Cryptanalysis of RSA Using the Ratio of the Primes

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 an RSA modulus, i.e. the product of two large unknown primes of equal bit-size. In the $X9.31$-1997 standard for public key cryptography, Section 4.1.2, there are a number of recommendations for the generation of the primes of an RSA modulus. Among them, the ratio of the primes shall not be close to the ratio of small integers. In this paper, we show that if the public exponent e satisfies an equation $eX - (N - (ap + bq))Y = Z$ with suitably small integers X, Y, Z, where $\frac{a}{b}$ is an unknown convergent of the continued fraction expansion of $\frac{q}{p}$, then N can be factored efficiently. In addition, we show that the number of such exponents is at least $N^{\frac{3}{4}-\varepsilon}$ where ε is arbitrarily small for large N.

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

1 Introduction

The RSA public-key cryptosystem [15] was invented by Rivest, Shamir, and Adleman in 1978. Since then, the RSA system has been the most widely accepted public key cryptosystem. In the RSA cryptosystem, the modulus $N = pq$ is a product of two primes of equal bit-size. Let e be an integer coprime with $\phi(N) = (p-1)(q-1)$, the Euler function of N. Let d be the integer solution of the equation $ed \equiv 1 \pmod{\phi(N)}$ with $d < \phi(N)$. We call e the public exponent and d the private exponent. The pair (N, e) is called the public key and the pair (N, d) is the corresponding private key.

RSA is computationally expensive as it requires exponentiations modulo the large RSA modulus N. For efficient modular exponentiation in the decryption/signing phase, one may be tempted to choose a small d. Unfortunately, Wiener [17] showed in 1990 that using continued fractions, one can efficiently recover the secret exponent d from the public key (N, e) as long as $d < \frac{1}{3}N^{\frac{1}{4}}$. Wiener's attack is based on solving the equation $ex - \phi(N)y = 1$ where $x < \frac{1}{3}N^{\frac{1}{4}}$. Since then, attacking RSA using information encoded in the public key (N, e) has been a stimulating area of research.

Based on the lattice basis reduction, Boneh and Durfee [2] proposed in 1999 a new attack on the use of short secret exponent d, namely, they improved the bound to $d < N^{0.292}$.

In 2004, Blömer and May [1] showed that N can be factored in polynomial time for every public key (N, e) satisfying an equation $ex-(N+1-(p+q))k = y$, with $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| < N^{-\frac{3}{4}}ex$.

Another attack using information encoded in (N, e) was recently proposed by Nitaj in [13]. The idea of [13] is based on solving the equation satisfied by the public exponent e. Suppose e satisfies an equation $eX - (p-u)(q-v)Y = 1$ with $1 \leq Y \leq X < 2^{-\frac{1}{4}}N^{\frac{1}{4}}$, $|u| < N^{\frac{1}{4}}$ and $v = \left\lfloor -\frac{qu}{p-u} \right\rfloor$. If the prime factors of $p-u$ or $q-v$ are less than 10^{50}, then N can be factored efficiently.

In this paper, we propose new attacks on RSA. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$. Define α such that $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$. We focus on the class of the public exponents satisfying an equation

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

with small parameters X, Y, Z satisfying

$$1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}, \ \gcd(X, Y) = 1,$$

and Z depends on the size of $|ap - bq|$. We present three attacks according to the size of the difference $|ap - bq|$. The first attack concerns small difference, i.e. $|ap - bq| < (abN)^{\frac{1}{4}}$, the second attack will work for medium difference, i.e. $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$, and the third attack concerns large difference, i.e. $|ap - bq| > aN^{\frac{1}{4}}$. The first attack always lead to the factorization of N. The second and the third attacks work if, in addition, $b \leq 10^{52}$. This corresponds to the current limit of the Elliptic Curve Method [8] to find large factors of integers.

The attacks combine techniques from the theory of continued fractions, Coppersmith's method [5] for finding small roots of bivariate polynomial equations and the Elliptic Curve Method [8] for Integer Factorization. We also show that the set of exponents e for which our approach works is at least $N^{\frac{3}{4}-\varepsilon}$ where ε is a small positive constant depending only on N.

Our approach is more efficient if $\frac{q}{p}$ is close to $\frac{a}{b}$ with small integers a and b. This is a step in the direction of the recommendations of the $X9.31$-1997 standard for public key cryptography (Section 4.1.2) which requires that the ratio of the primes shall not be close to the ratio of small integers. It is important to notice that, since $q < p < 2q$, then $\frac{0}{1}$ and $\frac{1}{1}$ are among the convergents of the continued fraction expansion of $\frac{q}{p}$ (see Section 2). For $a = 0$, $b = 1$, the equation $eX - (N - (ap + bq))Y = Z$ becomes

$$eX - q(p-1)Y = Z.$$

and was studied by Nitaj [12] with suitably small parameters X, Y, Z. Consequently, in this paper, we focus on the convergents $\frac{a}{b}$ with $a \geq 1$. For $a = b = 1$, our third attack applies and matches the attack of Blömer and May [1].

The rest of the paper is organized as follows. In Section 2 we give a brief introduction to continued fractions, Coppersmith's lattice-based method for finding small roots of polynomials [5] and the Elliptic Curve Method of Factorization. In Section 3 we study the properties of the convergents of the continued fraction expansion of the ratio of the primes of $N = pq$. In Section 4 we present the new attacks. In Section 5, we give an estimate for the size of the set of the public exponents for which our attacks work. Section 6 concludes the paper.

2 Preliminaries on Continued Fractions, Coppersmith's Method and The Elliptic Curve Method (ECM)

We first introduce some notation. The integer closest to x is denoted $[x]$ and the largest integer less than or equal to x is denoted $\lfloor x \rfloor$.

2.1 Continued Fractions and the Euclidean Algorithm

We briefly recall some basic definitions and facts that we use about continued fractions and the Euclidean algorithm, which can be found in [6].

