Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 3, pp. 945–961
DOI : 10.47974/JDMSC-1570

Improved cryptanalysis of RSA

Virgile Dossou-Yovo[†]
Institut de Mathématiques et de Sciences Physiques
Dangbo
Bénin

Abderrahmane Nitaj*
Normandie Univ
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Normandie
France

Alain Togbé [§]
Department of Mathematics, Statistics
Purdue University Northwest
Westville
U.S.A.

Abstract

Let $N = pq$ be an RSA modulus and e be a public exponent. Let $\varphi(N) = (p-1)(q-1)$ be the Euler's totient function. The equation $ex^2 - \varphi(N)y^2 = z$ has infinitely many solutions in integers (x, y, z). We show that if x, y and z are suitably small, then one can factor the RSA modulus. Our bounds on the size of the solutions x, y, and z improve the existing bounds of some attacks on RSA such as Wiener's continued fractions based attack, and Blömer-May's lattice reduction based attack.

Subject Classification: *94A60.*

Keywords: *RSA, Cryptanalysis, Factorization, Continued fractions.*

[†] *E-mail:* **dosvirs20@gmail.com**
* *E-mail:* **abderrahmane.nitaj@unicaen.fr (Corresponding Author)**
[§] *E-mail:* **atogbe@pnw.edu**

© Taru Publications

1. Introduction

RSA [20] is the most widely used public key cryptosystem. It is implemented in various industrial products to secure sensitive information, web traffic, and e-mails. The security of RSA is mainly based on two hard problems: the integer factorization problem, and the RSA problem. Despite the hardness of such problems, RSA has been extensively studied for vulnerabilities by several algebraic attacks. In RSA, the public parameters are a couple (N,e) of two positive integers. The parameter N is called the RSA modulus and is of the form $N=pq,$ where p and q are large prime numbers. The second parameter e is called the public exponent, and satisfies $\gcd(e,\varphi(N))=1,$ where $\varphi(N)=(p-1)(q-1)$ is the Euler's totient function. The private exponent is the positive integer d satisfying $ed\equiv 1(\mathrm{mod}\,\varphi(N)).$ Many variants of RSA have been proposed, and some can be parallelized as shown in [19], or can serve to build signatures as in [23].

Most of the algebraic attacks on RSA exploit the modular equation $ed\equiv 1(\mathrm{mod}\,\varphi(N))$ by transforming it to a key equation $ed-k\varphi(N)=1.$ In 1990, Wiener [24] presented an attack on RSA that can solve the key equation. The attack is based on the continued fractions expansion algorithm and factors the modulus N if $d<\frac{1}{3}N^{\frac{1}{4}}.$ This bound was improved in 1997 by Boneh and Durfee [4] up to $d<N^{0.292}$ by applying Coppersmith's method [6] and lattice reduction techniques [12]. In 2004, Blömer and May [1] transformed the key equation into a variant equation of the form $ex+z\equiv 0(\mathrm{mod}\,\varphi(N))$ and showed that the RSA modulus can be factored if the parameters x,z satisfy $0<x<\frac{1}{3}N^{\frac{1}{4}}$ and $|z|<N^{-\frac{3}{4}}ex.$ Their method is based on a combination of the continued fractions expansion algorithm and Coppersmith's lattice based method. More attacks on RSA can be fond in [3, 9, 15].

In this paper, we extend the Blömer-May attack by studying the variant equation $ex^2-\varphi(N)y^2=z.$ We show that our attack enables us to factor the RSA modulus N whenever the unknown parameters x, y, z satisfy

$$0<x<\frac{\sqrt{2}}{4}\sqrt{N}e^{-\frac{1}{4}},\quad |z|<\frac{p-q}{4(p+q)}N^{-\frac{3}{4}}ex^2.$$

In a typical situation when $e\approx N,$ the former bounds reduce to

$$0<x<\frac{\sqrt{2}}{4}N^{\frac{1}{4}},\quad |z|<\frac{p-q}{4(p+q)}N^{\frac{1}{4}}x^2.$$

For comparison, for $e \approx N$, the attack of Blömer-May with the equation $ex^2 - \varphi(N)y^2 = z$ is valid with significantly less bounds

$$0 < x < \frac{1}{\sqrt{3}} N^{\frac{1}{8}}, \quad |z| < N^{\frac{1}{4}} x^2.$$

The new attack is based on the following facts.

