A New Attack on RSA with Two or Three Decryption Exponents

No Author Given

No Institute Given

Abstract. Let $N = pq$ be an RSA modulus, i.e. the product of two large unknown primes of equal bit-size. In this paper, we describe an attack on RSA in the presence of two or three exponents e_i with the same modulus N and satisfying equations $e_i x_i - \phi(N) y_i = z_i$, where $\phi(N) = (p-1)(q-1)$ and x_i, y_i, z_i are unknown parameters. The new attack is an extension of Guo's continued fraction attack as well as the Blömer and May lattice-reduction basis attack.

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

1 Introduction

The RSA public-key cryptosystem was invented by Rivest, Shamir, and Adleman [9] in 1978. Since then, the RSA system has been the best known and most widely accepted public key cryptosystem. Encryption and decryption in RSA each requires an exponentiation modulo a large modulus N which is the product of two large primes, p and q. The exponents in the exponentiations are the public exponent e for encryption and the private exponent d for decryption. The exponents e and d are related by the equation $ed - k\phi(N) = 1$ for some positive integer k where $\phi(N) = (p-1)(q-1)$ is the Euler totient function of N. To reduce the decryption time or signature generation, it may be tempting to use a small private exponent d. Unfortunately, based on the convergents of the continued fraction expansion of $\frac{e}{N}$, Wiener [10] showed that the RSA system can be totally broken if $d < \frac{1}{3}N^{\frac{1}{4}}$. Then, in 1999, based on lattice basis reduction, Boneh and Durfee [2] proposed a new attack on the use of short secret exponents. They showed that the RSA system can be totally broken if $d < N^{0.292}$. In 1994, Blömer and May [1] proposed a different attack on RSA with a public exponent e satisfying the equation $ex + y = k\phi(N)$ with $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| < \mathcal{O}\left(N^{-\frac{3}{4}}ex\right)$. This attack combines the convergents of the continued fraction expansion of $\frac{e}{N}$ and the seminal work of Coppersmith [3] for solving bivariate polynomial equations.

In 1999, Guo (see [6]) proposed an attack on RSA when there are two or more instances of RSA, having the same modulus, with public exponents e_i, $i = 1, 2, \ldots$. The attack is based on the continued fraction algorithm and can be

used to factor the modulus if the private exponents d_i are each less than $N^{\frac{1}{3}-\varepsilon}$ for some $\varepsilon > 0$. In 1999, Howgrave-Graham and Seifert [6] proposed an extension of Guo's attack that allows the RSA system to be broken in the presence of two decryption exponents (d_1, d_2) with $d_1, d_2 < N^{\frac{5}{14}}$. In the presence of three decryption exponents, Howgrave-Graham and Seifert improved the bound to $N^{\frac{2}{5}}$. The attack of Howgrave-Graham and Seifert is based on lattice reduction methods. Very recently, Sarkar and Maitra [7] used a different lattice based technique and improved the bound $N^{\frac{5}{14}}$ for the case of two decryption exponents up to $N^{0.416}$. In [7], Sarkar and Maitra proposed a generalized attack when $n \geq 2$ many decryption exponents d_i are used with the same RSA modulus N and $d_i < N^{\frac{3n-1}{4n+4}}$ for each i, $1 \leq i \leq n$.

In this paper, we combine the attack of Guo and the attack of Blömer and May to mount a new attack on RSA with two or three decryption exponents and a common modulus. Let $N = pq$ be an RSA modulus with $q < p < 2q$ and e_i, $i = 1, 2, \ldots$ be two or three public exponents. Assume that each exponent satisfies an equation $e_i x_i - \phi(N) y_i = z_i$. We show, that, depending on certain inequalities verified by the parameters x_i, y_i, z_i, one can find the factorization of the RSA modulus N. The new approach still uses the continued fraction algorithm and the lattice-reduction basis technique of Coppersmith [3].

The rest of this paper is organized as follows. In Section 2 we present the attack of Guo as well as the attack of Blömer and May. In Section 3, we prove three lemmas to be used in our new approach. We present the new approach for two exponents in Section 4 and for three exponents in Section 5. We conclude the paper in Section 6.

2 Former Attacks

Since the motivation for our new attack originates from Guo's continued fraction attack and the Blömer and May lattice attack, we revisit these attacks in this section.

