Another Generalization of Wiener's Attack on RSA

Abderrahmane NITAJ

Université de Caen, France

Casablanca, June 12, 2008

الدار البيضاء، المغرب

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

RSA and Wiener The new attack

Conclusion

RSA setting Wiener's attack Generalizations

## **Colour conventions**

## Red

Secret parameters.

Blue or Black

Public parameters.

Abderrahmane NITAJ Another Generalization of Wiener's Attack on RSA

(日)

크

RSA and Wiener The new attack

Conclusion

RSA setting Wiener's attack Generalizations

## **Colour conventions**

## Red

Secret parameters.

## **Blue or Black**

Public parameters.

ヘロマ ヘロマ ヘロマ ヘ

크

RSA setting Wiener's attack Generalizations

## **RSA cryptosystem**

- Rivest, Shamir and Adleman (1977).
- The most successful public key encryption algorithm.
- The security of RSA is based on the problem of factoring large integers.

(I)

RSA setting Wiener's attack Generalizations

## The RSA modulus

- *p*, *q* large primes with the same bit-size.
- N = pq.

## The public and private exponents

- $\phi(N) = (p-1)(q-1)$ .
- $e \in \mathbb{N}$ , 1 <  $e < \phi(N)$ , the public exponent.
- $d \in \mathbb{N}$ ,  $1 < d < \phi(N)$ , the private exponent.
- $ed \equiv 1 \pmod{\phi(N)}$ .

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Main goal

Given *N*, *e*, find *p*, *q*.

< ロ > < 回 > < 回 > < 回 > < 回 > <</p>

æ

RSA setting Wiener's attack Generalizations

## The RSA modulus

- *p*, *q* large primes with the same bit-size.
- N = pq.

## The public and private exponents

- $\phi(N) = (p-1)(q-1)$ .
- $e \in \mathbb{N}$ ,  $1 < e < \phi(N)$ , the public exponent.
- $d \in \mathbb{N}$ ,  $1 < d < \phi(N)$ , the private exponent.
- $ed \equiv 1 \pmod{\phi(N)}$ .

### The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Main goal

Given *N*, *e*, find *p*, *q*.

<ロ> <四> <四> <四> <三> <三> <三> <三> <三> <三> <三

RSA setting Wiener's attack Generalizations

## The RSA modulus

- *p*, *q* large primes with the same bit-size.
- N = pq.

## The public and private exponents

- $\phi(N) = (p-1)(q-1)$ .
- $e \in \mathbb{N}$ ,  $1 < e < \phi(N)$ , the public exponent.
- $d \in \mathbb{N}$ ,  $1 < d < \phi(N)$ , the private exponent.
- $ed \equiv 1 \pmod{\phi(N)}$ .

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Main goal

Given *N*, *e*, find *p*, *q*.

<ロ> <四> <四> <四> <三> <三> <三> <三> <三> <三> <三

RSA setting Wiener's attack Generalizations

## The RSA modulus

- *p*, *q* large primes with the same bit-size.
- N = pq.

## The public and private exponents

- $\phi(N) = (p-1)(q-1)$ .
- $e \in \mathbb{N}$ ,  $1 < e < \phi(N)$ , the public exponent.
- $d \in \mathbb{N}$ ,  $1 < d < \phi(N)$ , the private exponent.
- $ed \equiv 1 \pmod{\phi(N)}$ .

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Main goal

Given *N*, *e*, find *p*, *q*.

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

#### Wiener's attack, 1990

If  $d < \frac{1}{3}N^{\frac{1}{4}}$  then  $\frac{k}{d}$  is among the convergents of the continued fraction expansion of  $\frac{e}{N}$  and the factorization of N = pq can be found.

#### The method

•  $\frac{k}{d} \approx \frac{e}{N}$ . • The continued fraction algorithm

・ロト ・ 日 ・ ・ ヨ ・ ・ ヨ ・

æ

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Wiener's attack, 1990

If  $d < \frac{1}{3}N^{\frac{1}{4}}$  then  $\frac{k}{d}$  is among the convergents of the continued fraction expansion of  $\frac{e}{N}$  and the factorization of N = pq can be found.

#### The method

•  $\frac{k}{d} \approx \frac{e}{N}$ . • The continued fraction algorithm

• □ • • □ • • □ • • □ • • □ •

1

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

### Wiener's attack, 1990

If  $d < \frac{1}{3}N^{\frac{1}{4}}$  then  $\frac{k}{d}$  is among the convergents of the continued fraction expansion of  $\frac{e}{N}$  and the factorization of N = pq can be found.