- For p and q of the same bit size with $q < p < 2q$, we show that $\sqrt{N}$ is a good approximation of $\sqrt{\varphi(N)}$.
- For sufficiently small parameters x, y, z, we show that $\frac{y}{x}$ is a convergent of the continued fractions expansion of $\frac{\sqrt{e}}{\sqrt{N}}$.
- Using x and y, we show that $N + 1 - \frac{ex^2}{y^2}$ is a good approximation of $p + q$.
- Under the former facts, we apply Coppersmith's method to find p and q which gives the factorization of N.
- Finally, we show that the number of exponents e that are vulnerable to our attack is exponentially large, namely, it is at least $\frac{p-q}{p+q} N^{\frac{1}{8}-\varepsilon} e^{\frac{1}{2}}$, where ε is a small positive constant. Typically, for $e \approx N$, this lowest bound is $N^{\frac{5}{8}-\varepsilon}$.

The rest of the paper is organized as follows. In Section 2, we briefly review some basic results that are used in the paper, including continued fractions expansions and Coppersmith's method. In Section 3, we review some attacks on RSA that are based on equations of the form $ex - \varphi(N)y = z$. In Section 4, we present the new attack. In Section 5, we give a comparative study between the new attack and former similar attacks. In Section 6, we give an explicit lower bound for the number of exponents that are vulnerable to our attack. We conclude the paper in Section 7.

2. Preliminaries

In this section, we present some results that will be used in the rest of the paper.

2.1 *Continued fractions*

Definition 1 (Continued fraction): Let ξ be a non-zero positive real number. The continued fractions expansion of ξ is defined by the expression

$$\xi = [a_0, a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

where the a_i's are integers with $a_0 \geq 0$ and $a_i > 0$, for $i > 0$.

A rational number is represented by a finite continued fractions expansion of the form $[a_0, \ldots, a_n]$. Using the Euclidean division, we can expand every rational number in a finite continued fractions expansion.

Definiton 2 (Convergent) : Let $[a_0, a_1, \ldots]$ be the continued fractions expansion of ξ. The convergents of ξ are the truncated series $[a_0, a_1, \ldots, a_m]$ with $m \geq 0$.

The list of the convergents of a rational number $\xi = \frac{a}{b}$ can be obtained by applying the Euclidean algorithm to a and b (see [18]). Each convergent is a rational number of the form $\frac{p_m}{q_m}$ with $\gcd(p_m, q_m) = 1$. Conversely, the following result gives a sufficient condition to assert that $\frac{u}{v}$ with $\gcd(u, v) = 1$ is one of the convergents of ξ (see [18]).

Theorem 1 : *Let ξ be a real number. Suppose $\gcd(u, v) = 1$ and*

$$\left|\xi - \frac{u}{v}\right| < \frac{1}{2v^2}.$$

Then $\frac{u}{v}$ is one of the convergents of the continued fractions expansion of ξ..

2.2 *Coppersmih's method*

At Eurocrypt'96, Coppersmith [6] described a polynomial-time algorithm for finding small roots of univariate modular equations. The method is based on lattice reduction techniques and has been applied for cryptanalysis of various variants of RSA as in [1, 2, 4, 5, 6, 7, 11, 13, 14, 16, 17, 22]. The following result is a direct application of Coppersmith's method (see [6, 14]).

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

When p and q are of the same bit size, they can be ordered such that $q < p < 2q$. The following result can be found in [17].

Lemma 1 : *Let* $N = pq$ *be an RSA modulus with* $q < p < 2q$. *Suppose we know an approximation S of* $p+q$ *such that* $S > 2N^{\frac{1}{2}}$ *and*

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

Then $\tilde{P} = \frac{1}{2}(S + \sqrt{S^2 - 4N})$ *is an approximation of p satisfying* $|p - \tilde{P}| < N^{\frac{1}{4}}$.

Similarly, the following result can be found in [16].

Lemma 2 : *Let* $N = pq$ *be the product of two unknown integers such that* $q < p < 2q$. *Then*

$$2\sqrt{N} < p+q < \frac{3\sqrt{2}\sqrt{N}}{2}.$$

From Lemma 2, we easily get

$$\varphi(N) = N + 1 - (p+q) > N + 1 - \frac{3\sqrt{2}\sqrt{N}}{2} > \frac{1}{2}N. \tag{1}$$

The following result is a direct consequence of the previous results.