2.1 Guo's attack for two exponents

Guo's attack was described in [6] by Howgrave-Graham and Seifert (see also [5]). It is based on the continued fraction algorithm and makes use of the following result (see [4], Theorem 184).

Theorem 1 (Legendre). *Let ξ be a real number. If a and b are coprime integers such that*

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

then $\frac{a}{b}$ is a convergent of the continued fraction expansion of ξ.

Guo's attack concerns at least two public exponents e_1, e_2 such that $e_1 d_1 - k_1 \lambda(N) = 1$ and $e_2 d_2 - k_2 \lambda(N) = 1$, where $\lambda(N) = \mathrm{lcm}(p-1, q-1)$. Eliminating

$\lambda(N)$, we find the equation $e_1d_1k_2 - e_2d_2k_1 = k_2 - k_1$. Dividing by $e_2d_1k_2$, we get

$$\left|\frac{e_1}{e_2} - \frac{d_2k_1}{d_1k_2}\right| = \frac{|k_2 - k_1|}{e_2d_1k_2}.$$

Hence, if $2|k_2 - k_1|d_1k_2 < e_2$, then

$$\frac{|k_2 - k_1|}{e_2d_1k_2} < \frac{1}{2(d_1k_2)^2}.$$

Thus, by Theorem 1, $\frac{d_2k_1}{d_1k_2}$ must be one of the convergents of the continued fraction of $\frac{e_1}{e_2}$. Moreover, if d_1 and d_2 are bounded, $d_1 < N^\delta$, $d_2 < N^\delta$ say, then k_1 and k_2 are also bounded since for $e_i < \phi(N)$ we have

$$k_i = \frac{e_id_i - 1}{\phi(N)} < \frac{e_id_i}{\phi(N)} < d_i.$$

It follows that the condition $2|k_2 - k_1|d_1k_2 < e_2$ reduces to $2N^{3\delta} < N$, or equivalently $\delta < \frac{1}{3} - \varepsilon$, where ε is a small positive constant.

In practice, Guo's attack is effective if one can find d_1 or d_2 using the convergent $\frac{d_2k_1}{d_1k_2}$. This means that the quantities d_i, k_i, $i = 1, 2$, must satisfy $\gcd(d_1k_2, d_2k_1) = 1$. Moreover, it is necessary to factor d_1k_2 or d_2k_1. Since $k_i < d_i < N^\delta$, $i = 1, 2$, then $\max(d_1k_2, d_2k_1) < N^{2\delta} < N^{\frac{2}{3}}$. Depending on the structure of the quantities d_i and k_i, $i = 1, 2$, the numbers d_1k_2 and d_2k_1 are not expected to be of a difficult factorization shape and can be factored easily. Using the exact values of d_1 and k_1 in $e_1d_1 - k_1\lambda(N) = 1$, this gives the factorization of N.

Later, using lattice based techniques, Howgrave-Graham and Seifert [6] increased the bound up to $d_1, d_2 < N^{\frac{5}{14}}$. This bound was recently improved to $d_1, d_2 < N^{0.416}$ by Sarkar and Maitra [7].

2.2 Guo's attack for three exponents

To avoid the factorization problem, Guo proposed to use three exponents. Consider that three public exponents e_1, e_2, e_3 satisfying the key equations

$$e_1d_1 - k_1\lambda(N) = 1, \qquad e_2d_2 - k_2\lambda(N) = 1, \qquad e_3d_3 - k_3\lambda(N) = 1,$$

satisfy also the inequalities $2|k_2 - k_1|d_1k_2 < e_2$ and $2|k_3 - k_1|d_1k_3 < e_3$. Combining the key equations, we get

$$e_1d_1k_2 - e_2d_2k_1 = k_2 - k_1, \qquad e_1d_1k_3 - e_3d_3k_1 = k_3 - k_1.$$

Proceeding as in Guo's first attack, we find the inequalities

$$\left|\frac{e_1}{e_2} - \frac{d_2k_1}{d_1k_2}\right| = \frac{|k_2 - k_1|}{e_2d_1k_2} < \frac{1}{2(d_1k_2)^2},$$
$$\left|\frac{e_1}{e_3} - \frac{d_3k_1}{d_1k_3}\right| = \frac{|k_3 - k_1|}{e_3d_1k_3} < \frac{1}{2(d_1k_3)^2}.$$