The process of finding the continued fraction expansion of a rational number $\frac{q}{p}$ involves the same series of long divisions that are used in the application of the Euclidean algorithm to the pair of integers (q, p). Starting with $r_{-2} = q$ and $r_{-1} = p$, define the recursions

$$a_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor, \quad r_i = r_{i-2} - a_i r_{i-1}, \ i \geq 0, \tag{1}$$

where a_i is the integer quotient $\lfloor r_{i-2}/r_{i-1} \rfloor$ and r_i is the integer remainder that satisfies $0 \leq r_i < r_{i-1}$. The Euclidean algorithm terminates with a series of remainders satisfying

$$0 = r_m < r_{m-1} < \cdots < r_2 < r_1 < r_0 < r_{-1} = p.$$

The continued fraction expansion of $\frac{q}{p}$ is then

$$\frac{q}{p} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_m}}}},$$

or alternatively, $\frac{q}{p} = [a_0, a_1, \cdots, a_m]$. The rational number $[a_0, a_1, \cdots, a_i]$ with $0 \leq i \leq m$ is called the i-th convergent of $\frac{q}{p}$ and satisfies

$$[a_0, a_1, \cdots, a_i] = \frac{p_i}{q_i},$$

where the integers p_i and q_i are coprime positive integers. Note that the integers p_i and q_i are also defined by the double recursions

$$p_{-2} = 0, \quad p_{-1} = 1, \quad p_i = a_i p_{i-1} + p_{i-2}, \ i \geq 0, \tag{2}$$
$$q_{-2} = 1, \quad q_{-1} = 0, \quad q_i = a_i q_{i-1} + q_{i-2}, \ i \geq 0. \tag{3}$$

Since $q < p < 2q$, we have $\frac{q}{p} < 1$ and taking $i = 0$ in (1), (2) and (3), we get

$$a_0 = \left\lfloor \frac{r_{-2}}{r_{-1}} \right\rfloor = \left\lfloor \frac{q}{p} \right\rfloor = 0, \quad r_0 = q, \quad p_0 = 0, \quad q_0 = 1.$$

Similarly, we have $1 < \frac{p}{q} < 2$ and taking $i = 1$ in (1), (2) and (3), we get

$$a_1 = \left\lfloor \frac{r_{-1}}{r_0} \right\rfloor = \left\lfloor \frac{p}{q} \right\rfloor = 1, \quad p_1 = 1, \quad q_1 = 1.$$

From this we deduce that the first convergents of the continued fraction expansion of $\frac{q}{p}$ are $\frac{0}{1}$ and $\frac{1}{1}$.

Proposition 1. *Let $\frac{q}{p} = [a_0, a_1, \cdots, a_m]$ be a continued fraction. For $0 \leq i < m$, we have*

$$\left| \frac{q}{p} - \frac{p_i}{q_i} \right| < \frac{1}{q_i^2}.$$

We terminate with a famous result on good rational approximations.

Theorem 1. *Let $\frac{q}{p} = [a_0, a_1, \cdots, a_m]$. If a and b are coprime positive integers such that $b < p$ and*

$$\left| \frac{q}{p} - \frac{a}{b} \right| < \frac{1}{2b^2},$$

then $a = p_i$ and $b = q_i$ for some i with $0 \leq i \leq m$.

2.2 Coppersmith's Method

At Eurocrypt'96, Coppersmith [5] introduced two lattice reduction based techniques to find small roots of polynomial diophantine equations. The first technique works for modular univariate polynomials, the second for bivariate integer polynomial equations. Since then, Coppersmith's techniques have been used in a huge variety of cryptanalytic applications. Coppersmith illustrated his technique for solving bivariate integer polynomial equations with the problem of finding the factors of $n = xy$ if we are given the high order $\frac{1}{4} \log_2 n$ bits of y.

Theorem 2. *Let $n = xy$ be the product of two unknown integers such that $x < y < 2x$. Given an approximation of y with additive error at most $n^{\frac{1}{4}}$, then x and y can be found in polynomial time.*

2.3 The Elliptic Curve Method of Factorization

The difficulty of factoring a large number is an element of the security of the RSA system. In the recent years, the limits of the best factorization algorithms have been extended greatly. There are two classes of algorithms for finding a nontrivial factor p of a composite integer n. The algorithms in which the run time depends on the size of n: Lehmans algorithm [7], the Continued Fraction algorithm [11], the Multiple Polynomial Quadratic Sieve algorithm [16], the Number Field Sieve [9]. And the algorithms in which the run time depends on the size of p: Trial Division, Pollard's "rho" algorithm [14], Lenstra's Elliptic Curve Method [8].

The Elliptic Curve Method (ECM for short) was originally proposed by H.W. Lenstra [8] and subsequently extended by Brent [3], [4], and Montgomery [10]. The original part of the algorithm proposed by Lenstra is typically referred to as Phase 1, and the extension by Brent and Montgomery is called Phase 2. ECM is suited to find small factors p of large numbers n and has complexity

$$\mathcal{O}\left(\exp\left\{c\sqrt{\log p \log\log p}\right\} M(n)\right),$$

where $c > 0$ and $M(n)$ denotes the cost of multiplication $\pmod n$. R. Brent [4] extrapolated that the Elliptic Curve Method record will be a D-digit factor in year $Y(D) = 9.3\sqrt{D} + 1932.3$. According to this formula, $Y(50) \approx 1998$ and $Y(67) \approx 2008$. A table of the largest factors found using the ECM is maintained by Zimmermann [18]. The largest prime factor found using the ECM had 67 decimal digits and was found by B. Dodson on August 24, 2006.

3 Useful Lemmas and Properties

First we recall a very useful lemma (see [13]).

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

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

The following lemma shows that a and b are of the same bit-size.

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. If $\frac{a}{b}$ is a convergent of $\frac{q}{p}$ with $a \geq 1$, then $a \leq b \leq 2a$.*

Proof. If $b = 1$, then $a = 1$ and the inequalities $a \leq b \leq 2a$ are satisfied. Next, suppose $b \geq 2$. Observe that if $\frac{a}{b}$ is a convergent of $\frac{q}{p}$ then by Proposition 1 we have $|ap - bq| \leq \frac{p}{b} \leq \frac{p}{2}$. Isolating bq and dividing by q, we get

$$a\frac{p}{q} - \frac{p}{2q} \leq b \leq a\frac{p}{q} + \frac{p}{2q}.$$

Combining this with $1 < \frac{p}{q} < 2$, we get

$$a - \frac{p}{2q} < a\frac{p}{q} - \frac{p}{2q} \leq b \leq a\frac{p}{q} + \frac{p}{2q} < 2a + \frac{p}{2q}.$$

Since $p < 2q$, then $0 < \frac{p}{2q} < 1$. Hence $a \leq b \leq 2a$ which completes the proof. □

The following lemma plays an important role in this paper. Recall that the integer closest to x is denoted $[x]$.