Lemma 3 : *Let* $N = pq$ *be an RSA modulus with* $q < p < 2q$. *Then*

$$\sqrt{N} - \sqrt{\varphi(N)} < \sqrt{2}.$$

Proof: We have $0 < N - \varphi(N) = p + q - 1 < p + q$. Then

$$0 < \sqrt{N} - \sqrt{\varphi(N)} < \frac{p+q}{\sqrt{N} + \sqrt{\varphi(N)}}.$$

By (1), we have $\sqrt{N} + \sqrt{\varphi(N)} > \sqrt{N} + \frac{\sqrt{2}}{2}\sqrt{N} > \frac{3}{2}\sqrt{N}$. Combining this with Lemma 2, we get

$$0 < \sqrt{N} - \sqrt{\varphi(N)} < \frac{3\sqrt{2}\sqrt{N}}{3\sqrt{N}} = \sqrt{2}.$$

This completes the proof of the lemma. □

3. Former attacks on RSA

In this section, we present two former attacks on RSA, namely the attack of Wiener, and the attack of Blömer and May. We always consider RSA moduli of the form $N = pq$ where the prime factors p and q are of the same bit-size with $q < p < 2q$.

3.1 *Wiener's attack*

Wiener's attack [24] on RSA consists in determining the private key d in the equation $ed - k\varphi(N) = 1$ with $\phi(N) = (p-1)(q-1)$, when $d < \frac{1}{3}N^{\frac{1}{4}}$, using the public key (e, N). It can be summarized as follows.

Since $q < p < 2q$ and $N = pq$, then $q < \sqrt{N}$ and $N - \varphi(N) = p + q - 1 < 3\sqrt{N}$. Also, since $d \equiv e^{-1} (\mathrm{mod}\, \varphi(N))$, then there exists an integer k such that $ed - k\varphi(N) = 1$. Therefore, $k = \frac{ed-1}{\varphi(N)}$. Since $e < \varphi(N)$ and $d < \frac{1}{3}N^{\frac{1}{4}}$, we get

$$k < d < \frac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Thus, applying Theorem 1, we get $\frac{k}{d}$ as a convergent of the continued fractions expansion of $\frac{e}{N}$. This enables to find k and d and to compute $\varphi(N)$ using $\varphi(N) = \frac{ed-1}{k}$. Knowing N and $\varphi(N)$, we can find p and q and factor N.

In 1999, Boneh and Durfee [4] improved Wiener's attack up to $d < N^{0.292}$ by applying a technique based on lattice reduction and Coppersmith's method.

3.2 *The attack of Blömer and May*

The attack of Blömer and May [2] is a generalization of Wiener's attack on RSA. It is based on continued fractions and Coppersmith's method, and consists in finding p and q using the public key (N, e) satisfying the equation $ex + z = \varphi(N)y$ with $0 < x \leq \frac{1}{3}N^{\frac{1}{4}}$, $|z| \leq N^{-\frac{3}{4}}ex$ and $N \geq 2^{12}$. It can be summarized as follows.

If $e < \varphi(N)$ satisfies the equation $ex + z = \varphi(N)y$ with $0 < x \leq \frac{1}{3}N^{\frac{1}{4}}$, $|z| \leq N^{-\frac{3}{4}}ex$ and $N \geq 2^{12}$, then

$$\left|\frac{e}{N}-\frac{y}{x}\right|<\frac{1}{2x^2},$$

which by Theorem 1, gives $\frac{y}{x}$ as one of the convergents of $\frac{e}{N}$. Let $s=N+1-\frac{ex}{y}$ and $t=\sqrt{s^2-4N}$. One can show that p satisfies

$$\left|p-\frac{1}{2}(s+t)\right|<6N^{\frac{1}{4}}.$$

Then, by Theorem 2, p and q can be found.

4. The new attack

In this section, we present our new attack to solve the equation $ex^2-\varphi(N)y^2=z$ when x, y and z are suitably small. The new method combines two techniques, the continued fractions expansion algorithm and Coppersmith's method.

Theorem 3 *: Let $N=pq$ be an RSA modulus with $q<p<2q$, and e a public exponent. If e satisfies the equation $ex^2-\varphi(N)y^2=z$ with*

$$0<x<\frac{\sqrt{2}}{4}\sqrt{N}e^{-\frac{1}{4}},\quad |z|<\frac{p-q}{4(p+q)}N^{-\frac{3}{4}}ex^2,$$

then one can factor N in polynomial time.