Using Theorem 1, we see that $\frac{d_2k_1}{d_1k_2}$ is one of the convergents of the continued fraction of $\frac{e_1}{e_2}$ and similarly, $\frac{d_3k_1}{d_1k_3}$ is one of the convergents of the continued fraction of $\frac{e_1}{e_3}$. Suppose in addition that $\gcd(d_2k_1, d_1k_2) = 1$, $\gcd(d_3k_1, d_1k_3) = 1$, $\gcd(d_2, d_3) = 1$ and $\gcd(k_2, k_3) = 1$, then $\frac{d_2k_1}{d_1k_2}$ and $\frac{d_3k_1}{d_1k_3}$ are in lowest terms and

$$\gcd(d_1k_2, d_1k_3) = d_1, \qquad \gcd(d_2k_1, d_3k_1) = k_1.$$

With d_1 and k_1 known, the factorization of N becomes trivial using the equation $e_1d_1 - k_1\lambda(N) = 1$.

In 1999, it was shown by Howgrave-Graham and Seifert [6] that the bound $d_i < N^{\frac{1}{3}}$ with $i = 1, 2, 3$ can be improved using lattice reduction techniques and very recently, Sarkar and Maitra [8] increased this bound up to $d_i < N^{\frac{1}{2}}$.

2.3 The Blömer and May attack

In 2004, Blömer and May[1] proposed an attack on RSA with a modulus $N = pq$ with $q < p < 2q$ and a public exponent e satisfying an equation $ex + y = k\phi(N)$. The attack is based on a combination of the continued fraction algorithm and Coppersmith's lattice-based technique for finding small roots of bivariate polynomial equation [3].

Theorem 2 (Coppersmith). *Let $N = pq$ be the product of two unknown primes such that $q < p < 2q$. Suppose we know an approximation $\widetilde{P}$ of p such that $\left|p - \widetilde{P}\right| < 2N^{\frac{1}{4}}$. Then N can be factored in polynomial time.*

Suppose that e satisfies an equation $ex + y = k\phi(N)$. Under the conditions

$$0 < x < \frac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad |y| = |ex - k\phi(N)| \leq \mathcal{O}\left(N^{-\frac{3}{4}}ex\right), \tag{1}$$

the fraction $\frac{k}{x}$ satisfies $\left|\frac{k}{x} - \frac{e}{N}\right| < \frac{1}{2x^2}$. By Theorem 1, this shows that $\frac{k}{x}$ can be found among the convergents of the continued fraction expansion of $\frac{e}{N}$. Using $\phi(N) = (p-1)(q-1) = N + 1 - p - q$ in the equation $ex + y = k\phi(N)$, Blömer and May showed that $N + 1 - \frac{ex}{k}$ is an approximation of $p + q$ satisfying

$$\left|p + q - \left(N + 1 - \frac{ex}{k}\right)\right| = \frac{|y|}{k} < \frac{4}{3}cN^{\frac{1}{4}},$$

where $c < 1$ is a positive constant satisfying $p - q > cN^{\frac{1}{2}}$. Next, they derived that $\sqrt{\left(N + 1 - \frac{ex}{k}\right)^2 - 4N}$ is an approximation of $p - q$ up to an error term at most $9N^{\frac{1}{4}}$. Finally, combining the approximations of $p+q$ and $p-q$, they found an approximation of p up to an error term of at most $6N^{\frac{1}{4}}$ which leads to the exact value of p using Coppersmith's Theorem 2.

3 Useful Lemmas

In this section we state and prove three lemmas needed for the new attack. The first is the following result.

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that S is an approximation of $p + q$ satisfying*

$$|p + q - S| < \frac{3(p-q)N^{\frac{1}{4}}}{2(p+q) + N^{\frac{1}{4}}}. \tag{2}$$

Then $\widetilde{P} = \frac{1}{2}\left(S + \sqrt{|S^2 - 4N|}\right)$ is an approximation of p with $\left|p - \widetilde{P}\right| < 2N^{\frac{1}{4}}$.

