a, b) = 1$, then the continued fraction expansion is finite and the Continued Fraction Algorithm (see [11], p. 134) finds the convergents in time $O((\log b)^2)$. We recall a result on diophantine approximations (see Theorem 184 of [11]).

Theorem 1. *Suppose* $\gcd(a, b) = \gcd(x, y) = 1$ *and*

$$\left|\frac{a}{b} - \frac{x}{y}\right| < \frac{1}{2y^2}.$$

Then $\frac{x}{y}$ *is one of the convergents of the continued fraction expansion of* $\frac{a}{b}$.

Let us recall Wiener's famous attack on RSA with $N = pq$ and $q < p < 2q$. The idea behind Wiener's attack on RSA [22] with small secret exponent d is that for $d < \frac{1}{3}N^{1/4}$, the fraction e/N is an approximation to k/d and hence, using Theorem 1, k/d can be found from the convergents of the continued fraction expansion of e/N. Wiener's attack works as follows. Since $ed - k\phi(N) = 1$ with $\phi(N) = N - (p + q - 1)$ and $p + q - 1 < 3\sqrt{N}$ then $kN - ed = k(p + q - 1) - 1$. Therefore,

$$\left|\frac{k}{d} - \frac{e}{N}\right| = \frac{|k(p + q - 1) - 1|}{Nd} < \frac{3k\sqrt{N}}{Nd}.$$

Now, assume that $d < \frac{1}{3}N^{1/4}$. Since $k\phi(N) = ed - 1 < ed$ and $e < \phi(N)$, then $k < d < \frac{1}{3}N^{1/4}$. Hence

$$\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{N^{3/4}}{Nd} = \frac{1}{dN^{1/4}} < \frac{1}{2d^2}.$$

From Theorem 1, we know that k/d is one of the convergents of the continued fraction expansion of e/N.

2.2 Coppersmith's method

The problem of finding small modular roots of a univariate polynomial has been extensively studied by Coppersmith [6], Howgrave-Graham [13], May [17] and others. Let $f(x)$ be a monic univariate polynomial with integer coefficients of degree δ. Let N be an integer of unknown factorization and $B = N^{1/\delta}$. The problem is to find all integers x_0 such that $|x_0| < B$ and $f(x_0) \equiv 0 \pmod N$. In 1997, Coppersmith presented a deterministic algorithm using $\left(2^\delta \log N\right)^{O(1)}$ bit operations to solve this problem. The algorithm uses lattice reduction techniques, and as an application, the following theorem was proved (see also [17], Theorem 11).

Theorem 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Given an approximation $\tilde{p}$ of p with $|p - \tilde{p}| < N^{\frac{1}{4}}$, N can be factored in time polynomial in $\log N$.*

2.3 Smooth numbers

A few words about notation: let f and g be functions of x. The notation $f \asymp g$ denotes that $f(x)/g(x)$ is bounded above and below by positive numbers for large values of x. The notation $f = O(g)$ denotes that $\exists c$ such that $f(x) \leq cg(x)$. The notation $f \sim g$ denotes that $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Let y be a positive constant. A positive number n is y-smooth if all prime factors of n are less than y. As usual, we use the notation $\Psi(x, y)$ for the counting function of the y-smooth numbers in the interval $[1, x]$, that is,

$$\Psi(x, y) = \#\left\{n : 1 \leq n \leq x,\ n \text{ is } y\text{-smooth}\right\}.$$

The ratio $\Psi(x, y)/[x]$ may be interpreted as the probability that a randomly chosen number n in the interval $[1, x]$ has all its prime factors less than y. The function $\Psi(x, y)$ plays a central role in the running times of many integer factoring and discrete logarithm algorithms, including the Elliptic Curve Method (ECM) [14] and the number field sieve method (NFS) [16]. Let $\rho(u)$ be the Dickman-de Bruijn function (see [9]). In 1986, Hildebrand [12] showed that

$$\Psi(x, y) = x\rho(u)\left\{1 + O\left(\frac{\log(u + 1)}{\log y}\right)\right\} \quad \text{where} \quad x = y^u \tag{2}$$

holds uniformly in the range $y > \exp\left\{(\log\log x)^{5/3+\varepsilon}\right\}$. Studying the distribution in short intervals of integers without large prime factors, Friedlander and Granville [8] showed that

$$\Psi(x + z, y) - \Psi(x, y) \geq c\frac{z}{x}\Psi(x, y), \tag{3}$$

in the range $x \geq z \geq x^{\frac{1}{2}+\delta}$, $x \geq y \geq x^{1/\gamma}$ and x is sufficiently large where δ and γ are positive constants and $c = c(\delta, \gamma) > 0$.

In order to study the distribution of divisors of a positive integer n, Hall and Tenenbaum [10] studied the counting function

$$U(n,\alpha) = \#\left\{(d,d') : d|n, d'|n, \gcd(d,d') = 1, \left|\log\frac{d}{d'}\right| < (\log n)^{\alpha}\right\}, \quad (4)$$

where α is a real number. They proved that for any fixed $\alpha < 1$ and almost all n,

$$U(n,\alpha) \leq (\log n)^{\log 3 - 1 + \alpha + o(1)}, \quad (5)$$

where the $o(1)$ term tends to 0 as n tends to $+\infty$.