Proof : Suppose that $ex^2-\varphi(N)y^2=z$ with $x>0$ and $y>0$. Then

$$\left|\frac{\sqrt{e}}{\sqrt{\varphi(N)}}-\frac{y}{x}\right|=\frac{|z|}{(\sqrt{e}x+\sqrt{\varphi(N)}y)x\sqrt{\varphi(N)}}.$$

Since $x>0$ and $y>0$, then $\sqrt{e}x+\sqrt{\varphi(N)}y>\sqrt{e}x$. By (1), we have $\varphi(N)>\frac{1}{2}N$. Then

$$\left|\frac{\sqrt{e}}{\sqrt{\varphi(N)}}-\frac{y}{x}\right|<\frac{|z|}{\sqrt{e\varphi(N)}x^2}<\frac{\sqrt{2}\,|z|}{\sqrt{eN}x^2},$$

and

$$\left|\frac{\sqrt{e}}{\sqrt{N}}-\frac{x}{y}\right| \le\left|\frac{\sqrt{e}}{\sqrt{N}}-\frac{\sqrt{e}}{\sqrt{\varphi(N)}}\right|+\left|\frac{\sqrt{e}}{\sqrt{\varphi(N)}}-\frac{y}{x}\right|$$

$$< \sqrt{e}\frac{\sqrt{N}-\sqrt{\varphi(N)}}{\sqrt{N\varphi(N)}}+\frac{\sqrt{2}\,|z|}{\sqrt{eN}x^2}.$$

By Lemma 3, we have $\sqrt{N}-\sqrt{\varphi(N)}<\sqrt{2}$. Combining with $\varphi(N)>\frac{1}{2}N$, this implies

$$\left|\frac{\sqrt{e}}{\sqrt{N}}-\frac{y}{x}\right|<\frac{2\sqrt{e}}{N}+\frac{\sqrt{2}\,|z|}{\sqrt{eN}x^2}.$$

Now, suppose that $|z|<\frac{p-q}{4(p+q)}N^{-\frac{3}{4}}ex^2$. Then

$$\left|\frac{\sqrt{e}}{\sqrt{N}}-\frac{y}{x}\right|<\frac{2\sqrt{e}}{N}+\frac{p-q}{4(p+q)}\frac{\sqrt{2}\sqrt{e}}{N^{\frac{5}{4}}}<\frac{4\sqrt{e}}{N}.$$

Finally, suppose that $x<\frac{\sqrt{2}}{4}\sqrt{N}e^{-\frac{1}{4}}$. Then

$$\left|\frac{\sqrt{e}}{\sqrt{N}}-\frac{y}{x}\right|<\frac{1}{2x^2}.$$

Hence, by Theorem 1, it follows that $\frac{y}{x}$ is a convergent of the continued fractions expansion of $\frac{\sqrt{e}}{\sqrt{N}}$. Using the values of x and y in the equation $ex^2-\varphi(N)y^2=z$, we get

$$\left|p+q-\left(N+1-\frac{ex^2}{y^2}\right)\right|=\frac{|z|}{y^2}. \tag{2}$$

On the other hand, we have $y^2=\frac{ex^2-z}{\varphi(N)}$ with $|z|<\frac{p-q}{4(p+q)}N^{-\frac{3}{4}}ex^2$. Then

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

This gives

$$\frac{|z|}{y^2}<\frac{\frac{p-q}{4(p+q)}N^{-\frac{3}{4}}ex^2}{\frac{4(p+q)-(p-q)N^{-\frac{3}{4}}}{4(p+q)\varphi(N)}ex^2}=\frac{(p-q)\varphi(N)}{4(p+q)N^{\frac{3}{4}}-(p-q)}.$$

Since $\varphi(N)<N$ and $4(p+q)N^{\frac{3}{4}}-(p-q)>3(p+q)N^{\frac{3}{4}}$, then the above inequality gives

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

Plugging this in (2), we get $\left| p+q-\left(N+1-\frac{ex^2}{y^2} \right) \right| < \frac{p-q}{3(p+q)} N^{\frac{1}{4}}$. This implies that $S = N+1-\frac{ex^2}{y^2}$ is an approximation of $p+q$ satisfying the conditions of Lemma 1, and $\tilde{P} = \frac{1}{2}(S+\sqrt{S^2-4N})$ is an approximation of p with an error term less than $N^{\frac{1}{4}}$. Then, using Theorem 2, we find p and q in polynomial time. This completes the proof. □

The method described in Theorem 3 is summarized in Algorithm 1.

Algorithm 1 : The new attack on RSA

Require: A modulus $N = pq$ and a public exponent e satisfying $ex^2 - \varphi(N)y^2 = z$, for some unknown parameters x, y and z with $0 < x < \frac{\sqrt{2}}{4}\sqrt{N}e^{-\frac{1}{4}}$, and $|z| < \frac{p-q}{4(p+q)} N^{-\frac{3}{4}} ex^2$.

Ensure: The prime factors p and q.

1: Compute the convergents $\frac{y}{x}$ of the continued fractions expansion of $\frac{\sqrt{e}}{\sqrt{N}}$ with $0 < x < \frac{\sqrt{2}}{4}\sqrt{N}e^{-\frac{1}{4}}$.