Proof. Suppose that S is a positive integer satisfying (2). Let $D = \sqrt{|S^2 - 4N|}$. We have

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

Dividing by $p - q + D$, we get

$$|p - q - D| \leq \frac{p + q + S}{p - q + D} \times \frac{3(p-q)N^{\frac{1}{4}}}{2(p+q) + N^{\frac{1}{4}}}. \tag{3}$$

Let us find a bound for $\frac{p+q+S}{p-q+D}$. From (2), we derive

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

On the other hand, we have $p - q + D > p - q$. Plugging in (3), we deduce

$$|p - q - D| \leq \frac{2(p+q) + N^{\frac{1}{4}}}{p-q} \times \frac{3(p-q)N^{\frac{1}{4}}}{2(p+q) + N^{\frac{1}{4}}} = 3N^{\frac{1}{4}}. \tag{4}$$

Now, using (2) and (4), we get

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

Dividing by 2, we find

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

which terminates the proof. □

The second lemma is the following.

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e_1, e_2 be integers satisfying the equations*

$$e_1 x_1 - \phi(N) y_1 = z_1, \qquad e_2 x_2 - \phi(N) y_2 = z_2.$$

If $2x_1 y_2 |z_1 y_2 - z_2 y_1| < e_2$ then $\frac{x_2 y_1}{x_1 y_2}$ is a convergent of $\frac{e_1}{e_2}$.

Proof. Suppose that e_1, e_2 satisfy the equations $e_1 x_1 - \phi(N) y_1 = z_1$ and $e_2 x_2 - \phi(N) y_2 = z_2$. Then eliminating $\phi(N)$, we get

$$e_1 x_1 y_2 - e_2 x_2 y_1 = z_1 y_2 - z_2 y_1.$$

Dividing both sides by $e_2 x_1 y_2$, we get

$$\left| \frac{e_1}{e_2} - \frac{x_2 y_1}{x_1 y_2} \right| = \frac{|z_1 y_2 - z_2 y_1|}{e_2 x_1 y_2}. \tag{5}$$

Suppose that the parameters satisfy the inequality $2x_1 y_2 |z_1 y_2 - z_2 y_1| < e_2$. Then (5) yields

$$\left| \frac{e_1}{e_2} - \frac{x_2 y_1}{x_1 y_2} \right| < \frac{1}{2(x_1 y_2)^2}.$$

Combining with Theorem 1, we see that $\frac{x_2 y_1}{x_1 y_2}$ is a convergent of $\frac{e_1}{e_2}$. □

Finally, we will use the following result.

Lemma 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e_1 be an integer satisfying the equation $e_1 x_1 - \phi(N) y_1 = z_1$, with known positive parameters x_1, y_1. Then, under the condition*

$$|z_1| < \frac{3(p-q)N^{\frac{1}{4}} y_1}{2(p+q) + N^{\frac{1}{4}}},$$

N can be factored in polynomial time.

Proof. Suppose that e_1 satisfies the conditions of the theorem where x_1, y_1 are known positive integers. Using $\phi(N) = N + 1 - p - q$ in the equation $e_1 x_1 - \phi(N) y_1 = z_1$, we get

$$\left| p + q - \left(N + 1 - \frac{e_1 x_1}{y_1} \right) \right| = \frac{|z_1|}{y_1} < \frac{3(p-q)N^{\frac{1}{4}}}{2(p+q) + N^{\frac{1}{4}}}.$$

This implies that $S = N + 1 - \frac{e_1 x_1}{y_1}$ is an approximation of $p + q$ up to an error term satisfying the condition of Lemma 1. Hence $\widetilde{P} = \frac{1}{2}\left(S + \sqrt{|S^2 - 4N|} \right)$ is an approximation of p up to an error term at most $2N^{\frac{1}{4}}$. Thus, using Coppersmith's Theorem 2, one can find p in polynomial time. □