# The method • $\frac{k}{d} \approx \frac{e}{N}$ . • The continued fraction algorithm.

Abderrahmane NITAJ Another Generalization of Wiener's Attack on RSA

・ロト ・四ト ・ヨト

æ

RSA and Wiener	RSA setting
The new attack	Wiener's attack
Conclusion	Generalizations

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Boneh-Durfee's attack, 2000

If  $d < N^{0.292}$ , then the factorization of N = pq can be found.

#### The method

- $k(N+1-x) \equiv 1 \pmod{e}$ , where x = p + q.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

<ロ> <四> <四> <四> <三> <三> <三> <三> <三> <三> <三

RSA and Wiener	RSA setting
The new attack	Wiener's attack
Conclusion	Generalizations

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Boneh-Durfee's attack, 2000

If  $d < N^{0.292}$ , then the factorization of N = pq can be found.

#### The method

- $k(N+1-x) \equiv 1 \pmod{e}$ , where x = p + q.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

(日) (圖) (E) (E) (E)

RSA and Wiener	RSA setting
The new attack	Wiener's attack
Conclusion	Generalizations

## The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

## Boneh-Durfee's attack, 2000

If  $d < N^{0.292}$ , then the factorization of N = pq can be found.

## The method

- $k(N + 1 x) \equiv 1 \pmod{e}$ , where x = p + q.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

(日) (圖) (E) (E) (E)

RSA and Wiener **RSA** setting The new attack Conclusion

#### Wiener's attack Generalizations

## The variant RSA equation

$$ex-(p-1)(q-1)k=y.$$

If 
$$x < \frac{1}{3}N^{\frac{1}{4}}$$
 and  $|y| = O\left(N^{-\frac{3}{4}}ex\right)$  then the factorization of  $N = pq$  can be found.

• 
$$\frac{k}{x} \approx \frac{e}{N}$$
.

ヘロン ヘロン ヘビン ヘビン

RSA and Wiener **RSA** setting The new attack Conclusion

Wiener's attack Generalizations

## The variant RSA equation

$$ex-(p-1)(q-1)k=y.$$

## Blömer-May's attack, 2004

If 
$$x < \frac{1}{3}N^{\frac{1}{4}}$$
 and  $|y| = O\left(N^{-\frac{3}{4}}ex\right)$  then the factorization of  $N = pq$  can be found.

• 
$$\frac{k}{x} \approx \frac{e}{N}$$
.

ヘロン ヘロン ヘビン ヘビン

## The variant RSA equation

$$ex-(p-1)(q-1)k=y.$$

## Blömer-May's attack, 2004

If 
$$x < \frac{1}{3}N^{\frac{1}{4}}$$
 and  $|y| = O\left(N^{-\frac{3}{4}}ex\right)$  then the factorization of  $N = pq$  can be found.

## The method

- $\frac{k}{x} \approx \frac{e}{N}$ .
- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

< 白⇒ <

RSA and Wiener The new attack Conclusion The proof

## The new attack

## The variant RSA equation

$$eX - (p-u)(q-v)Y = 1.$$

u = v = 1 implies the RSA equation ed - (p - 1)(q - 1)k = 1.

#### The new attack

If 
$$1 \le Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}, \ |u| < N^{\frac{1}{4}}, \ v = \left[-\frac{qu}{p-u}\right]$$
, and all prime

factors of p - u or q - v are less than  $10^{50}$ , then the factorization of N = pq can be found.

## The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

RSA and Wiener The new attack Conclusion The proof

## The new attack

## The variant RSA equation

$$eX - (p - u)(q - v)Y = 1.$$

u = v = 1 implies the RSA equation ed - (p - 1)(q - 1)k = 1.

## The new attack

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

factors of p - u or q - v are less than  $10^{50}$ , then the factorization of N = pq can be found.

#### The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

RSA and Wiener The new attack Conclusion The proof

## The new attack

## The variant RSA equation

$$eX - (p - u)(q - v)Y = 1.$$

u = v = 1 implies the RSA equation ed - (p - 1)(q - 1)k = 1.

## The new attack

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

factors of p - u or q - v are less than  $10^{50}$ , then the factorization of N = pq can be found.

## The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

**RSA** and Wiener Overview The new attack Tools Conclusion The proof

## The Continued fraction alorithm

• e and N are coprime positive integers.

• 
$$\frac{e}{N} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$
.

- $\frac{e}{N} = [a_0, a_1, a_2, \cdots]$  where  $a_i$  are positive integers.  $\frac{r_i}{s_i} = [a_0, a_1, a_2, \cdots, a_i]$  are called the convergents.