2.4 ECM

The Elliptic Curve Method (ECM) was originally proposed by H.W. Lenstra [14] in 1984 and then extended by Brent [4] and Montgomery [18]. It is suited to find small prime factors of large numbers. The original part of the algorithm proposed by Lenstra is referred to as Phase 1, and the extension by Brent and Montgomery is called Phase 2. ECM relies on Hasse's theorem: if p is a prime factor of a large number M, then an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ has group order $p + 1 - t$ with $|t| < 2\sqrt{p}$, where t depends on the curve. If $p + 1 - t$ is a smooth number, then ECM will probably succeed and reveal the unknown factor p. ECM is a sub-exponential factoring algorithm, with expected run time of

$$O\left(\exp\left\{\sqrt{(2 + o(1))\log p \log\log p}\right\} Mult(M)\right)$$

where the $o(1)$ term tends to 0 as p tends to $+\infty$ and $Mult(M)$ denotes the cost of multiplication mod M. The largest factor known to have been found by ECM is a 67-digit factor of the number $10^{381} + 1$, found by B. Dodson with P. Zimmerman's GMP-ECM program in August 2006 (see [23]). According to Brent's formula [5] $\sqrt{D} = (Y - 1932.3)/9.3$ where D is the number of decimal digits in the largest factor found by ECM up to a given date Y, a 70-digit factor could be found by ECM around 2010.

In Table 1, we give the running times obtained on a Intel(R) Pentium(R) 4 CPU 3.00 GHz to factor an RSA modulus $N = pq$ of size $2n$ bits with $q < p < 2q$ with ECM, using the algebra system Pari-GP[19].

Table 1. Running times for factoring $N = pq$ with $q < p < 2q$

n = Number of bits of q	60	70	80	90	100	110	120	130
T = Time in seconds	0.282	0.844	3.266	13.453	57.500	194.578	921.453	3375.719

Extrapolating Table 1, we find the formula

$$\log T = 2.609\sqrt{n} - 21.914 \quad \text{or equivalently} \quad T = \exp\left\{2.609\sqrt{n} - 21.914\right\},$$

where T denotes the running time to factor an RSA modulus $N = pq$ with $2n$ bits. Extrapolating, we can extract a prime factor of 50 digits (≈ 166 bits) in 1 day, 9 hours and 31 minutes. Throughout this paper, we then assume that ECM is efficient to extract prime factors up to the bound $B_{\text{ecm}} = 10^{50}$.

3 Useful lemmas

In this section we prove three useful lemmas. We begin with a simple lemma fixing the sizes of the prime factors of the RSA modulus.

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

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

Proof. Assume $q < p < 2q$. Multiplying by p, we get $N < p^2 < 2N$ or equivalently $N^{\frac{1}{2}} < p < \sqrt{2}N^{\frac{1}{2}}$. Since $q = \frac{N}{p}$, we obtain $2^{-\frac{1}{2}} N^{\frac{1}{2}} < q < N^{\frac{1}{2}}$ and the lemma follows. □

Our second lemma is a consequence of Theorem 2 and Lemma 1.

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose $|u| < N^{\frac{1}{4}}$. If $p - u < N^{\frac{1}{2}}$ or $p - u > \sqrt{2}N^{\frac{1}{2}}$, then the factorization of N can be found in polynomial time.*

Proof. Assume $q < p < 2q$ and $|u| < N^{\frac{1}{4}}$. If $p - u < N^{\frac{1}{2}}$, then $p < N^{\frac{1}{2}} + u < N^{\frac{1}{2}} + N^{\frac{1}{4}}$. Combining this with Lemma 1, we obtain

$$N^{\frac{1}{2}} < p < N^{\frac{1}{2}} + N^{\frac{1}{4}}.$$

It follows that $\tilde{p} = N^{\frac{1}{2}}$ is an approximation of p with $0 < p - \tilde{p} < N^{\frac{1}{4}}$. By Theorem 2, we deduce that the factorization of N can be found in polynomial time.

Similarly, if $p - u > \sqrt{2}N^{\frac{1}{2}}$, then $p > \sqrt{2}N^{\frac{1}{2}} + u > \sqrt{2}N^{\frac{1}{2}} - N^{\frac{1}{4}}$ and using Lemma 1, we get

$$\sqrt{2}N^{\frac{1}{2}} > p > \sqrt{2}N^{\frac{1}{2}} - N^{\frac{1}{4}}.$$

It follows that $\tilde{p} = \sqrt{2}N^{\frac{1}{2}}$ satisfies $0 > p - \tilde{p} > -N^{\frac{1}{4}}$. Again, by Theorem 2, we conclude that the factorization of N can be found in polynomial time. □

Our third lemma is a consequence of the Fermat Factoring Method (see e.g. [21]). We show here that it is an easy consequence of Theorem 2 and Lemma 1.

Lemma 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. If $p - q < N^{\frac{1}{4}}$, then the factorization of N can be found in polynomial time.*

Proof. Assume $q < p < 2q$ and $p - q < N^{\frac{1}{4}}$. Combining with Lemma 1, we get

$$N^{\frac{1}{2}} < p < q + N^{\frac{1}{4}} < N^{\frac{1}{2}} + N^{\frac{1}{4}}.$$

It follows that $\tilde{p} = N^{\frac{1}{2}}$ is an approximation of p with $0 < p - \tilde{p} < N^{\frac{1}{4}}$. By Theorem 2, we conclude that the factorization of N can be found in polynomial time. □

4 Properties of $\psi(u, v)$

Let $N = pq$ be an RSA modulus with $q < p < 2q$. The principal object of investigation of this section is the polynomial $\psi(u, v) = (p - u)(q - v)$ when p and q are fixed.