4 The New Attack on RSA with Two Exponents

In this section, we investigate RSA with the same modulus and two public exponents e_1 and e_2 satisfying the equations $e_1x_1-\phi(N)y_1 = z_1$, and $e_2x_2-\phi(N)y_2 = z_2$, where the parameters satisfy

$$\gcd(x_2y_1, x_1y_2) = 1, \tag{6}$$

$$x_1y_2|z_1y_2 - z_2y_1| < \frac{e_2}{2}. \tag{7}$$

This means that the conditions of Lemma 2 are satisfied which implies that $\frac{x_2y_1}{x_1y_2}$ can be found in the continued fraction expansion of $\frac{e_1}{e_2}$. The condition (6) implies that the convergent $\frac{x_2y_1}{x_1y_2}$ is in lowest terms which gives x_2y_1 and x_1y_2. Now, we wish to recover the values of the parameters x_1, y_1, x_2, y_2. Using the assumptions that x_1, y_2, $|z_1y_2 - z_2y_1|$ are at most N^δ and that $e_2 \approx N$, the condition (7) is satisfied whenever $N^{3\delta} < \frac{1}{2}N$, that is $\delta = \frac{1}{3} - \varepsilon$, for some small $\varepsilon > 0$. Moreover, if x_2y_1 and x_1y_2 are not of a difficult factorization shape, then their factorization is feasible for instances of RSA with a 1024-bit modulus. Thus, factoring x_2y_1 and x_1y_2 will reveal the parameters x_1, y_1.

To find the prime factors p and q of the RSA modulus $N = pq$, we must make the assumption that the parameter z_1 satisfies

$$|z_1| < \frac{3(p-q)N^{\frac{1}{4}}y_1}{2(p+q) + N^{\frac{1}{4}}}.$$

Thus, the conditions of Lemma 3 are satisfied which leads to the factorization of N.

We summarize the first attack in Algorithm 1.

An Example for the New Attack with Two Exponents

As an example, let us take

$$\begin{aligned} N &= 78783023222142579402299, \\ e_1 &= 20339472065400293617, \\ e_2 &= 16071808231974749459. \end{aligned}$$

The first 30 partial quotients of $\frac{e_1}{e_2}$ are

$$\begin{aligned} [1,\ 3,\ 1,\ 3,\ 3,\ 1,\ 2,\ 59,\ 1,\ 2,\ 2,\ 2,\ 1,\ 1,\ 3,\ 1,\ 1, \\ 4,\ 3,\ 1,\ 7,\ 18,\ 10,\ 1,\ 13,\ 1,\ 1,\ 316,\ 4,\ 1,\ \cdots] \end{aligned}$$

Each convergent $\frac{a}{b}$ is a candidate for $\frac{x_2y_1}{x_1y_2}$. The 27th convergent is

$$\frac{a}{b} = \frac{3889559329731}{3073445144167}$$

Algorithm 1 Two exponents

Input: $N = pq$ with $q < p < 2q$, two public exponents e_i, $i = 1, 2$ satisfying $e_i x_i - \phi(N) y_i = z_i$ with unknown parameters x_i, y_i, z_i.

Output: The prime factors p and q.

```
Compute the continued fraction expansion of e1/e2.
for every convergent pk/qk of e1/e2 with max(pk, qk) < N^(2/3) do
    Factor pk and qk.
    for every divisor y1 of pk do
        for every divisor x1 of qk do
            Compute S = N + 1 − e1x1/y1 and P̃ = 1/2 (S + √|S^2 − 4N|).
            Apply Coppersmith's algorithm (Theorem 2) with P̃ as an approximation of
            p.

            if Coppersmith's algorithm outputs the factorization of N, then
                stop.
            end if
        end for
    end for
end for
```

We see that $a \approx N^{0.550}$, $b \approx N^{0.546}$ are not of difficult factorization shape. We get easily $a = 3^3 \cdot 229 \cdot 6079 \cdot 103483$ and $b = 41 \cdot 43 \cdot 71 \cdot 1693 \cdot 14503$ and we see that the largest prime factor is $103483 \approx N^{0.22}$. Next, the decomposition

$$a = x_2 y_1 = 71092821 \cdot 54711, \qquad b = x_1 y_2 = 211917889 \cdot 14503,$$

gives $x_1 = 211917889$, $y_1 = 54711$, $x_2 = 71092821$ and $y_2 = 14503$. Using the equation $e_1 x_1 - \phi(N) y_1 = z_1$, we get $p + q = N + 1 - \frac{e_1 x_1}{y_1} + \frac{z_1}{y_1}$. We then make the assumption that

$$p + q \approx S = N + 1 - \frac{e_1 x_1}{y_1} \approx 594807230437.$$

From this, we get the approximation

$$p - q \approx D = \sqrt{|S^2 - 4N|} \approx 196630487186.$$

Combining the approximations of $p + q$ and $p - q$, we get

$$p \approx \frac{S + D}{2} \approx 395718858812.$$

Then Coppersmith's algorithm 2 gives $p = 395718860549$ and $q = 199088370751$.