Lemma 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and $\frac{a}{b}$ a convergent of the continued fraction expansion of $\frac{q}{p}$ with $a \geq 1$. Let $ap + bq = N^{\frac{1}{2}+\alpha}$ with $\alpha < \frac{1}{2}$. If $|ap + bq - M| < \frac{1}{2}N^{\frac{1}{2}-\alpha}$, then*

$$ab = \left[\frac{M^2}{4N}\right].$$

Proof. Set $M = ap + bq + x$. Using $(ap - bq)^2 = (ap + bq)^2 - 4abN$, we get, after rearrangement,

$$M^2 - 4abN = (ap + bq + x)^2 - 4abN = (ap - bq)^2 + 2(ap + bq)x + x^2. \quad (4)$$

Consider the term $(ap - bq)^2$ on the right side of (4). If $b = 1$, then by Lemma 2, $a = 1$. Hence, since $q < p < 2q$, we have $|ap - bq| = |p - q| = p - q < \frac{p}{2}$. If $b \geq 2$, then by Proposition 1, we have $|ap - bq| < \frac{p}{b} \leq \frac{p}{2}$. Combining with Lemma 1, we get in both cases

$$(ap - bq)^2 < \left(\frac{p}{2}\right)^2 < \left(\frac{2^{\frac{1}{2}}N^{\frac{1}{2}}}{2}\right)^2 = \frac{N}{2}.$$

Hence, using $|x| < \frac{1}{2}N^{\frac{1}{2}-\alpha}$, the right side of (4) becomes

$$\begin{aligned}\left|(ap - bq)^2 + 2(ap + bq)x + x^2\right| &\leq (ap - bq)^2 + 2(ap + bq)|x| + x^2 \\ &< \frac{N}{2} + 2N^{\frac{1}{2}+\alpha} \cdot \frac{1}{2}N^{\frac{1}{2}-\alpha} + \frac{1}{4}N^{1-2\alpha} \\ &= \left(\frac{1}{2} + 1 + \frac{1}{4}N^{-2\alpha}\right)N \\ &< 2N,\end{aligned}$$

where we used $\alpha > 0$. Plugging this in (4) and dividing by $4N$, we get

$$\left|\frac{M^2}{4N} - ab\right| = \frac{\left|M^2 - 4abN\right|}{4N} = \frac{\left|(ap - bq)^2 + 2(ap + bq)x + x^2\right|}{4N} < \frac{2N}{4N} = \frac{1}{2}.$$

It follows that $ab = \left[\frac{M^2}{4N}\right]$ which terminates the proof. □

The following lemma indicates that ap and bq are of the same bit-size.

Lemma 4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and $\frac{a}{b}$ a convergent of the continued fraction expansion of $\frac{q}{p}$ with $a \geq 1$. Then*

$$ap < bq < 2ap \quad or \quad bq < ap < 2bq$$

Proof. First, assume $ap < bq$. By Lemma 2, we have $b \leq 2a$. Combining this with $q < p$, we get $bq < 2ap$, and consequently $ap < bq < 2ap$.

Next, assume $bq < ap$. By Lemma 2, we have $a \leq b$. Combining this with $p < 2q$, we get $ap < 2bq$ and finally $bq < ap < 2bq$. This terminates the proof. □

4 The New Attacks on RSA

In this section, we show how to factor the RSA modulus N if (N, e) is a public key satisfying an equation $eX-(N-(ap+bq))Y = Z$ with small parameters X, Y and Z where $\frac{a}{b}$ is an unknown convergent of $\frac{q}{p}$ with $a \geq 1$. We shall consider separately the cases when the difference $|ap-bq|$ is small, i.e. $|ap-bq| < (abN)^{\frac{1}{4}}$, medium, i.e. $(abN)^{\frac{1}{4}} < |ap-bq| < aN^{\frac{1}{4}}$, and large, i.e. $|ap-bq| > aN^{\frac{1}{4}}$. This corresponds approximately to $b > 2^{\frac{1}{2}}N^{\frac{1}{6}}$, $2^{\frac{1}{2}}N^{\frac{1}{6}} > b > 2^{\frac{1}{4}}N^{\frac{1}{8}}$ and $b < 2^{\frac{1}{4}}N^{\frac{1}{8}}$ respectively.

First we present a result based on continued fractions.

Lemma 5. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let a, b be coprime positive integers such that $ap+bq = N^{\frac{1}{2}+\alpha}$ with $\alpha < \frac{1}{2}$. Let e be a public exponent satisfying the equation $eX-(N-(ap+bq))Y = Z$ with $\gcd(X, Y) = 1$. If $|Z| < N^{\frac{1}{2}+\alpha}X$ and $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$, then $\frac{Y}{X}$ is a convergent of $\frac{e}{N}$.*

Proof. Set $ap + bq = N^{\frac{1}{2}+\alpha}$ with $\alpha < \frac{1}{2}$. Rewrite $eX - (N - ap - bq)Y = Z$ as $eX - NY = Z - (ap + bq)Y$. Now suppose $|Z| < N^{\frac{1}{2}+\alpha}X$, $1 \leq Y \leq X$ and $\gcd(X, Y) = 1$. Then

$$\begin{aligned}\left|\frac{e}{N} - \frac{Y}{X}\right| &= \frac{|eX - NY|}{NX} \\ &= \frac{|Z - (ap + bq)Y|}{NX} \\ &\leq \frac{|Z|}{NX} + \frac{(ap + bq)Y}{NX} \\ &< \frac{N^{\frac{1}{2}+\alpha}}{N} + \frac{N^{\frac{1}{2}+\alpha}}{N} \\ &= 2N^{-\frac{1}{2}+\alpha}.\end{aligned}$$

Since $X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$, then $2N^{-\frac{1}{2}+\alpha} < \frac{1}{2X^2}$. Hence, by Theorem 1, $\frac{Y}{X}$ is one of the convergents of the continued fraction expansion of $\frac{e}{N}$. □

4.1 An Attack for Small Difference $|ap - bq|$

We now present the first attack.

Theorem 3. *Let $N = pq$ be an RSA modulus with unknown factors p, q such that $q < p < 2q$. Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ with $a \geq 1$ and $|ap - bq| < (abN)^{\frac{1}{4}}$. Let e be a public exponent satisfying an equation $eX - (N - ap - bq)Y = Z$ with $\gcd(X, Y) = 1$. Set $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$. If $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ and $|Z| < \inf\left((abN)^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right)Y$, then N can be factored in polynomial time.*

Proof. Assume $|Z| < \inf\left((abN)^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right) Y$, $1 \leq Y \leq X$ with $\gcd(X, Y) = 1$. Then

$$|Z| < \inf\left((abN)^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right) X \leq \frac{1}{2}N^{\frac{1}{2}-\alpha}X < N^{\frac{1}{2}+\alpha}X.$$

Hence by Lemma 5, $\frac{Y}{X}$ is one of the convergents of $\frac{e}{N}$. Set $M = N - \frac{eX}{Y}$. Starting with the equation $eX - (N - (ap + bq))Y = Z$, we get

$$|ap + bq - M| = \frac{|Z|}{Y} < \inf\left((abN)^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right) < \frac{1}{2}N^{\frac{1}{2}-\alpha}.$$