2: **for** every convergent $\frac{y}{x}$ **do**

3: Compute $S = N+1-\frac{ex^2}{y^2}$.

4: Compute $\tilde{P} = \frac{1}{2}(S+\sqrt{S^2-4N})$.

5: Apply Coppersmith's algorithm to $\tilde{P}$.

6: **if** Coppersmith's algorithm succeeds **then**

7: Return p and q.

8: Stop.

9: **end if**

10: **end for**

5. Comparison with former attacks

In this section, we compare our attack on RSA and to the three attacks proposed by Wiener, Bonech-Durfee and Blömer-May.

5.1 *Comparison with the attack of Wiener and the attack of Boneh-Durfee*

Wiener [24] showed that if d satisfies the equation $ed - k\varphi(N) = 1$, with $d < \frac{1}{3}N^{\frac{1}{4}}$, then $N = pq$ can be factored. Boneh and Durfee [4] improved the bound to $d < N^{0.292}$. In our attack, the equation is of the form $ex^2 - \varphi(N)y^2 = z$, and Theorem 3 works whenever

$$0 < x^2 < \frac{1}{8}Ne^{-\frac{1}{2}}, \quad |z| < \frac{p-q}{4(p+q)}N^{-\frac{3}{4}}ex^2.$$

In the typical situation when $e \approx N$, this reduces to

$$0 < x^2 < \frac{1}{8}N^{\frac{1}{2}}, \quad |z| < \frac{p-q}{4(p+q)}N^{\frac{1}{4}}x^2.$$

We can observe here that the bound $0 < x^2 < \frac{1}{8}N^{\frac{1}{2}}$ is much larger than the bound in Wiener's attack, that is $x^2 < \frac{1}{3}N^{\frac{1}{4}}$, and the bound of Boneh-Durfee which works if $x^2 < \frac{1}{3}N^{0.292}$. On the other hand, as it is shown in [21], the bound in Wiener's method is optimal and cannot be improved. This shows that our attack exceeds the method of Wiener as well as the method of Boneh-Durfee when e satisfies an equation of the form $ex^2 - \varphi(N)y^2 = z$.

5.2 *Comparison with the attack of Blömer and May*

The attack of Blömer and May[2] shows that it is possible to factor the RSA modulus N if the public exponent satisfies an equation of the form $eX - \varphi(N)Y = Z$ whenever

$$0 \le X \le \frac{1}{3}N^{\frac{1}{4}}, \quad |Z| \le cN^{-\frac{3}{4}}eX,$$

for some constant $c \le 1$. In our attack, the equation is $ex^2 - \varphi(N)y^2 = z$, where

$$0 < x^2 < \frac{1}{8}Ne^{-\frac{1}{2}}, \quad |z| < \frac{p-q}{4(p+q)}N^{-\frac{3}{4}}ex^2.$$

In the typical situation when $e \approx N$, the former inequalities reduce to

$$0 < x^2 < \frac{1}{8}N^{\frac{1}{2}}, \quad |z| < \frac{p-q}{4(p+q)}N^{\frac{1}{4}}x^2,$$

while the bounds of Blömer and May with the equation $ex^2 - \varphi(N)y^2 = z$ are

$$0 \le x^2 \le \frac{1}{3}N^{\frac{1}{4}}, \quad \left|Z\right| \le cN^{-\frac{3}{4}}ex^2,$$

As we can see, our bound $0 < x^2 < \frac{1}{8}N^{\frac{1}{2}}$ is much larger than the bound $0 \le x^2 \le \frac{1}{3}N^{\frac{1}{4}}$ of Blömer and May.

5.3 *A numerical example*

Consider the RSA modulus N and the public exponent e:

$N = 44254807952654506026358254774170994794330953716214094547946055878610008163047964853309116998767353736709508953 9,$

$e = 32733564153123767345772372407533036640929859286265193518387060498430053692717604276259876815649249720661489806 53.$

Then, using the convergent $\frac{y}{x} = \frac{562161147956321250258287517}{65364871214712145302492 8143}$ of $\frac{\sqrt{e}}{\sqrt{N}}$, we get an approximation S of $p+q$ with

$$S = \left[N + 1 - \frac{ex^2}{y^2}\right]$$
$$= 136913931902577004232972607047219095922112063342217983569,$$

from which we get an approximation $\tilde{P}$ for p with

$$\tilde{P} = \left[\frac{1}{2}(S + \sqrt{S^2 - 4N})\right]$$
$$= 84608603391202224093130640096334886934102128855948705716.$$

Then by Coppersmith's method (Theorem 1), we get

$$p = 84608603391202224093130640096334886961765531427889000229.$$

Hence

$$q = \frac{N}{p} = 52305328511374780139841966950884208970908324233024000391.$$

Using $\phi(N)=(p-1)(q-1)$, we get

$$\begin{aligned} d &\equiv e^{-1} (\mathrm{mod}\, \phi(N)) \\ &\equiv 10260679836500383925881429687897941177025120569916086328 \\ &\quad 48235614793145714535338696765556756380130948486344412677. \end{aligned}$$

We observe that $d \approx N^{0.994} \gg N^{0.292}$. This shows that the attack of Wiener as well as the attack of Boneh-Durfee will not succeed to factor N.