Lemma 4. *Let u be an integer with $|u| < N^{\frac{1}{4}}$. Put $v = \left\lfloor -\frac{qu}{p-u} \right\rceil$. Then*

$$|\psi(u, v) - N| < 2^{-\frac{1}{2}} N^{\frac{1}{2}}.$$

Proof. Since v is the nearest integral value to $-\frac{qu}{p-u}$, then

$$-\frac{1}{2} \leq -\frac{qu}{p-u} - v < \frac{1}{2}.$$

Hence

$$q + \frac{qu}{p-u} - \frac{1}{2} \leq q - v < q + \frac{qu}{p-u} + \frac{1}{2}.$$

Multiplying by $p - u$, we get

$$N - \frac{1}{2}(p-u) \leq (p-u)(q-v) < N + \frac{1}{2}(p-u).$$

It follows that

$$|(p-u)(q-v) - N| \leq \frac{1}{2}(p-u).$$

Since $|u| < N^{\frac{1}{4}}$, then by Lemma 2, we can assume $p - u < \sqrt{2} N^{\frac{1}{2}}$ and we obtain

$$|(p-u)(q-v) - N| \leq 2^{-\frac{1}{2}} N^{\frac{1}{2}}.$$

This completes the proof. □

Lemma 5. *Let u be an integer with $|u| < N^{\frac{1}{4}}$. Set $v = \left\lfloor -\frac{qu}{p-u} \right\rceil$. Then $|v| \leq |u|$.*

Proof. Assume $q < p < 2q$ and $|u| < N^{\frac{1}{4}}$. By Lemma 3, we can assume that $p - q > N^{\frac{1}{4}}$. Then

$$u < N^{\frac{1}{4}} < p - q,$$

and $q < p - u$. Hence

$$|v| = \left\lfloor \frac{q|u|}{p-u} \right\rfloor \leq \frac{q|u|}{p-u} + \frac{1}{2} < |u| + \frac{1}{2}.$$

Since u and v are integers, then $|v| \leq |u|$ and the lemma follows. □

Lemma 6. *Let u, u', be integers with $|u|, |u'| < N^{\frac{1}{4}}$. Define*

$$v = \left\lfloor -\frac{qu}{p-u} \right\rceil \quad \text{and} \quad v' = \left\lfloor -\frac{qu'}{p-u'} \right\rceil.$$

If $v = v'$, then $|u' - u| \leq 1$.

Proof. Suppose $v' = v$. Then, from the definitions of v and v', we obtain

$$\left| \frac{qu'}{p-u'} - \frac{qu}{p-u} \right| < 1,$$

Transforming this, we get

$$|u' - u| < \frac{(p-u)(p-u')}{N}.$$

By Lemma 3 we can assume that $p - u < \sqrt{2}N^{\frac{1}{2}}$ and $p - u' < \sqrt{2}N^{\frac{1}{2}}$. Then

$$|u' - u| < \frac{\left(\sqrt{2}N^{\frac{1}{2}}\right)^2}{N} = 2.$$

Since u and u' are integers, the lemma follows. □

Lemma 7. *Let u, u', be integers with $|u|, |u'| < N^{\frac{1}{4}}$. Define*

$$v = \left[-\frac{qu}{p-u} \right] \quad \text{and} \quad v' = \left[-\frac{qu'}{p-u'} \right].$$

If $\psi(u, v) = \psi(u', v')$, then $u = u'$.

Proof. Assume that $\psi(u, v) = \psi(u', v')$, that is $(p-u)(q-v) = (p-u')(q-v')$. If $v = v'$, then $p-u = p-u'$ and $u = u'$. Next, assume for contradiction that $v \neq v'$. Without loss of generality, assume that $u > u'$. Put $\psi = \psi(u, v) = \psi(u', v')$ and let $U(\psi, \alpha)$ as defined by (4), i.e.

$$U(\psi, \alpha) = \# \left\{ (d, d') : d|\psi, d'|\psi, \gcd(d, d') = 1, \left| \log \frac{d}{d'} \right| < (\log \psi)^{\alpha} \right\}.$$

Let $g = \gcd(p-u, p-u')$, $d = \frac{p-u}{g}$ and $d' = \frac{p-u'}{g}$. Hence $\gcd(d, d') = 1$. We have

$$\frac{d}{d'} = \frac{p-u}{p-u'} = 1 - \frac{u-u'}{p-u'}.$$

By Lemma 2, we can assume that $p - u > N^{\frac{1}{4}}$. For $N > 2^8$ we have

$$0 < \frac{u-u'}{p-u'} < \frac{2N^{\frac{1}{4}}}{N^{\frac{1}{2}}} = 2N^{-\frac{1}{4}} < \frac{1}{2}.$$

Using that $|\log(1-x)| < 2x$ holds for $0 < x < \frac{1}{2}$ this yields

$$\left| \log \frac{d}{d'} \right| = \left| \log \left(1 - \frac{u-u'}{p-u'} \right) \right| < 2 \times \frac{u-u'}{p-u'} < 2\sqrt{2}N^{-\frac{1}{4}} = (\log \psi)^{\alpha},$$

where

$$\alpha = \frac{\log \left(2\sqrt{2}N^{-\frac{1}{4}} \right)}{\log(\log(\psi))}.$$