Hence, by Lemma 3, we find $ab = \left\lfloor \frac{M^2}{4N} \right\rfloor$. On the other hand, we have

$$|ap + bq - M| < \inf\left((abN)^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right) < (abN)^{\frac{1}{4}}.$$

Moreover, if $|ap - bq| < (abN)^{\frac{1}{4}}$, then

$$\left|ap - \frac{M}{2}\right| \leq \frac{1}{2}|ap + bq - M| + \frac{1}{2}|ap - bq| < \frac{1}{2}(abN)^{\frac{1}{4}} + \frac{1}{2}(abN)^{\frac{1}{4}} = (abN)^{\frac{1}{4}}.$$

It follows that the term $\frac{M}{2}$ is an approximation of the factor ap of $n = abN$ with additive error at most $n^{\frac{1}{4}}$. In addition, by Lemma 4, the factors ap and bq of n are of the same bit-size. Hence, using Theorem 2 with n and $\frac{M}{2}$, we find ap, and since $a < q$, we get $p = \gcd(N, ap)$ which terminates the proof. □

Let us summarize the first factorization algorithm.

Algorithm 1 Small $|ap - bq|$

Input: a public key (N, e) satisfying $N = pq$, $q < p < 2q$ and $eX-(N-(ap+bq))Y = Z$ for small parameters X, Y, Z where $\frac{a}{b}$ is an unknown convergent of $\frac{q}{p}$ with $a \geq 1$.
Output: the prime factors p and q.

1: Compute the continued fraction expansion of $\frac{e}{N}$.
2: For every convergent $\frac{Y}{X}$ of $\frac{e}{N}$ with $X < \frac{1}{2}N^{\frac{1}{4}}$:
3: Compute $M = N - \frac{eX}{Y}$ and $N_0 = \left\lfloor \frac{M^2}{4N} \right\rfloor$.
4: Apply Coppersmith's algorithm (Theorem 2) with $n = N_0N$ and $\frac{M}{2}$ as an approximation of y.
5: Compute $g = \gcd(y, N)$. If $1 < g < N$, then stop.

4.2 An Attack for Medium Difference $|ap - bq|$

Here we present the second attack. It is based on the Elliptic Curve Method (ECM) which can find factors of about 52-digits. Assuming the efficiency of ECM, every step in this attack can be done in polynomial time and the number of convergents is bounded by $\mathcal{O}(\log N)$. To express this fact, the term *efficient* is used.

Theorem 4. *Let $N = pq$ be an RSA modulus with unknown factors p, q such that $q < p < 2q$. Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ such that $a \geq 1$, $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$ and $b \leq 10^{52}$. Let e be a public exponent satisfying an equation $eX - (N - ap - bq)Y = Z$ with $\gcd(X, Y) = 1$. Set $M = N - \frac{eX}{Y}$ and $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$. If $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ and $|Z| < \min\left(aN^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right)Y$, then, under ECM, N can be factored efficiently.*

Proof. Assume $|Z| < \min\left(aN^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right)Y$, $1 \leq Y \leq X$ and $\gcd(X, Y) = 1$. Then

$$|Z| < \min\left(aN^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right)X \leq \frac{1}{2}N^{\frac{1}{2}-\alpha}X < N^{\frac{1}{2}+\alpha}X.$$

It follows, by Lemma 5, that $\frac{Y}{X}$ is among the convergents of $\frac{e}{N}$.
Next, set $M = N - \frac{eX}{Y}$. Using the equation $eX - (N - (ap + bq))Y = Z$, we get

$$|ap + bq - M| = \frac{|Z|}{Y} < \min\left(aN^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right) \leq \frac{1}{2}N^{\frac{1}{2}-\alpha}.$$

Hence, by Lemma 3, we find $ab = \left\lfloor \frac{M^2}{4N} \right\rfloor$ and by Lemma 2, we know that a and b are of equal bit-size. Hence, applying the Elliptic Curve Method with $\left\lfloor \frac{M^2}{4N} \right\rfloor$, we can efficiently find a and b assuming $b \leq 10^{52}$.
From $|ap + bq - M| < aN^{\frac{1}{4}}$, we get

$$\left| p + \frac{bq}{a} - \frac{M}{a} \right| < \frac{aN^{\frac{1}{4}}}{a} = N^{\frac{1}{4}}. \tag{5}$$

On the other hand, by assumption, $|ap - bq| < aN^{\frac{1}{4}}$. Then $\left|p - \frac{bq}{a}\right| < N^{\frac{1}{4}}$, and combining with (5), we get

$$\begin{aligned}
\left| p - \frac{M}{2a} \right| &= \left| \frac{1}{2}\left(p + \frac{bq}{a} - \frac{M}{a} \right) + \frac{1}{2}\left(p - \frac{bq}{a} \right) \right| \\
&\leq \frac{1}{2}\left| p + \frac{bq}{a} - \frac{M}{a} \right| + \frac{1}{2}\left| p - \frac{bq}{a} \right| \\
&< \frac{1}{2}N^{\frac{1}{4}} + \frac{1}{2}N^{\frac{1}{4}} \\
&= N^{\frac{1}{4}}.
\end{aligned}$$

This implies that $\frac{M}{2a}$ is an approximation of p with additive error at most $N^{\frac{1}{4}}$. Then, using Theorem 2, this gives p which terminates the proof. □

Here we summarize the second factorization algorithm.

Algorithm 2 Medium $|ap - bq|$

Input: a public key (N, e) satisfying $N = pq$, $q < p < 2q$ and $eX-(N-(ap+bq))Y = Z$ for small parameters X, Y, Z where $\frac{a}{b}$ is an unknown convergent of $\frac{q}{p}$ with $a \geq 1$.
Output: the prime factors p and q.
1: Compute the continued fraction expansion of $\frac{e}{N}$.
2: For every convergent $\frac{Y}{X}$ of $\frac{e}{N}$ with $X < \frac{1}{2}N^{\frac{1}{4}}$:
3: Compute $M = N - \frac{eX}{Y}$ and $N_0 = \left[\frac{M^2}{4N}\right]$.
4: **if** $N_0 < 10^{104}$ **then**
5: Apply ECM to find a and b such that $N_0 = ab$ and $a \leq b \leq 2a$.
6: Apply Coppersmith's algorithm (Theorem 2) with $n = N$ and $\frac{M}{2a}$ as an approximation of y. If Coppersmith's algorithm outputs the factors p and q of N, then stop.
7: **end if**

4.3 An Attack for Large Difference $|ap - bq|$

Here we present the last attack. We suppose $|ap - bq| > aN^{\frac{1}{4}}$ so that the Small and the Medium difference attacks should not succeed. This attack depends on the efficiency of the Elliptic Curve Method (ECM) to find factors up to 10^{52}. Assuming the efficiency of ECM, the term *efficient* is also used to express the fact that every step in this attack can be done in polynomial time.