Note that, in this example, the private exponents $d_i \equiv e_i^{-1} \pmod{\phi(N)}$, $i = 1, 2$, are

$$d_1 = 63426822067770650216953 \approx N^{0.996},$$
$$d_2 = 68134122111136587656939 \approx N^{0.997},$$

so that $d_1, d_2 > N^{\frac{1}{2}}$, which explains why Guo's attack would fail in this case. On the other hand, in connection with the attack of Blömer and May as described in Subsection 2.3, the fraction $\frac{y_1}{x_1}$ is not among the convergents of the continued fraction of $\frac{e_1}{N}$. Similarly, $\frac{y_2}{x_2}$ is not among the convergents of the continued fraction of $\frac{e_2}{N}$. Moreover, all the convergents $\frac{x}{k}$ of $\frac{e_1}{N}$ with $x < \frac{1}{3}N^{\frac{1}{4}}$ are such that $|e_1x - k\phi(N)| > N^{-\frac{3}{4}}e_1x$ so that the condition (1) is never satisfied. We have a similar result with the convergents of $\frac{e_2}{N}$. This explains why Blömer and May's attack would also fail in this case.

5 The New Attack on RSA with Three Exponents

To avoid factoring integers of size $N^{\frac{2}{3}}$, we consider in this section that a third instance of RSA with the same modulus is available. Suppose we have three public exponents e_1, e_2, e_3 satisfying the equations

$$e_1x_1 - \phi(N)y_1 = z_1, \qquad e_2x_2 - \phi(N)y_2 = z_2, \qquad e_3x_3 - \phi(N)y_3 = z_3,$$

where the parameters satisfy $\gcd(x_2y_1, x_1y_2) = 1$, $\gcd(x_3y_1, x_1y_3) = 1$ and

$$x_1y_2\ |z_1y_2 - z_2y_1| < \frac{e_2}{2},$$
$$x_1y_3\ |z_1y_3 - z_3y_1| < \frac{e_3}{2}.$$

This immediately shows that the conditions of Lemma 2 are satisfied for (e_1, e_2) and for (e_1, e_3). Hence $\frac{x_2y_1}{x_1y_2}$ is in lowest terms and is a convergent of $\frac{e_1}{e_2}$. Similarly, $\frac{x_3y_1}{x_1y_3}$ is in lowest terms and is a convergent of $\frac{e_1}{e_3}$. This gives

$$\gcd(x_1y_2, x_1y_3) = x_1, \qquad \gcd(x_2y_1, x_3y_1) = y_1.$$

Now, if the condition

$$|z_1| < \frac{3(p-q)N^{\frac{1}{4}}y_1}{2(p+q) + N^{\frac{1}{4}}},$$

is satisfied, then by Lemma 3 one can find p using Coppersmith's Theorem with the approximation

$$\widetilde{P} = \frac{1}{2}\left(S + \sqrt{|S^2 - 4N|}\right),$$

of p where $S = N + 1 - \frac{e_1x_1}{y_1}$.

We summarize the attack in Algorithm 2

An Example for the New Attack with Three Exponents

Here we take an RSA modulus $N = pq$ and three public exponents e_1, e_2 and e_3 as

$$N = 95026423511070214659367,$$
$$e_1 = 988283832402044225959,$$
$$e_2 = 35887685050144510339,$$
$$e_3 = 4465685820126103902929.$$

Algorithm 2 Three Exponents

Input: $N = pq$ with $q < p < 2q$, three public exponents e_i, $i = 1, 2, 3$, satisfying $e_i x_i - \phi(N) y_i = z_i$ with unknown parameters x_i, y_i, z_i.