It follows that $U(\psi, \alpha) \geq 1$. On the other hand, we have

$$\alpha = \frac{\log\left(2\sqrt{2}N^{-\frac{1}{4}}\right)}{\log(\log(\psi))} \leq \frac{\log\left(2\sqrt{2}N^{-\frac{1}{4}}\right)}{\log\left(\log\left(N - 2^{-\frac{1}{2}}N^{\frac{1}{2}}\right)\right)} < 1 - \log 3,$$

where we used Lemma 4 in the medium step and $N > 2^7$ in the final step. Using the bound (5), we have actually

$$U(\psi, \alpha) \leq (\log \psi)^{\log 3 - 1 + \alpha + o(1)} \leq (\log N)^{\delta + o(1)},$$

where $\delta = \log 3 - 1 + \alpha < 0$ and we deduce $U(\psi, \alpha) = 0$, a contradiction. Hence $v = v'$, $u = u'$ and the lemma follows. □

Lemma 8. *Let u, u' be integers with $|u|, |u'| < N^{\frac{1}{4}}$. Define*

$$v = \left\lfloor -\frac{qu}{p-u} \right\rfloor \quad \textit{and} \quad v' = \left\lfloor -\frac{qu'}{p-u'} \right\rfloor.$$

Assume that $\psi(u, v) < \psi(u', v')$. Let $[a_0, a_1, a_2, \cdots]$ be the continued fraction expansion of $\frac{\psi(u,v)}{\psi(u',v')}$. Then $a_0 = 0$, $a_1 = 1$ and $a_2 > 2^{-\frac{1}{2}}N^{\frac{1}{2}} - \frac{1}{2}$.

Proof. Let us apply the continued fraction algorithm (see e.g. of [11], p. 134). Assuming $\psi(u, u) < \psi(u', v')$, we get

$$a_0 = \left\lfloor \frac{\psi(u, v)}{\psi(u', v')} \right\rfloor = 0.$$

Next, we have

$$a_1 = \left\lfloor \frac{1}{\frac{\psi(u,v)}{\psi(u',v')} - a_0} \right\rfloor = \left\lfloor \frac{\psi(u', v')}{\psi(u, v)} \right\rfloor.$$

By Lemma 4, we have

$$0 < \psi(u', v') - \psi(u, v) \leq |\psi(u, v) - N| + |\psi(u', v') - N| < \sqrt{2}N^{\frac{1}{2}}. \tag{6}$$

Combining this with Lemma 4, we get

$$0 < \frac{\psi(u', v')}{\psi(u, v)} - 1 = \frac{\psi(u', v') - \psi(u, v)}{\psi(u, v)} < \frac{\sqrt{2}N^{\frac{1}{2}}}{\psi(u, v)} < \frac{\sqrt{2}N^{\frac{1}{2}}}{N - 2^{-\frac{1}{2}}N^{\frac{1}{2}}} < 1.$$

From this, we deduce $a_1 = 1$. Finally, combining (6) and Lemma 4, we get

$$a_2 = \left\lfloor \frac{1}{\frac{\psi(u',v')}{\psi(u,v)} - a_1} \right\rfloor = \left\lfloor \frac{\psi(u, v)}{\psi(u', v') - \psi(u, v)} \right\rfloor > \frac{N - 2^{-\frac{1}{2}}N^{\frac{1}{2}}}{\sqrt{2}N^{\frac{1}{2}}} = 2^{-\frac{1}{2}}N^{\frac{1}{2}} - \frac{1}{2}.$$

This completes the proof. □

5 The new attack

In this section we state our new attack. Let $N = pq$ be an RSA modulus with $q < p < 2p$. Let e be a public exponent satisfying an equation $eX - \psi(u, v)Y = 1$ with integers X, Y, u, v such that

$$1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}, \quad |u| < N^{\frac{1}{4}}, \quad v = \left\lfloor -\frac{qu}{p-u} \right\rfloor,$$

and with the condition that all prime factors of $p-u$ or $q-v$ are $\leq B_{\text{ecm}} = 10^{50}$. Our goal is to solve this equation. As in Wiener's approach, we use the continued fraction algorithm to recover the unknown values X and Y.

Theorem 3. *Let $N = pq$ be an RSA modulus with $q < p < 2p$. Suppose that the public exponent e satisfies an equation $eX - \psi(u, v)Y = 1$ with*

$$|u| < N^{\frac{1}{4}}, \quad v = \left\lfloor -\frac{qu}{p-u} \right\rfloor, \quad 1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}.$$

Then $\frac{Y}{X}$ is one of the convergents of the continued fraction expansion of $\frac{e}{N}$.

Proof. Starting with the equation $eX - \psi(u, v)Y = 1$, we get

$$eX - NY = 1 - (N - \psi(u, v))Y.$$

Together with Lemma 4, this implies

$$\begin{aligned} \left| \frac{e}{N} - \frac{Y}{X} \right| &= \frac{|1 - (N - \psi(u, v))Y|}{NX} \\ &\leq \frac{1 + |(N - \psi(u, v))|\, Y}{NX} \\ &\leq \frac{1 + 2^{-\frac{1}{2}} N^{\frac{1}{2}} Y}{NX} \\ &\leq \frac{2 + \sqrt{2} N^{\frac{1}{2}} (X - 1)}{2NX}. \end{aligned}$$

Suppose we can upperbound the right-hand side term by $\frac{1}{2X^2}$, that is

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

then, applying Theorem 1 the claim follows. Rearranging to isolate X, this leaves us with the condition

$$\sqrt{2} N^{\frac{1}{2}} X^2 - \left(\sqrt{2} N^{\frac{1}{2}} - 2 \right) X - N < 0.$$

It is not hard to see that the condition is satisfied if $X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$. This gives us the theorem. □

Afterwards, we combine ECM, integer relation detection algorithms and Coppersmith's method to factor $N = pq$.