Theorem 5. *Let $N = pq$ be an RSA modulus with unknown factors p, q such that $q < p < 2q$. Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ such that $a \geq 1$ and $b \leq 10^{52}$. Let e be a public exponent satisfying an equation $eX - (N - (ap + bq))Y = Z$ with $\gcd(X, Y) = 1$. Let $M = N - \frac{eX}{Y}$. Set $D = \sqrt{|M^2 - 4abN|}$ and $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$. If $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ and $|Z| < \frac{1}{3}a|ap - bq|N^{-\frac{1}{4}-\alpha}Y$ then, under ECM, N can be factored efficiently.*

Proof. Combining Proposition 1 and Lemma 1, we have

$$|ap - bq| < \frac{p}{b} < \frac{2^{\frac{1}{2}}N^{\frac{1}{2}}}{b}.$$

Hence, since $a \leq b$, this gives

$$\frac{1}{3}a|ap - bq|N^{-\frac{1}{4}-\alpha} < \frac{1}{3}a \cdot \frac{2^{\frac{1}{2}}N^{\frac{1}{2}}}{b} \cdot N^{-\frac{1}{4}-\alpha} \leq \frac{2^{\frac{1}{2}}}{3}N^{\frac{1}{4}-\alpha}. \tag{6}$$

Now, suppose $|Z| < \frac{1}{3}a|ap - bq|N^{-\frac{1}{4}-\alpha}Y$, $1 \leq Y \leq X$ and $\gcd(X, Y) = 1$. Then using (6), we get

$$|Z| < \frac{2^{\frac{1}{2}}}{3}N^{\frac{1}{4}-\alpha}X < N^{\frac{1}{2}+\alpha}X.$$

Consequently, by Lemma 5, $\frac{Y}{X}$ is a convergent of $\frac{e}{N}$. Next, set $M = N - \frac{eX}{Y}$. Using the equation $eX - (N - ap - bq)Y = Z$, we get

$$|ap + bq - M| = \frac{|Z|}{Y} < \frac{1}{3}a|ap - bq|N^{-\frac{1}{4}-\alpha}. \tag{7}$$

Then using (6), we get

$$|ap + bq - M| < \frac{2^{\frac{1}{2}}}{3}N^{\frac{1}{4}-\alpha} < \frac{1}{2}N^{\frac{1}{2}-\alpha}.$$

Hence, by Lemma 3, $ab = \left[\frac{M^2}{4N}\right]$ and by Lemma 2, we know that a and b are of the same bit-size. Hence, if $b \leq 10^{52}$, then applying the Elliptic Curve Method with $\left[\frac{M^2}{4N}\right]$, we can find a and b.
Next, using $|ap - bq| < 2N^{\frac{1}{2}}$, we can rewrite (7) as

$$|ap + bq - M| < \frac{1}{3}a \cdot 2N^{\frac{1}{2}} \cdot N^{-\frac{1}{4}-\alpha} = \frac{2}{3}aN^{\frac{1}{4}-\alpha} < aN^{\frac{1}{4}}. \tag{8}$$

Now, let $D = \sqrt{|M^2 - 4abN|}$. Then

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

From this we deduce

$$\left||ap - bq| - D\right| \leq \frac{|ap + bq - M||ap + bq + M|}{|ap - bq| + D}.$$

Next, by (8), we have $|ap + bq - M| < aN^{\frac{1}{4}}$. Then $M < ap + bq + aN^{\frac{1}{4}}$ and

$$ap + bq + M < 2(ap + bq) + aN^{\frac{1}{4}} < 3(ap + bq) = 3N^{\frac{1}{2}+\alpha}.$$

Combining with (7), this leads to

$$\left||ap - bq| - D\right| < \frac{3 \cdot \frac{1}{3}a|ap - bq|N^{-\frac{1}{4}-\alpha}N^{\frac{1}{2}+\alpha}}{|ap - bq|} = aN^{\frac{1}{4}}.$$

If $ap - bq > 0$, then combining with (8), we get

$$\begin{aligned}|2ap - M - D| &= \left|ap + bq - M + |ap - bq| - D\right| \\ &\leq \left|ap + bq - M\right| + \left||ap - bq| - D\right| \\ &< 2aN^{\frac{1}{4}}.\end{aligned}$$

Dividing by $2a$, we find that $\frac{M+D}{2a}$ is an approximation of p with additive error at most $N^{\frac{1}{4}}$.

If $ap - bq < 0$, then combining with (8), we get

$$\begin{aligned} |2ap - M + D| &= |ap + bq - M - (bq - ap - D)| \\ &< |ap + bq - M| + \big||ap - bq| - D\big| \\ &< 2aN^{\frac{1}{4}}. \end{aligned}$$

Dividing again by $2a$, we find that $\frac{M-D}{2a}$ is an approximation of p with additive error at most $N^{\frac{1}{4}}$. We can then apply Theorem 2 to the values $\frac{M\pm D}{2a}$. The correct term will lead to the factorization of N. □

Now we summarize the third factorization algorithm.

Algorithm 3 Large $|ap - bq|$

Input: a public key (N, e) satisfying $N = pq$, $q < p < 2q$ and $eX-(N-(ap+bq))Y = Z$ for small parameters X, Y, Z where $\frac{a}{b}$ is an unknown convergent of $\frac{q}{p}$ with $a \geq 1$.
Output: the prime factors p and q.

1: Compute the continued fraction expansion of $\frac{e}{N}$.
2: For every convergent $\frac{Y}{X}$ of $\frac{e}{N}$ with $X < \frac{1}{2}N^{\frac{1}{4}}$:
3: Compute $M = N - \frac{eX}{Y}$ and $N_0 = \left[\frac{M^2}{4N}\right]$.
4: **if** $N_0 < 10^{104}$ **then**
5: Apply ECM to find a and b such that $N_0 = ab$ and $a \leq b \leq 2a$.
6: Compute $D = \sqrt{|M^2 - 4N_0N|}$.
7: Compute $m_1 = \frac{M+D}{2a}$ and $m_2 = \frac{M-D}{2a}$.
8: Apply Coppersmith's algorithm (Theorem 2) with $n = N$ and m_1 and m_2 as approximations of y. If Coppersmith's algorithm outputs the factors p and q, then stop.
9: **end if**

5 Estimation of the Public Exponents for which the Attacks Apply

In this Section, we will study the size of the class of the public keys for which our attacks can be applied. Let $\frac{a}{b}$ be a convergent of $\frac{q}{p}$ with $a \geq 1$. Define α by $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$ and let

$$\mathcal{P}(a,b) = \left\{ (X,Y,z) \;\middle|\; 1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}},\ \gcd(X,Y) = 1,\ |z| < N^{\frac{1}{4}-\frac{\alpha}{2}} \right\},$$

be the set of the parameters and

$$\mathcal{E}(a,b) = \left\{ e \;\middle|\; e = \left\lfloor (N - (ap+bq))\frac{Y}{X} \right\rfloor + z,\ (X,Y,z) \in \mathcal{P}(a,b) \right\},$$

the set of the exponents. We will show that much of these exponents are vulnerable to our attacks. To find a lower bound for the size of the sets $\mathcal{E}(a,b)$, we show that different convergents $\frac{a}{b}$ of $\frac{q}{p}$ and different parameters in the set $\mathcal{P}(a,b)$ define different exponents in the sets $\mathcal{E}(a,b)$.