On the other hand, all the convergents $\frac{Y}{X}$ of the continued fractions expansion of $\frac{e}{n}$ with $X < \frac{1}{3}N^{\frac{1}{4}}$ are such that $|eX - \phi(N)Y| > N^{-\frac{3}{4}}eX$. This shows that the attack of Blömer and May will not succeed to factor N.

6. The Number of Weak Exponents

In this section, we show that there are at least $\frac{p-q}{p+q}N^{\frac{1}{8}-\varepsilon}e^{\frac{1}{2}}$ public exponents that are vulnerable to our attack for $N=pq$ with $q<p<2q$.

Lemma 4 : *For* $i=1,2$, *let* $e_i = \left\lfloor \varphi(N)\frac{y_i^2}{x_i^2} \right\rfloor + u_i$ *where*

$$0 < x_i < \frac{\sqrt{2}}{4}N^{\frac{7}{16}}e^{-\frac{1}{4}}, \quad |u_i| < \frac{p-q}{4(p+q)}N^{-\frac{3}{4}}e, \quad 0 < y_i < x_i, \quad \gcd(x_i, y_i) = 1.$$

If $e_1 = e_2$, *then* $(x_1, y_1, u_1) = (x_2, y_2, u_2)$.

Proof: For $i=1,2$, let $e_i = \left\lfloor \varphi(N)\frac{y_i^2}{x_i^2} \right\rfloor + u_i$. Suppose that $e_1 = e_2$. Then, for $i=1,2$, we have

$$e_1 - u_1 \le \varphi(N)\frac{y_1^2}{x_1^2} < e_1 - u_1 + 1,$$

$$e_1 - u_2 \le \varphi(N)\frac{y_2^2}{x_2^2} < e_1 - u_2 + 1.$$

Eliminating e_1, we get

$$u_2 - u_1 - 1 < \varphi(N)\left(\frac{y_1^2}{x_1^2} - \frac{y_2^2}{x_2^2}\right) < u_2 - u_1 + 1,$$

from which we get

$$\varphi(N)\left|x_2^2y_1^2 - x_1^2y_2^2\right| < (u_1+u_2+1)x_1^2x_2^2. \tag{3}$$

Using the facts that $0 < x_i < \frac{\sqrt{2}}{4} N^{\frac{7}{16}} e^{-\frac{1}{4}}$ and $|u_i| < \frac{p-q}{4(p+q)} N^{-\frac{3}{4}} e$ for $i = 1, 2,$ we get

$$\begin{aligned}(u_1 + u_2 + 1)x_1^2 x_2^2 &< 3\max(|u_1|, |u_2|)x_1^2 x_2^2 \\ &< \frac{3(p-q)}{4(p+q)} N^{-\frac{3}{4}} e \cdot \left(\frac{\sqrt{2}}{4} N^{\frac{7}{16}} e^{-\frac{1}{4}} \right)^4 \\ &= \frac{3(p-q)}{256(p+q)} N \\ &< N.\end{aligned}$$

Plugging this in (3), we get

$$\varphi(N) \left| x_2^2 y_1^2 - x_1^2 y_2^2 \right| < N. \tag{4}$$

If $\left| x_2^2 y_1^2 - x_1^2 y_2^2 \right| = 1,$ then $|x_2 y_1 - x_1 y_2| \, |x_2 y_1 + x_1 y_2| = 1,$ and $x_2 y_1 = 0$ or $x_1 y_2 = 0,$ which contradicts $x_i > 0$ and $y_i > 0$ for $i = 1, 2.$ If $\left| x_2^2 y_1^2 - x_1^2 y_2^2 \right| \geq 2,$ then $2\varphi(N) < N$ and $N + 2 < 2(p+q),$ which contradicts Lemma 2. As a consequence, (4) implies that $x_2^2 y_1^2 - x_1^2 y_2^2 = 0,$ and since $\gcd(x_i, y_i) = 1$ for $i = 1, 2,$ we get $x_1 = x_2,$ and $y_1 = y_2.$ Plugging this in $e_1 = e_2,$ we get