Theorem 4. *Let $N = pq$ be an RSA modulus with $q < p < 2p$. Let B_{ecm} be the ECM-bound. Suppose that the public exponent $e < N$ satisfies an equation $eX - \psi(u, v)Y = 1$ with*

$$|u| < N^{\frac{1}{4}}, \quad v = \left[-\frac{qu}{p-u}\right], \quad 1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}.$$

If $p - u$ or $q - v$ is B_{ecm}-smooth, then we can efficiently factor N.

Proof. By Theorem 3 we know that X and Y can be found among the convergents of the continued expansion of $\frac{e}{N}$. From X and Y, we get

$$\psi(u, v) = (p - u)(q - v) = \frac{eX - 1}{Y}.$$

Without loss of generality, suppose that $p - u$ is B_{ecm}-smooth. Using ECM, write $\frac{eX-1}{Y} = M_1 M_2$ where M_1 is B_{ecm}-smooth. Let $\omega(M_1)$ denote the number of distinct prime factors of M_1. Then the prime factorization of M_1 is of the form

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i},$$

where the $a_i \geq 1$ are integers and the p_i are distinct primes $\leq B_{\text{ecm}}$. Since $p - u$ is B_{ecm}-smooth, then $p - u$ a divisor of M_1, so that

$$p - u = \prod_{i=1}^{\omega(M_1)} p_i^{x_i}, \tag{7}$$

where the x_i are integers satisfying $0 \leq x_i \leq a_1$. By Lemma 2, we can assume that $N^{\frac{1}{2}} < p - u < \sqrt{2} N^{\frac{1}{2}}$. Combining this with (7) and taking logarithms, we get

$$0 < \sum_{i=1}^{\omega(M_1)} x_i \log p_i - \frac{1}{2} \log N < \frac{1}{2} \log 2. \tag{8}$$

These inequalities are related to Baker's famous theory of linear forms in logarithms [1] and can be formulated as a nearly closest lattice problem in the 1-norm. They can be solved using the LLL [15] or the PSLQ algorithm [7]. The complexity of LLL and PSLQ depends on $\omega(M_1)$. Since Hardy and Ramanujan (see e.g.Theorem 431 of [11]), we know that, in average, $\omega(M_1) \sim \log \log M_1$ if M_1 is uniformly distributed. Since $X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$, we have for $e < N$

$$M_1 \leq \frac{eX - 1}{Y} < \frac{eX}{Y} \leq eX < N^{\frac{5}{4}},$$

This implies that the number of primes dividing M_1 satisfies

$$\omega(M_1) \sim \log\log M_1 \sim \log\log N.$$

Next, let us investigate the number of solutions of (8) which is related to the number of divisors of M_1. Let $\tau(M_1)$ denote the number of positive divisors of M_1. The prime decomposition of M_1 gives the exact value

$$\tau(M_1) = \prod_{i=1}^{\omega(M_1)} (1+a_i).$$

By Dirichlet's Theorem, we know that if M_1 is uniformly distributed, then the average order of $\tau(M_1)$ is $\log M_1$ (see Theorem 319 of [11]). It follows that the average number of divisors of M_1 is

$$\tau(M_1) \sim \log(M_1) \sim \log(N).$$

This gives in average the number of solutions to the inequalities (8).

Next, let D be a divisor of M_1 satisfying (8). If D is a good candidate for $p-u$ with $|u| < N^{\frac{1}{4}}$, then applying Theorem 2, we get the desired factor p. This concludes the theorem. □

Notice that the running time is dominated by ECM since every step in our attack can be done in polynomial time and the number of convergents and divisors are bounded by $O(\log N)$.

6 The number of exponents for the new method

In this section, we estimate the number of exponents for which our method works. Let $N = pq$ be an RSA modulus with $q < p < 2q$. The principal object of investigation of this section is the set

$$H(N) = \left\{ e : e < N,\ \exists u \in V(p),\ \exists X < 2^{-\frac{1}{4}} N^{\frac{1}{4}},\ e \equiv X^{-1} \pmod{\psi(u,v)} \right\},$$

where

$$V(p) = \left\{ u :\ |u| < p^{\frac{1}{2}},\ p-u \text{ is } B_{\text{ecm}}\text{-smooth} \right\}, \tag{9}$$

and $v = \left\lfloor -\frac{qu}{p-u} \right\rfloor$.

We will first show that every public exponent $e \in H(N)$ is uniquely defined by a tuple (u, X). We first deal with the situation when an exponent e is defined by different tuples (u, X) and (u, X').

Lemma 9. *Let $N = pq$ be an RSA modulus with $q < p < 2p$. Let u, v, X, X' be integers with $1 \le X, X' < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$ and $\gcd(XX', \psi(u,v)) = 1$ where $v = \left\lfloor -\frac{qu}{p-u} \right\rfloor$. Define*

$$e \equiv X^{-1} \pmod{\psi(u,v)} \quad \text{and} \quad e' \equiv X'^{-1} \pmod{\psi(u,v)}.$$

If $e = e'$, then $X = X'$.