First, we show that our attacks will work for the exponents in $\mathcal{E}(a,b)$: given an exponent in $\mathcal{E}(a,b)$, it is possible to find the factorization of N according to Theorem 3, Theorem 4 or Theorem 5. First, we start with a result for small difference $|ap-bq|$.

Corollary 1. *Let $N=pq$ be an RSA modulus with $q<p<2q$. Let $\frac{a}{b}$ be an unknown convergent of $\frac{q}{p}$ with $a\geq 1$ and $|ap-bq|<(abN)^{\frac{1}{4}}$. Let X, Y be unknown coprime positive integers with $1\leq Y\leq X<\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ where $ap+bq=N^{\frac{1}{2}+\alpha}$ and $0<\alpha<\frac{1}{2}$. If $e=\left\lfloor (N-(ap+bq))\frac{Y}{X}\right\rfloor+z$ is a public exponent with*

$$|z|<\inf\left((abN)^{\frac{1}{4}}\frac{Y}{X},N^{\frac{1}{4}-\frac{\alpha}{2}}\right),$$

then N can be factored in polynomial time.

Proof. Set $e_0=\left\lfloor (N-(ap+bq))\frac{Y}{X}\right\rfloor$, $e=e_0+z$, $Z=eX-(N-(ap+bq))Y$. We want to show that the conditions of Theorem 3 are satisfied. Assume that $|z|<\inf\left((abN)^{\frac{1}{4}}\frac{Y}{X},N^{\frac{1}{4}-\frac{\alpha}{2}}\right)$. Then, since

$$\left|(N-(ap+bq))\frac{Y}{X}-e_0\right|<1,$$

we get

$$\begin{aligned}|Z|=|eX-(N-(ap+bq))Y|&=|(e_0+z)X-(N-(ap+bq))Y|\\&\leq|e_0X-(N-(ap+bq))Y|+|z|X\\&<(1+|z|)X.\end{aligned}$$

Observe that $(1+|z|)X<(abN)^{\frac{1}{4}}Y$ and, assuming $X<\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$, we find

$$(1+|z|)X<N^{\frac{1}{4}-\frac{\alpha}{2}}\cdot\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}\leq\frac{1}{2}N^{\frac{1}{2}-\alpha}Y.$$

From this, we deduce $|Z|<\inf\left((abN)^{\frac{1}{4}},\frac{1}{2}N^{\frac{1}{2}-\alpha}\right)Y$. It follows that the conditions of Theorem 3 are fulfilled which leads to the factorization of N. □

Next, we give a result for medium difference $|ap-bq|$.

Corollary 2. *Let $N=pq$ be an RSA modulus with $q<p<2q$. Let $\frac{a}{b}$ be an unknown convergent of $\frac{q}{p}$ with $a\geq 1$, $b\leq 10^{52}$ and $(abN)^{\frac{1}{4}}<|ap-bq|<aN^{\frac{1}{4}}$. Let X, Y be unknown coprime positive integers with $1\leq Y\leq X<\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ where $ap+bq=N^{\frac{1}{2}+\alpha}$ and $0<\alpha<\frac{1}{2}$. If $e=\left\lfloor (N-(ap+bq))\frac{Y}{X}\right\rfloor+z$ is a public exponent with*

$$|z|<\inf\left(aN^{\frac{1}{4}}\frac{Y}{X},N^{\frac{1}{4}-\frac{\alpha}{2}}\right),$$

then, under ECM, N can be factored efficiently.

Proof. The proof is similar to that of Corollary 1 and the parameters satisfy the condition of Theorem 4. □

Finally, we give a result which concerns large difference $|ap-bq|$.

Corollary 3. *Let $N=pq$ be an RSA modulus with $q<p<2q$. Let $\frac{a}{b}$ be an unknown convergent of $\frac{q}{p}$ with $a\geq 1$, $b\leq 10^{52}$ and $|ap-bq|>aN^{\frac{1}{4}}$. Let X, Y be unknown coprime positive integers with $1\leq Y\leq X<\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ where $ap+bq=N^{\frac{1}{2}+\alpha}$ and $0<\alpha<\frac{1}{2}$. If $e=\left\lfloor (N-(ap+bq))\frac{Y}{X}\right\rfloor+z$ is a public exponent with*

$$|z|<\min\left(\frac{1}{3}a|ap-bq|N^{-\frac{1}{4}-\alpha}\frac{Y}{X}, N^{\frac{1}{4}-\frac{\alpha}{2}}\right),$$

then, under ECM, N can be factored efficiently.

Proof. Let $Z=eX-(N-(ap+bq))Y$, $e=\left\lfloor (N-(ap+bq))\frac{Y}{X}\right\rfloor+z$ with $|z|<\min\left(\frac{1}{3}a|ap-bq|N^{-\frac{1}{4}-\alpha}\frac{Y}{X}, N^{\frac{1}{4}-\frac{\alpha}{2}}\right)$ and $1\leq Y\leq X<\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$. Using the same arguments as in the proof of Corollary 1, we get

$$|Z|<(1+|z|)X<\frac{1}{3}a|ap-bq|N^{-\frac{1}{4}-\alpha}Y.$$

It follows that all the conditions of Theorem 5 are fulfilled which leads to the factorization of N. □

The following result shows that distinct parameters from $\mathcal{P}(a,b)$ define different exponents in $\mathcal{E}(a,b)$.

Lemma 6. *Let $N=pq$ be an RSA modulus with $q<p<2q$. Let $\frac{a}{b}$ be a convergent of $\frac{q}{p}$ with $a\geq 1$ and $ap+bq=N^{\frac{1}{2}+\alpha}$. Let $(X,Y,z),(X',Y',z')\in\mathcal{P}(a,b)$. Let*

$$e=\left\lfloor (N-(ap+bq))\frac{Y}{X}\right\rfloor+z,\quad e'=\left\lfloor (N-(ap+bq))\frac{Y'}{X'}\right\rfloor+z'.$$

If $e=e'$ then $X=X'$, $Y=Y'$ and $z=z'$.