$$\left\lfloor \varphi(N) \frac{y_1^2}{x_1^2} \right\rfloor + u_1 = \left\lfloor \varphi(N) \frac{y_2^2}{x_2^2} \right\rfloor + u_2,$$

and $u_1 = u_2.$ This terminates the proof. □

Lemma 4 shows that two different tuples (x_1, y_1, u_1) and (x_2, y_2, u_2) produce different public exponents $e_1 = \left\lfloor \varphi(N) \frac{y_1^2}{x_1^2} \right\rfloor + u_1$ and $e_2 = \left\lfloor \varphi(N) \frac{y_2^2}{x_2^2} \right\rfloor + u_2$ that are vulnerable to our attack. The following result gives a very conservative estimation of the number of such weak exponents.

Theorem 4 : *Let $N = pq$ be an RSA modulus with $q < p < 2q$. The number of the exponents e of the form*

$$e = \left\lfloor \varphi(N)\frac{y^2}{x^2} \right\rfloor + u,$$

with the conditions $\gcd(e, \varphi(N)) = 1$ *and*

$$0 < x < \frac{\sqrt{2}}{4} N^{\frac{7}{16}} e^{-\frac{1}{4}}, \ 0 < y < x, \ \gcd(x, y) = 1, |u_i| < \frac{p-q}{4(p+q)} N^{-\frac{3}{4}} e,$$

is at least

$$\frac{p-q}{p+q} N^{\frac{1}{8}-\varepsilon} e^{\frac{1}{2}},$$

where ε *is a small positive constant.*

Proof: Set $M_x = \left\lfloor \frac{\sqrt{2}}{4} N^{\frac{7}{16}} e^{-\frac{1}{4}} \right\rfloor$, and $M_u = \left\lfloor \frac{p-q}{4(p+q)} N^{-\frac{3}{4}} e \right\rfloor$. Then, the number N_e of exponents e of the form

$$e = \left\lfloor \varphi(N)\frac{y^2}{x^2} \right\rfloor + u,$$

with the conditions $0 < x \le M_x$, $\gcd(x, y) = 1$, $0 < y < x$, and $|u_i| \le M_u$ is

$$N_e = M_u \sum_{x=1}^{M_x} \sum_{\substack{y=1 \\ \gcd(y,x)=1}}^{x-1} 1 = M_u \sum_{x=1}^{M_x} \varphi(x).$$

By the totient summatory function property (see Theorem 330 of [8]), we have $\sum_{x=1}^{M_x} \varphi(x) \ge \frac{3}{\pi^2} M_x^2$. Then

$$N_e \ge \frac{3}{\pi^2} M_u M_x^2 \approx \frac{3(p-q)}{32\pi^2(p+q)} N^{\frac{1}{8}} e^{\frac{1}{2}}.$$

Actually, one needs $\gcd(e, \varphi(N)) = 1$. Since the probability that e and $\varphi(N)$ should be coprime is $\frac{6}{\pi^2}$ (see Theorem 332 of [8]), then, with the additional condition $\gcd(e, \varphi(N)) = 1$, the number N_e reduces to $N_{e'}$ with

$$N_{e'} = \frac{6}{\pi^2} N_e \ge \frac{9(p-q)}{16\pi^4(p+q)} N^{\frac{1}{8}} e^{\frac{1}{2}} = \frac{p-q}{p+q} N^{\frac{1}{8}-\varepsilon} e^{\frac{1}{2}},$$

where ε is a small positive constant. This completes the proof. □

In the standard situation that $p-q=\mathcal{O}\left(N^{\frac{1}{2}}\right)$ and $e=\mathcal{O}(N)$, we get

$$\frac{p-q}{p+q}N^{\frac{1}{8}-\varepsilon}e^{\frac{1}{2}}=\mathcal{O}(N^{\frac{5}{8}-\varepsilon}).$$

This shows that the number of exponents that are vulnerable to our attack is more significant compared to Wiener's attack and Boneh-Durfee's attack where such numbers are $\mathcal{O}(N^{\frac{1}{4}-\varepsilon})$ and $\mathcal{O}(N^{0.292-\varepsilon})$ respectively.

7. Conclusion

In this paper, we studied the general equation $ex^2-\varphi(N)y^2=z$ where N is an RSA modulus and e is a public exponent. By combining the continued fractions expansion algorithm and Coppersmith's technique, we showed that it is possible to solve the equation and to factor the RSA modulus under the conditions $0<x<\frac{\sqrt{2}}{4}\sqrt{N}e^{-\frac{1}{4}}$, $|z|<\frac{p-q}{4(p+q)}N^{-\frac{3}{4}}ex^2$. We compared our attack to the attack of Wiener and the attack of Blömer-May on RSA. In both cases, our attack works with improved bounds. Moreover, we showed that the number of exponents that are vulnerable to our attack is significant.