Proof. Since $e \equiv X^{-1} \pmod{\psi(u,v)}$, there exists a positive integer Y such that $eX - \psi(u,v)Y = 1$ with $\gcd(X,Y) = 1$. Similarly, e' satisfies $e'X' - \psi(u,v)Y' = 1$ with $\gcd(X',Y') = 1$. Assume that that $e = e'$. Then

$$\frac{1+\psi(u,v)Y}{X} = \frac{1+\psi(u,v)Y'}{X'}.$$

Combining this with Lemma 4, we get

$$|XY' - X'Y| = \frac{|X'-X|}{\psi(u,v)} < \frac{2^{-\frac{1}{4}}N^{\frac{1}{4}}}{N - 2^{-\frac{1}{2}}N^{\frac{1}{2}}} < 1.$$

Hence $XY' = X'Y$ and since $\gcd(X,Y) = 1$, we get $X' = X$ and the lemma follows. □

Next, we deal with the situation when an exponent e is defined by different tuples (u,X) and (u',X') with $u \neq u'$ and $v = v'$.

Lemma 10. *Let $N = pq$ be an RSA modulus with $q < p < 2p$. Let u, u' be integers with $|u|, |u'| < N^{\frac{1}{4}}$. Let X, X' be integers with $1 \leq X, X' < 2^{-\frac{1}{4}}N^{\frac{1}{4}}$, $\gcd(X, \psi(u,v)) = 1$, $\gcd(X', \psi(u',v')) = 1$ where $v = \left\lfloor -\frac{qu}{p-u} \right\rfloor$ and $v' = \left\lfloor -\frac{qu'}{p-u'} \right\rfloor$. Define*

$$e \equiv X^{-1} \pmod{\psi(u,v)} \quad \textit{and} \quad e' \equiv X'^{-1} \pmod{\psi(u',v')}.$$

If $v = v'$ and $e = e'$, then $X = X'$ and $u = u'$.

Proof. As in the proof of Lemma 9, rewrite e and e' as

$$e = \frac{1+\psi(u,v)Y}{X} \quad \text{and} \quad e' = \frac{1+\psi(u',v')Y'}{X'}.$$

Suppose $e = e'$. Then

$$|\psi(u',v')XY' - \psi(u,v)X'Y| = |X'-X|. \tag{10}$$

Assuming $v = v'$ and using $\psi(u,v) = (p-u)(q-v)$, $\psi(u',v') = (p-u')(q-v)$ in (10), we get

$$(q-v)\,|(p-u')XY' - (p-u)X'Y| = |X'-X|.$$

By Lemma 2, we have $q - v > 2^{-\frac{1}{2}}N^{\frac{1}{2}} - N^{\frac{1}{4}} > N^{\frac{1}{4}}$ and since $|X'-X| < 2^{-\frac{1}{4}}N^{\frac{1}{4}}$, we get

$$\begin{cases} X' - X = 0, \\ (p-u')XY' - (p-u)X'Y = 0. \end{cases}$$

Hence $X = X'$ and $(p-u')Y' = (p-u)Y$. Suppose for contradiction that $u' \neq u$. Put $g = \gcd(p-u', p-u)$. Then g divides $(p-u) - (p-u') = u' - u$. Since $v = v'$, by Lemma 6 we have $|u'-u| \leq 1$, so $g = 1$. Hence $\gcd(p-u', p-u) = 1$ and $p-u$ divides Y'. Since $p - u > N^{\frac{1}{2}}$ and $Y' < X' < 2^{-\frac{1}{4}}N^{\frac{1}{4}}$, this leads to a contradiction, so we deduce that $u' = u$. This terminates the proof. □

Using the methods used to prove Lemma 9 and Lemma 10 plus some additional arguments, we shall prove the following stronger result.

Theorem 5. *Let $N = pq$ be an RSA modulus with $q < p < 2p$. Let u, u' be integers with $|u|, |u'| < N^{\frac{1}{4}}$. Let X, X' be integers with $1 \leq X, X' < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$, $\gcd(X, \psi(u,v)) = 1$, $\gcd(X', \psi(u',v')) = 1$ where $v = \left\lfloor -\frac{qu}{p-u} \right\rceil$ and $v' = \left\lfloor -\frac{qu'}{p-u'} \right\rceil$. Define*

$$e \equiv X^{-1} \pmod{\psi(u,v)} \quad \text{and} \quad e' \equiv X'^{-1} \pmod{\psi(u',v')}.$$

If $e = e'$, then $u = u'$, $v = v'$ and $X = X'$.

Proof. Assume that $e = e'$. Then, as in the proof of Lemma 10, e and e' satisfy (10). We first take care of some easy cases.

If $u = u'$, then $v = v'$ and by Lemma 9, we get $X = X'$.

If $v = v'$, then by Lemma 10, we get $u = u'$ and $X = X'$.