If 
$$\left|\frac{e}{N} - \frac{x}{y}\right| < \frac{1}{2y^2}$$
, then  $\frac{x}{y}$  is one of the convergents of the continued fraction expansion of  $\frac{e}{N}$ .

**RSA** and Wiener Overview The new attack Tools Conclusion The proof

## The Continued fraction alorithm

• e and N are coprime positive integers.

• 
$$\frac{e}{N} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$
.

- $\frac{e}{N} = [a_0, a_1, a_2, \cdots]$  where  $a_i$  are positive integers.  $\frac{r_i}{s_i} = [a_0, a_1, a_2, \cdots, a_i]$  are called the convergents.

### The convergent theorem

If 
$$\left|\frac{e}{N} - \frac{x}{y}\right| < \frac{1}{2y^2}$$
, then  $\frac{x}{y}$  is one of the convergents of the continued fraction expansion of  $\frac{e}{N}$ .

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

## Coppermith's theorem

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

・ 同 ト ・ ヨ ト ・ ヨ ト ・ ヨ

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

## **Smooth numbers**

Let y be a positive constant. A positive number n is y-smooth if all prime factors of n are less than y.

### The Elliptic Curve Method (ECM)

- H.W. Lenstra, 1985, phase 1.
- Brent, Montgomery, 1986-87, phase 2.
- ECM is very efficient to factor *B*<sub>ecm</sub>-smooth integers where

*B*ecm = 10<sup>50</sup>

・ロト ・ 戸 ト ・ ヨ ト ・ ヨ ト

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

## **Smooth numbers**

Let y be a positive constant. A positive number n is y-smooth if all prime factors of n are less than y.

## The Elliptic Curve Method (ECM)

- H.W. Lenstra, 1985, phase 1.
- Brent, Montgomery, 1986-87, phase 2.
- ECM is very efficient to factor B<sub>ecm</sub>-smooth integers where

 $B_{\rm ecm} = 10^{50}$ 

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

## The counting function

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

## Theorem (Hildebrand)

$$\Psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

holds in the range  $x = y^u$  and  $y > \exp \{(\log \log x)^{5/3+\varepsilon}\}$  where  $\rho(u)$  be the Dickman-de Bruijn function.

#### Theorem (Friedlander and Granville)

 $\Psi(x + z, y) - \Psi(x, y) \ge c \frac{z}{x} \Psi(x, y)$ in the range  $x \ge z \ge x^{\frac{1}{2} + \delta}$ ,  $x \ge y \ge x^{1/\gamma}$ ,  $\delta > 0$ ,  $\gamma > 0$ ,  $c = c(\delta, \gamma) > 0$ .

・ロ・ ・ 四・ ・ ヨ・ ・ 日・ ・

э

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

## The counting function

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

## Theorem (Hildebrand)

$$\Psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

holds in the range  $x = y^u$  and  $y > \exp\{(\log \log x)^{5/3+\varepsilon}\}$  where  $\rho(u)$  be the Dickman-de Bruijn function.

#### Theorem (Friedlander and Granville)

 $\Psi(x + z, y) - \Psi(x, y) \ge c_x^{\mathbb{Z}} \Psi(x, y)$ in the range  $x \ge z \ge x^{\frac{1}{2} + \delta}$ ,  $x \ge y \ge x^{1/\gamma}$ ,  $\delta > 0$ ,  $\gamma > 0$ ,  $c = c(\delta, \gamma) > 0$ .

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

## The counting function

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

## **Theorem (Hildebrand)**

$$\Psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

holds in the range  $x = y^u$  and  $y > \exp\{(\log \log x)^{5/3+\epsilon}\}$  where  $\rho(u)$  be the Dickman-de Bruijn function.

## Theorem (Friedlander and Granville)

$$\begin{split} \Psi(x+z,y)-\Psi(x,y) &\geq c_x^{\underline{z}}\Psi(x,y)\\ \text{in the range } x &\geq z \geq x^{\frac{1}{2}+\delta}, \, x \geq y \geq x^{1/\gamma}, \, \delta > 0, \, \gamma > 0,\\ c &= c(\delta,\gamma) > 0. \end{split}$$

• □ ▶ • □ ▶ • □ ▶ • □ ▶

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

## The proof

## Setting

• 
$$eX - (p - u)(q - v)Y = 1.$$

• 
$$1 \le Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$$
.

• 
$$|\boldsymbol{u}| < \boldsymbol{N}^{\frac{1}{4}}, \quad \boldsymbol{v} = \left[-\frac{q\boldsymbol{u}}{\boldsymbol{p}-\boldsymbol{u}}\right].$$

• Without loss of generality, suppose p - u is  $B_{ecm}$ -smooth.