References

[1] J. Blömer and A. May, A generalized Wiener attack on RSA. In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, 1-13. Springer-Verlag.

[2] J. Blömer and A. May, New partial key exposure attacks on RSA, Proceedings of CRYPTO 2003, LNCS 2729 (2003), pp. 27–43. Springer Verlag.

[3] D. Boneh, Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 (2), pp. 203–213, 1999.

[4] D. Boneh and G. Durfee, 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, pp. 1–11, 1999.

[5] D. Boneh, G. Durfee and Y. Frankel, An attack on RSA given a small fraction of the private key bits. In: Ohta, K., Pei, D. (eds.) Advances

in Cryptology Asiacrypt'98. Lecture Notes in Computer Science, vol. 1514, pp. 25–34. Springer-Verlag 1998.

[6] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10(4), pp. 233–260, 1997.

[7] M. Ernst, E. Jochemsz, A. May and B. de Weger, Partial key exposure attacks on RSA up to full size exponents. In: Cramer, R. (ed.) Advances in Cryptology Eurocrypt 2005. Lecture Notes in Computer Science, vol. 3494, pp. 371–386. Springer-Verlag 2005.

[8] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers. Oxford University Press, London, 1965.

[9] M. Hinek, Cryptanalysis of RSA and Its Variants, Chapman & Hall/ CRC, Cryptography and Network Security Series, Boca Raton, (2009).

[10] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, pp. 131–142, Springer-Verlag (1997).

[11] E. Jochemsz and A. May, A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: ASIACRYPT 2006, LNCS, vol. 4284, 2006, pp. 267–282, Springer-Verlag.

[12] A.K. Lenstra, H.W. Lenstra and Lovász, Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, 1982.

[13] S. Maitra and S. Sarkar, Revisiting Wiener's Attack - New Weak Keys in RSA. In: Wu TC., Lei CL., Rijmen V., Lee DT. (eds) Information Security. ISC 2008. Lecture Notes in Computer Science, vol 5222. Springer, Berlin, Heidelberg 2008.

[14] A. May, New RSA Vulnerabilities Using Lattice Reduction Methods. PhD thesis, University of Paderborn (2003). Available at

http://wwwcs.upb.de/cs/ag-bloemer/personen/alex/publikationen/

[15] M. Mumtaz and L. Ping, Forty years of attacks on the RSA cryptosystem: A brief survey, *Journal of Discrete Mathematical Sciences and Cryptography*, 22:1, pp. 9–29 (2019)

[16] A. Nitaj, Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (Ed.) Africacrypt 2008. LNCS, vol. 5023, 174–190. Springer, Heidelberg (2008).

[17] A. Nitaj, M.R.K. Ariffin, D.I. Nassr and H.M. Bahig, New Attacks on the RSA Cryptosystem, In: Pointcheval D., Vergnaud D. (eds), Progress in Cryptology - Africacrypt 2014. LNCS, vol. 8469, pp. 178–198. Springer, Cham (2014).

[18] I. Niven, H. S. Zuckerman and H.L. Montgomery, An Introduction to the theory of numbers, John Wiley & Sons, Inc. New York, Chichester, Brisbane, Toronto and Singapore 1991.

[19] A. Rawat, K. Sehgal, A. Tiwari, A. Sharma and A. Joshi, A novel accelerated implementation of RSA using parallel processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 22:2, pp. 309–322, 2019.

[20] R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126,1978.

[21] R. Steinfeld, S. Contini, H. Wang and J. Pieprzyk, Converse Results to the Wiener Attack on RSA. In: Vaudenay S. (eds) Public Key Cryptography - PKC 2005. PKC 2005. Lecture Notes in Computer Science, vol 3386. Springer, Berlin, Heidelberg 2005.

[22] H.M Sun, Mu-EnWu, R. Steinfeld, J. Guo and H. Wang, Cryptanalysis of Short Exponent RSA with Primes Sharing Least Significant Bits. M.K. Franklin, L.C.K. Hui, D.S. Wong (Eds.): CANS 2008, LNCS 5339, pp. 49–63, 2008.

[23] S. Tanwar and A. Kumar, An efficient and secure identity based multiple signatures scheme based on RSA, *Journal of Discrete Mathematical Sciences and Cryptography,* 22:6, pp. 953–971, 2019.

[24] M. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Transactions on Information Theory,* Vol. 36, pp. 553–558, 1990.

Received June, 2021