Without loss of generality, suppose that $\psi(u,v) < \psi(u',v')$. Transforming (10), we get

$$\left| \frac{XY'}{X'Y} - \frac{\psi(u,v)}{\psi(u',v')} \right| = \frac{|X' - X|}{X'Y\psi(u',v')} \leq \frac{\max(X', X)}{X'Y\psi(u',v')} < \frac{1}{2(X'Y)^2},$$

where the final step is trivial since, for $N \geq 2^{10}$

$$2\max(X', X)X'Y < 2 \times \left(2^{-\frac{1}{4}} N^{\frac{1}{4}}\right)^3 < N - 2^{-\frac{1}{2}} N^{\frac{1}{2}} < \psi(u',v').$$

Combined with Theorem 1, this implies that $\frac{XY'}{X'Y}$ is one of the convergents of the continued fraction expansion of $\frac{\psi(u,v)}{\psi(u',v')}$. By Lemma 8, the first non trivial convergents are $\frac{1}{1}$ and $\frac{a_2}{a_2+1}$ where $a_2 > 2^{-\frac{1}{2}} N^{\frac{1}{2}} - \frac{1}{2}$. Observe that

$$a_2 + 1 > 2^{-\frac{1}{2}} N^{\frac{1}{2}} - \frac{1}{2} + 1 = 2^{-\frac{1}{2}} N^{\frac{1}{2}} + \frac{1}{2} > 2^{-\frac{1}{2}} N^{\frac{1}{2}} = \left(2^{-\frac{1}{4}} N^{\frac{1}{4}}\right)^2 > X'Y.$$

This implies that the only possibility for $\frac{XY'}{X'Y}$ to be a convergent of $\frac{\psi(u,v)}{\psi(u',v')}$ is $\frac{1}{1}$. This gives $XY' = X'Y$. Since $\gcd(X, Y) = \gcd(X', Y') = 1$ then $X = X'$ and $Y = Y'$. Replacing in (10), we get $\psi(u',v') = \psi(u,v)$ and by Lemma 7, we deduce $u = u'$. This completes the proof. □

We now determine the order of the cardinality of the set $H(N)$. Recall that the elements of $H(N)$ are uniquely defined by the congruence

$$e \equiv X^{-1} \pmod{\psi(u,v)},$$

where $|u| < N^{\frac{1}{4}}$, $v = \left\lfloor -\frac{qu}{p-u} \right\rceil$, $1 \leq X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$ and $\gcd(X, \psi(u,v)) = 1$. In addition, $p - u$ is B_{ecm}-smooth.

Theorem 6. *Let $N = pq$ be an RSA modulus with $q < p < 2p$. We have*

$$\#H(N) \geq N^{\frac{1}{2}-\varepsilon},$$

where ε is a small positive constant.

Proof. Assume $B_{\text{ecm}} < p - p^{\frac{1}{2}}$. Let us consider the set $V(p)$ as defined by (9). Put $x = p - p^{\frac{1}{2}}$, $z = 2p^{\frac{1}{2}}$ and $y = B_{\text{ecm}}$. Define $\delta > 0$ and $\gamma > 0$ such that

$$x^{\frac{1}{2}+\delta} \leq z, \qquad y = x^{1/\gamma}.$$

Then $x \geq z \geq x^{\frac{1}{2}+\delta}$, $x \geq y \geq x^{1/\gamma}$ and the conditions to apply (3) are fulfilled. On the other hand, we have $y > \exp\left\{(\log\log x)^{5/3+\varepsilon}\right\}$ for $x < \exp\left\{10^{7-\varepsilon}\right\}$ and the condition to apply (2) is fulfilled. Combining (3) and (2), we get

$$\#V(p) = \Psi(x+z,y) - \Psi(x,y) \geq c\frac{z}{x}\Psi(x,y) = cz\rho(\gamma)\left\{1 + O\left(\frac{\log(\gamma+1)}{\log(y)}\right)\right\},$$

where $c = c(\delta,\gamma) > 0$ and $\rho(\gamma)$ is the Dickman-de Bruijn ρ-function (see Table 2). Hence

$$\#V(p) \geq c\rho(\gamma)\, z = 2c\rho(\gamma)\, p^{\frac{1}{2}}.$$

Since trivially $\#V(p) < z = 2p^{\frac{1}{2}}$, we get $\#V(p) \asymp p^{\frac{1}{2}}$. Combining this with Table 2, we conclude that $\#V(p)$ is lower bounded as follows

$$\#V(p) \geq p^{\frac{1}{2}-\varepsilon'} = N^{\frac{1}{4}-\varepsilon_1},$$

with small constants $\varepsilon' > 0$ and $\varepsilon_1 > 0$.

Next, for every integer u with $|u| < N^{\frac{1}{4}}$ put

$$W(u) = \left\{X :\ 1 \leq X < 2^{-\frac{1}{4}}N^{\frac{1}{4}},\ (X, \psi(u,v)) = 1\right\},$$

where $v = \left\lfloor -\frac{qu}{p-u} \right\rfloor$. Setting $m = \left\lfloor 2^{-\frac{1}{4}}N^{\frac{1}{4}} \right\rfloor$, we have

$$\#W(u) = \sum_{\substack{X=1 \\ (X,\psi(u,v))=1}}^{m} 1 = \sum_{d|\psi(u,v)} \mu(d)\left\lfloor \frac{m}{d} \right\rfloor \geq m \sum_{d|\psi(u,v)} \frac{\mu(d)}{d} = \frac{m\phi(\psi(u,v))}{\psi(u,v)}$$

where $\mu(.)$ is the Möbius function and $\phi(.)$ is the Euler totient function. We shall need the well known result (see Theorem 328 of [11]),

$$\frac{\phi(n)}{n} \geq \frac{C}{\log\log n},$$

where C is a positive constant. Applying this with $n = \psi(u,v)$ and using Lemma 4, we get

$$\#W(u) \geq \frac{Cm}{\log\log\psi(u,v)} \geq \frac{2^{-\frac{1}{4}}CN^{\frac{1}{4}}}{\log\log\left(N + 2^{-\frac{1}{2}}N^{\frac{1}{2}}\right)} = N^{\frac{1}{4}-\varepsilon_2},$$

with a small constant $\varepsilon_2 > 0$.