Proof. Let $e_0=\left\lfloor (N-(ap+bq))\frac{Y}{X}\right\rfloor$, $e_0'=\left\lfloor (N-(ap+bq))\frac{Y'}{X'}\right\rfloor$. If $e=e_0+z$ and $e'=e_0'+z'$ then

$$\begin{aligned}
&\left|(N-(ap+bq))\left(\frac{Y'}{X'}-\frac{Y}{X}\right)-e'+e\right|\\
&\leq\left|(N-(ap+bq))\frac{Y'}{X'}-e_0'-z'\right|+\left|(N-(ap+bq))\frac{Y}{X}-e_0-z\right|\\
&\leq\left|(N-(ap+bq))\frac{Y'}{X'}-e_0'\right|+|z'|+\left|(N-(ap+bq))\frac{Y}{X}-e_0\right|+|z|\\
&<2+|z|+|z'|.
\end{aligned}$$

Suppose $e = e'$. Then, multiplying by XX', we get

$$(N - (ap + bq))\,|Y'X - YX'| < (2 + |z| + |z'|)XX'. \tag{9}$$

We want to compare the sides of (9). Assume that $X, X' < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ and $|z|, |z'| < N^{\frac{1}{4}-\frac{\alpha}{2}}$. Then

$$(2 + |z| + |z'|)XX' < 2N^{\frac{1}{4}-\frac{\alpha}{2}} \cdot \frac{1}{4}N^{\frac{1}{2}-\alpha} = \frac{1}{2}N^{\frac{3}{4}-\frac{3\alpha}{2}}.$$

On the other hand, we have

$$N - (ap + bq) = N - N^{\frac{1}{2}+\alpha} = N^{\frac{3}{4}-\frac{3\alpha}{2}}\left(N^{\frac{1}{4}+\frac{3\alpha}{2}} - N^{-\frac{1}{4}+\frac{5\alpha}{2}}\right).$$

Since $0 < \alpha < \frac{1}{2}$, then $\frac{1}{4} + \frac{3\alpha}{2} > -\frac{1}{4} + \frac{5\alpha}{2}$ and $N^{\frac{1}{4}+\frac{3\alpha}{2}} > N^{-\frac{1}{4}+\frac{5\alpha}{2}} + 1$. Hence $N - (ap + bq) > N^{\frac{3}{4}-\frac{3\alpha}{2}}$. From our comparison of the sides of (9), we conclude that $Y'X - YX' = 0$. Since $\gcd(X, Y) = 1$ and $\gcd(X', Y') = 1$, we find $X = X'$ and $Y = Y'$ and consequently $z = z'$. This terminates the proof. □

Finally, the following result shows that different convergents of $\frac{q}{p}$ lead to different exponents in $\mathcal{E}(a, b)$.

Lemma 7. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $\frac{a}{b}$ and $\frac{a'}{b'}$ be convergents of $\frac{q}{p}$ with $a \geq 1$, $a' \geq 1$, $ap + bq = N^{\frac{1}{2}+\alpha}$ and $a'p + b'q = N^{\frac{1}{2}+\alpha'}$. Let $(X, Y, z) \in \mathcal{P}(a, b)$ and $(X', Y', z') \in \mathcal{P}(a', b')$. Let*

$$e = \left\lfloor (N - (ap + bq))\frac{Y}{X} \right\rfloor + z, \quad e' = \left\lfloor (N - (a'p + b'q))\frac{Y'}{X'} \right\rfloor + z'.$$

If $e = e'$ then $X = X'$, $Y = Y'$, $a = a'$, $b = b'$ and $z = z'$.

Proof. Assume for contradiction that $a \neq a'$, $a < a'$ say. Then $b < b'$. Hence $ap + bq < a'p + b'q$ and $\alpha < \alpha'$. Combining with Lemma 1, we get

$$N - (ap + bq) - (N - (a'p + b'q)) = (a' - a)p + (b' - b)q > p + q > p > N^{\frac{1}{2}},$$

which leads to

$$N - (ap + bq) > N - (a'p + b'q) + N^{\frac{1}{2}} \tag{10}$$

Now, set $e = \left\lfloor (N - (ap + bq))\frac{Y}{X} \right\rfloor + z$, $e' = \left\lfloor (N - (a'p + b'q))\frac{Y'}{X'} \right\rfloor + z'$ and assume $e = e'$. Then, since $|z| < N^{\frac{1}{4}-\frac{\alpha}{2}}$ and $|z'| < N^{\frac{1}{4}-\frac{\alpha'}{2}} < N^{\frac{1}{4}-\frac{\alpha}{2}}$, we get

$$\left|(N - (a'p + b'q))\frac{Y'}{X'} - (N - (ap + bq))\frac{Y}{X}\right| < 2 + |z| + |z'| < 2N^{\frac{1}{4}-\frac{\alpha}{2}}. \tag{11}$$

On the other hand, we know that $\frac{Y}{X}$ and $\frac{Y'}{X'}$ are convergents of the continued fraction expansion of $\frac{e}{N}$. Hence $\frac{Y}{X} \approx \frac{Y'}{X'}$ and, combining (10) with $X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$, we get

$$\begin{aligned}(N-(ap+bq))\frac{Y}{X} &> (N-(a'p+b'q))\frac{Y}{X} + N^{\frac{1}{2}}\frac{Y}{X} \\ &> (N-(a'p+b'q))\frac{Y}{X} + N^{\frac{1}{2}} \cdot \frac{1}{\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}} \\ &\approx (N-(a'p+b'q))\frac{Y'}{X'} + 2N^{\frac{1}{4}+\frac{\alpha}{2}}\end{aligned}$$

It follows that

$$\left|(N-(a'p+b'q))\frac{Y'}{X'} - (N-(ap+bq))\frac{Y}{X}\right| > 2N^{\frac{1}{4}+\frac{\alpha}{2}}.$$

Comparing with (11), we get a contradiction. Hence $a = a'$ and $b = b'$. Now, we have $\left\lfloor (N-(ap+bq))\frac{Y}{X} \right\rfloor + z = \left\lfloor (N-(ap+bq))\frac{Y'}{X'} \right\rfloor + z'$. By Lemma 6, we conclude that $X = X'$, $Y = Y'$ and $z = z'$. This terminates the proof. □

Let us now prove a lower bound for the size of the number of the exponents e that are vulnerable to our approach. Note that we do not require $\gcd(e, \phi(N)) = 1$ as usual.