Output: The prime factors p and q.

```
Compute the continued fraction expansion of e1/e2.
Compute the continued fraction expansion of e1/e3.
for every convergent a/b of e1/e2 do
  for every convergent c/d of e1/e3 do
    Compute x1 = gcd(b, d), y1 = gcd(a, c).
    Compute S = N + 1 − e1x1/y1 and P̃ = 1/2 (S + sqrt(|S^2 − 4N|)).
    Apply Coppersmith's algorithm (Theorem 2) with P̃ as an approximation of p.

    if Coppersmith's algorithm outputs the factorization of N, then
      stop.
    end if
  end for
end for
```

The candidates for $\frac{x_2 y_1}{x_1 y_2}$ are the convergents of $\frac{e_1}{e_2}$. Indeed, the 25th convergent of $\frac{e_1}{e_2}$ is $\frac{44398785042941}{1612259112200}$. Similarly, the candidates for $\frac{x_3 y_1}{x_1 y_3}$ are the convergents of $\frac{e_1}{e_3}$. The 35th convergent of $\frac{e_1}{e_3}$ is $\frac{6433869008153}{29072252986700}$. From the two convergents, we get

$$x_1 = \gcd(1612259112200, 29072252986700) = 59365900,$$
$$y_1 = \gcd(44398785042941, 6433869008153) = 617411.$$

Using the equation $e_1 x_1 - \phi(N) y_1 = z1$, we get $p + q = N + 1 - \frac{e_1 x_1}{y_1} + \frac{z_1}{y_1}$, and neglecting $\frac{z_1}{y_1}$, we get

$$p + q \approx S = N + 1 - \frac{e_1 x_1}{y_1} \approx 642772787002.$$

From this, we get the approximation

$$p - q \approx D = \sqrt{|S^2 - 4N|} \approx 181799784560.$$

Using the approximations S and D, we get $p \approx \frac{S+D}{2} \approx 412286285781$. Finally, applying Coppersmith's Theorem 2, we get

$$p = 412286285849, \qquad q = \frac{N}{p} = 230486501183.$$

We notice that, for $i = 1, 2, 3$, the integers d_i related to e_i by the relations $e_i d_i \equiv 1 \pmod{\phi(N)}$ satisfy $d_i > N^{0.98}$ which is far from Guo's upper bound $N^{\frac{1}{3}}$ as described in Subsection 2.2. This shows that Guo's method would fail here. On the other hand, for $i = 1, 2, 3$, the convergents of the rational numbers $\frac{e_i}{N}$ are all different from the expected convergents $\frac{y_i}{x_i}$. Moreover, for $i = 1, 2, 3$,

the conditions (1) are not satisfied by the convergents of $\frac{e_i}{N}$. This shows that the method of Blömer and May would also fail in this case.

6 Conclusion

In this paper, we have presented a new attack on RSA with the same modulus $N = pq$ and two or three exponents satisfying equations $e_i x_i - \phi(N) y_i = z_i$ with specific unknown parameters x_i, y_i, z_i. Our attack is an extension of Guo's attack as well as an extension of the Blömer and May attack. The new attack enables us to find p and q efficiently with two exponents and in polynomial time with three exponents. This proves once again that, under some conditions, RSA is insecure even when the private exponents are sufficiently large.

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 Ű Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, pp. 1–11 (1999)
3. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
4. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, London (1965)
5. Hinek, M.J., Lam, C.C.Y.: Common modulus attacks on small private exponent RSA and some fast variants (in Practice), J. Math. Cryptology, Volume 4, Issue 1, July 2010, pp. 58–93 (2010)
6. Howgrave-Graham, N. and Seifert, J.-P.: Extending Wiener's attack in the presence of many decrypting exponents. In Secure Networking - CQRE (Secure)'99, volume 1740 of Lecture Notes in Computer Science, pp. 153–166. Springer-Verlag, (1999)
7. Sarkar,S., Maitra, S.: Cryptanalysis of RSA with two decryption exponents, Inform. Process. Lett. 110 (5) pp. 178–181 (2010)
8. Sarkar,S., Maitra, S.: Cryptanalysis of RSA with more than one decryption exponent, Inform. Process. Lett. 110 (8-9) pp. 336–340 (2010)
9. Rivest, R., Shamir A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)
10. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, pp. 553– 558 (1990)