It remains to show that $\#H(n) \geq N^{\frac{1}{4}-\varepsilon}$ where ε is a positive constant. Indeed, for every $u \in V(p)$ there are at least $N^{\frac{1}{4}-\varepsilon_2}$ integers $X \in W(u)$. Hence

$$\#H(n) \geq \#V(p)\#W(u) \geq N^{\frac{1}{2}-\varepsilon_1-\varepsilon_2}.$$

Setting $\varepsilon = \varepsilon_1 + \varepsilon_2$, this completes the proof of the theorem. □

Table 2. Table of values of $\rho(\gamma)$ with $\left(p-\sqrt{p}\right)^{\frac{1}{\gamma}} = B_{\text{ecm}} = 10^{50}$

Number of bits of p	256	512	1024	2048
$\gamma = \dfrac{\log\left(p-\sqrt{p}\right)}{\log B_{\text{ecm}}} \approx$	1.5	3	6.25	12.50
$\rho(\gamma) \approx$(see[9])	5.945×10^{-1}	4.861×10^{-2}	9.199×10^{-6}	1.993×10^{-15}

7 Conclusion

Wiener's famous attack on RSA with $d < \frac{1}{3}N^{0.25}$ shows that using the equation $ed - k(p-1)(q-1) = 1$ and a small d makes RSA insecure. In this paper, we performed a generalization of this attack. We showed that we can find any X and Y with $1 \leq Y < X < 2^{-0.25}N^{0.25}$ from the continued fraction expansion of e/N when they satisfy an equation

$$eX - Y(p-u)\left(q + \left[\frac{qu}{p-u}\right]\right) = 1,$$

and if $p-u$ or $q + [qu/(p-u)]$ is smooth enough to factor, then p and q can be found from X and Y. Our results illustrate that one should be very cautious when choosing some class of RSA exponent. Note that our attack, as well as all the attacks based on continued fractions do not apply to RSA with modulus N and small public exponents as the popular values $e = 3$ or $e = 2^{16}+1$ because the non-trivial convergents of $\frac{e}{N}$ are large enough to use diophantine approximation techniques, namely Theorem 1.

References

1. Baker, A.: Linear forms in the logarithms of algebraic numbers IV. Mathematika 15, 204–216, 1966.
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., 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.
4. Brent, R.P.: Some integer factorization algorithms using elliptic curves, Australian Computer Science Communications, vol. 8, 149-163, 1986.
5. Brent, R.P.: Recent progress and prospects for integer factorisation algorithms, Springer-Verlag LNCS 1858, 3–22, 2000.
6. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), 233-260, 1997.
7. Ferguson, H.R.P., Bailey, D.H.: A polynomial time, numerically stable integer relation algorithm. RNR Technical Report RNR-91-032, NASA Ames Research Center, Moffett Field, CA. (December 1991)
8. Friedlander, J., Granville, A.: Smoothing "Smooth" Numbers, Philos. Trans. Roy. Soc. London Ser. A 345, 339–347, 1993.
9. Granville, A.: Smooth numbers: computational number theory and beyond, Proc. MSRI Conf. Algorithmic Number Theory: Lattices, Number Fields, Curves, and Cryptography, Berkeley, 2000, J. Buhler and P. Stevenhagen, eds., Cambridge University Press.
10. Hall, R.R., Tenenbaum, G.: Divisors. Cambridge Tracts in Mathematics, 90, Cambridge University Press, 1988.
11. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, London, 1965.
12. Hildebrand, A.: On the number of positive integers $\leq x$ and free of prime factors $> y$, J. Number Theory 22, 289–307, 1986.
13. Howgrave-Graham, N.A.: Finding small roots of univariate modular equations revisited. In Cryptography and Coding, LNCS 1355, pp. 131-142, Springer-Verlag, 1997.
14. Lenstra, H.W.: Factoring integers with elliptic curves, Annals of Mathematics, vol. 126, 649-673, 1987.
15. Lenstra, A.K., Lenstra, H.W., Lovasz, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, 513-534, 1982.
16. Lenstra, A.K., Lenstra, H.W., Manasse, M.S., Pollard, J.M.: The number field sieve, Proc. 22nd Annual ACM Conference on Theory of Computing, pp. 564–572, Baltimore, Maryland, 1990.
17. 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`
18. Montgomery, P.L.: Speeding the Pollard and elliptic curve methods of factorization, Mathematics of Computation, vol. 48, 243-264, 1987.
19. PARI/GP, version `2.1.7`, Bordeaux, 2007, `http://pari.math.u-bordeaux.fr/`
20. 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.
21. de Weger, B.: Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering, Communication and Computing,Vol. 13(1), 17-28, 2002.
22. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553-558, 1990.
23. Zimmerman, P.: The ECMNET Project,
`http://www.loria.fr/~zimmerma/records/ecmnet.html`