크

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

• Write eX - NY = 1 - (N - (p - u)(q - v))Y. Then  $\frac{e}{N} \approx \frac{Y}{X}$ .

• Compute X and Y via the continued fraction expansion of  $\frac{e}{N}$ .

• Compute 
$$(p-u)(q-v) = \frac{eX-1}{V}$$

• Apply **ECM** to write  $\frac{eX - 1}{Y} = M_1 M_2$  where  $M_1$  is  $B_{ecm}$ -smooth, i.e.

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i}, \qquad p_i \leq B_{ ext{ecm}}, \qquad a_i \geq 1.$$

• Im • • m • • m

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

• Write eX - NY = 1 - (N - (p - u)(q - v))Y. Then  $\frac{e}{N} \approx \frac{Y}{X}$ .

• Compute X and Y via the continued fraction expansion of  $\frac{e}{N}$ .

• Compute 
$$(p-u)(q-v) = \frac{eX-1}{V}$$
.

• Apply **ECM** to write  $\frac{eX - 1}{Y} = M_1 M_2$  where  $M_1$  is  $B_{\text{ecm}}$ -smooth, i.e.

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i}, \qquad p_i \leq B_{ ext{ecm}}, \qquad a_i \geq 1.$$

(本部) (本語) (本語) (語)

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

• Write eX - NY = 1 - (N - (p - u)(q - v))Y. Then  $\frac{e}{N} \approx \frac{Y}{X}$ .

- Compute X and Y via the continued fraction expansion of  $\frac{e}{N}$ .
- Compute  $(p u)(q v) = \frac{eX 1}{v}$ .
- Apply **ECM** to write  $\frac{eX 1}{Y} = M_1 M_2$  where  $M_1$  is  $B_{ecm}$ -smooth, i.e.

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i}, \qquad p_i \leq B_{ ext{ecm}}, \qquad a_i \geq 1.$$

◆□▶ ◆□▶ ◆ □ ▶ ◆ □ ▶ ◆ □ ▶

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

- Write eX NY = 1 (N (p u)(q v))Y. Then  $\frac{e}{N} \approx \frac{Y}{X}$ .
- Compute X and Y via the continued fraction expansion of  $\frac{e}{N}$ .
- Compute  $(p u)(q v) = \frac{eX 1}{v}$ .
- Apply **ECM** to write  $\frac{eX 1}{Y} = M_1 M_2$  where  $M_1$  is  $B_{ecm}$ -smooth, i.e.

$$M_1 = \prod_{i=1}^{\omega(M_1)} p_i^{a_i}, \qquad p_i \leq B_{ ext{ecm}}, \qquad a_i \geq 1.$$

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

• Since p - u is  $B_{ecm}$ -smooth, then

$$\boldsymbol{\rho}-\boldsymbol{u}=\prod_{i=1}^{\omega(M_1)}\boldsymbol{\rho}_i^{\boldsymbol{X}_i},\qquad \boldsymbol{X}_i\geq \mathbf{0}.$$

• Since  $N^{\frac{1}{2}} , then$ 

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

To solve this

The Lenstra-Lenstra-Lovasz LLL algorithm.

- The Ferguson PSLQ algorithm.
- Exhaustive search since  $\omega(M_1) \sim \log \log M_1$ .

・ロト ・日 ・ ・ 日 ・ ・ 日 ・

э

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

• Since p - u is  $B_{ecm}$ -smooth, then

$$\boldsymbol{p}-\boldsymbol{u}=\prod_{i=1}^{\omega(M_1)}\boldsymbol{p}_i^{\boldsymbol{X}_i},\qquad \boldsymbol{X}_i\geq 0.$$

• Since  $N^{\frac{1}{2}} , then$ 

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

To solve this

The Lenstra-Lenstra-Lovasz LLL algorithm.

- The Ferguson PSLQ algorithm.
- Exhaustive search since ω(M<sub>1</sub>) ~ log log M<sub>1</sub>.

< 日 > < 回 > < 回 > < 回 > < 回 > <

э

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

• Since p - u is  $B_{ecm}$ -smooth, then

$$\boldsymbol{p}-\boldsymbol{u}=\prod_{i=1}^{\omega(M_1)}\boldsymbol{p}_i^{\boldsymbol{x}_i}, \qquad \boldsymbol{x}_i\geq 0.$$

• Since  $N^{\frac{1}{2}} , then$ 

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

To solve this

- The Lenstra-Lenstra-Lovasz LLL algorithm.
- The Ferguson PSLQ algorithm.
- Exhaustive search since  $\omega(M_1) \sim \log \log M_1$ .