Theorem 6. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then the number of the exponents $e \in \mathcal{E}(a,b)$ that are vulnerable to the attacks for some convergent $\frac{a}{b} \neq \frac{0}{1}$ of $\frac{q}{p}$ is at least $N^{\frac{3}{4}-\varepsilon}$ where ε is arbitrarily small for suitably large N.*

Proof. We focus on $\mathcal{E}(1,1)$ since the total number of exponents is much higher. Let α_0 such that $p + q = N^{\frac{1}{2}+\alpha_0}$. Since $q < p$, then $2q < p + q < 2p$ and by Lemma 1, we get $2^{\frac{1}{2}}N^{\frac{1}{2}} < N^{\frac{1}{2}+\alpha_0} < 2^{\frac{3}{2}}N^{\frac{1}{2}}$. From this we deduce $\alpha_0 \approx 0$. On the other hand, by Corollary 3, we need

$$|z| < \min\left(\frac{1}{3}|p-q|N^{-\frac{1}{4}-\alpha_0}\frac{Y}{X}, N^{\frac{1}{4}-\frac{\alpha_0}{2}}\right),$$

where $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha_0}{2}}$ and $\gcd(X,Y) = 1$. Observe that for the normal RSA, we have $p - q > cN^{\frac{1}{2}}$ with a constant $c > 0$. So let

$$|z| < \min\left(\frac{c}{3}N^{\frac{1}{4}-\alpha_0}\frac{Y}{X}, N^{\frac{1}{4}-\frac{\alpha_0}{2}}\right),$$

and put

$$X_0 = \left\lfloor \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha_0}{2}} \right\rfloor.$$

We want to estimate

$$\#\mathcal{E}(1,1) = \sum_{X=1}^{X_0} \sum_{\substack{Y=1 \\ \gcd(X,Y)=1}}^{X-1} |z|.$$

Taking $|z| < \frac{c}{3} N^{\frac{1}{4}-\alpha_0} \frac{Y}{X}$, we get

$$\#\mathcal{E}(1,1) = \frac{c}{3} N^{\frac{1}{4}-\alpha_0} \sum_{X=1}^{X_0} \sum_{\substack{Y=1 \\ \gcd(X,Y)=1}}^{X-1} \frac{Y}{X} = \frac{c}{6} N^{\frac{1}{4}-\alpha_0} \sum_{X=1}^{X_0} \phi(X), \tag{12}$$

where we used the well known identity

$$\sum_{\substack{Y=1 \\ \gcd(X,Y)=1}}^{X-1} Y = \frac{1}{2} X \phi(X).$$

Similarly, taking $|z| < N^{\frac{1}{4}-\frac{\alpha_0}{2}}$, we get

$$\#\mathcal{E}(1,1) = N^{\frac{1}{4}-\frac{\alpha_0}{2}} \sum_{X=1}^{X_0} \sum_{\substack{Y=1 \\ \gcd(X,Y)=1}}^{X-1} 1 = N^{\frac{1}{4}-\frac{\alpha_0}{2}} \sum_{X=1}^{X_0} \phi(X). \tag{13}$$

We can rewrite (12) and (13) in a single expression

$$\#\mathcal{E}(1,1) = N^{\frac{1}{4}-\varepsilon_0} \sum_{X=1}^{X_0} \phi(X),$$

for a suitable $\varepsilon_0 > 0$. It is well known (see Theorem 328 of [6]), that

$$\phi(X) > \frac{CX}{\log\log X},$$

where C is a positive constant. Since $X < N$, then $\phi(X) > XN^{-\varepsilon_1}$ for a small positive constant ε_1. From this, we deduce

$$\#\mathcal{E}(1,1) > N^{\frac{1}{4}-\varepsilon_0-\varepsilon_1} \sum_{X=1}^{X_0} X > N^{\frac{1}{4}-\varepsilon_0-\varepsilon_1} \frac{X_0^2}{2} > \frac{1}{8} N^{\frac{3}{4}-\alpha_0-\varepsilon_0-\varepsilon_1},$$

where we used $X_0 \approx \frac{1}{2} N^{\frac{1}{4}-\frac{\alpha_0}{2}}$. We get finally $\#\mathcal{E}(1,1) > N^{\frac{3}{4}-\varepsilon}$, with a constant $\varepsilon \approx \alpha_0 + \varepsilon_0 + \varepsilon_1$ depending only on N. This terminates the proof. □

6 Conclusion

In this paper, we showed how to perform three attacks on RSA using the ratio of the primes. The attacks apply when the public key (N, e) satisfies an equation $eX - (N - (ap + bq))Y = Z$ with suitably small parameters X, Y and Z where $\frac{a}{b}$ is an unknown convergent of $\frac{q}{p}$ with $a \geq 1$. The attacks combine a variety of techniques, including continued fractions, Coppersmith's lattice based method and H.W. Lenstra's Elliptic Curve Method for Factoring (ECM). Our results illustrate once again the fact that we should be very cautious when using RSA with specific exponents. Moreover, we showed that the number of such exponents is at least $N^{\frac{3}{4}-\varepsilon}$. Using the notion of weak keys, as defined by Blömer and May [1], the results of this paper show that this set of RSA public keys is a class of weak keys.

References

1. 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)
2. 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)
3. Brent, R.P.: Some integer factorization algorithms using elliptic curves, Australian Computer Science Communications, vol. 8, 149-163 (1986)
4. Brent, R.P.: Recent progress and prospects for integer factorisation algorithms, Springer-Verlag LNCS 1858, 3–22 (2000)
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 (1965)
7. Lehman, R.S.: Factoring large integers. Mathematics of Computation, Vol. 28, 637-646, (1974)
8. Lenstra, H.W.: Factoring integers with elliptic curves, Annals of Mathematics, vol. 126, 649-673 (1987)
9. 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 (May 1990)
10. Montgomery, P.L.: Speeding the Pollard and elliptic curve methods of factorization, Mathematics of Computation, vol. 48, 243-264 (1987)
11. Morrison, M.A., Brillhart, J.: A method of factoring and the factorization of F7, Math. of Comput., t. 29, pp. 183–205 (1975)
12. Nitaj, A.: Cryptanalysis of RSA with constrained keys, International Journal of Number Theory (to appear).
13. Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (ed.) Africacrypt 2008. LNCS, vol. 5023, pp. 174–190. Springer, Heidelberg (2008)
14. Pollard, J.M.: A Monte Carlo method for factorization. BIT 15, pp. 331- 334 (1975)
15. 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)
16. Silverman, R.D.: The multiple polynomial quadratic sieve, Mathematics of Computation, Vol. 48, pp. 329-339 (1987)
17. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553-558 (1990)
18. Zimmermann, P.: 50 largest factors found by ECM
`http://www.loria.fr/~zimmerma/records/top50.html`