- 同下 - ヨト - ヨト

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

Finally, apply Coppersmith's algorithm to find p using

$$\boldsymbol{p}-\boldsymbol{u}=\prod_{i=1}^{\omega(M_1)}\boldsymbol{p}_i^{x_i}, \qquad x_i\geq 0.$$

#### Cardinality

- eX (p u)(q v)Y = 1.
- $1 \leq Y < X < 2^{-\frac{1}{4}}N^{\frac{1}{4}}$ .
- $|\boldsymbol{u}| < \boldsymbol{N}^{\frac{1}{4}}, \quad \boldsymbol{v} = \left[-\frac{q\boldsymbol{u}}{p-\boldsymbol{u}}\right]$
- Without loss of generality, suppose p u is  $B_{ecm}$ -smooth.
- Then using Hildebrand and Friedlander and Granville results on smooth numbers, we find that there are at least N<sup>1/2-ε</sup> such keys.

・ロト ・ 戸 ト ・ ヨ ト ・ ヨ ト

RSA and Wiener	Overview
The new attack	Tools
Conclusion	The proof

Finally, apply Coppersmith's algorithm to find p using

$$\boldsymbol{p}-\boldsymbol{u}=\prod_{i=1}^{\omega(M_1)}\boldsymbol{p}_i^{x_i}, \qquad x_i\geq 0.$$

## Cardinality

- eX (p u)(q v)Y = 1.
- $1 \le Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}.$
- $|\boldsymbol{u}| < \boldsymbol{N}^{\frac{1}{4}}, \quad \boldsymbol{v} = \left[-\frac{q\boldsymbol{u}}{p-\boldsymbol{u}}\right].$
- Without loss of generality, suppose p u is Becm-smooth.
- Then using Hildebrand and Friedlander and Granville results on smooth numbers, we find that there are at least N<sup>1/2-ε</sup> such keys.

(日)

Comparison Thanks

## Comparison

## Wiener's attack

- The equation
  - ed (p-1)(q-1)k = 1.
- The method : The continued fraction algorithm
- The size of such keys :

## The new attack

• The equation :

eX - (p - u)(q - v)Y = 1.

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

Comparison Thanks

## Comparison

## Wiener's attack

The equation :

ed - (p-1)(q-1)k = 1.

- The method : The continued fraction algorithm
- The size of such keys :

The new attack

The equation :

eX - (p - u)(q - v)Y = 1.

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

Comparison Thanks

## Comparison

## Wiener's attack

• The equation :

ed - (p-1)(q-1)k = 1.

- The method : The continued fraction algorithm
- The size of such keys :

The new attack

• The equation :

eX - (p - u)(q - v)Y = 1.

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.

The size of such keys :

Comparison Thanks

## Comparison

## Wiener's attack

• The equation :

ed - (p-1)(q-1)k = 1.

 The method : The continued fraction algorithm

The size of such keys :

## The new attack

• The equation :

eX - (p-u)(q-v)Y = 1.

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.

The size of such keys :

Comparison Thanks

## Comparison

## Wiener's attack

The equation :

ed - (p-1)(q-1)k = 1.

 The method : The continued fraction algorithm

The size of such keys :

## The new attack

• The equation :

eX - (p - u)(q - v)Y = 1.

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.

Comparison Thanks

## Comparison

## Wiener's attack

The equation :

ed - (p-1)(q-1)k = 1.

- The method : The continued fraction algorithm
- The size of such keys :

 $\mathcal{O}\left(\boldsymbol{N}^{\frac{1}{4}}\right).$ 

## The new attack

• The equation :

eX - (p - u)(q - v)Y = 1.

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.

Comparison Thanks

## Comparison

## Wiener's attack

The equation :

ed - (p-1)(q-1)k = 1.

- The method : The continued fraction algorithm
- The size of such keys :

 $\mathcal{O}\left(\boldsymbol{N}^{\frac{1}{4}}\right).$ 

## The new attack

• The equation :

eX - (p - u)(q - v)Y = 1.

- The method :
  - The continued fraction algorithm.
  - Lenstra'ECM .
  - The Lenstra-Lenstra-Lovasz LLL algorithm. or the Ferguson PSLQ algorithm.
  - Coppersmith's method.
- The size of such keys :

 $\mathcal{O}\left(\boldsymbol{N}^{\frac{1}{2}-\varepsilon}\right).$ 

Comparisor Thanks

## Thank you for your attention

Merci



Abderrahmane NITAJ Another Generalization of Wiener's Attack on RSA

3