2013 13th International Conference on Computational Science and Its Applications

Attacks on low private exponent RSA: an experimental study

Thuc D. Nguyen*, Than Duc Nguyen*, Long D. Tran†
*Faculty of Information Technology
University of Science, Ho Chi Minh City, Vietnam
ndthuc@fit.hcmus.edu.vn
0912441@student.hcmus.edu.vn
†Faculty of Mathematics
University of Sciences, Hue, Vietnam
tdlong@husc.edu.vn

***Abstract*—RSA cryptosystem is the most popular public key cryptosystem which provides both secrecy and digital signatures. Due to RSA's popularity, many attacks on it have been developed. In this paper, we consider experimentally attacks on low private exponent RSA and find that: (i) lattice attack using Gauss lattice reduction algorithm is more effective than Wiener attack, and (ii) it is not always to recover decryption exponent even if its bit-length is less than one-quarter bit-length of the modulus. The results also raise an open question on the conditions to recover the RSA private key from public key.**

***Keywords*-RSA cryptanalysis; Wiener attack; lattice attack**

I. Introduction

RSA cryptosystem, named after R. Rivest, A. Shamir, and L. Adleman, who invented RSA [15] in 1978, is the public-key cryptosystem which is used the most widely. It can be used to provide both secrecy and digital signatures. Additionally, its security is based on the intractability of the integer factorization problem.

RSA cryptosystem is described by the modulus N, which is a product of two large primes, p and q. The integers e and d are called the encryption exponent and the decryption exponent respectively. The exponents e and d are interrelated by the relation $ed \equiv 1 \pmod{\varphi(N)}$, where $\varphi(N) = (p-1)(q-1)$ is called the Euler's totient function. In a typical RSA cryptosystem, p and q have the same bit-length and $e < N$. Encryption and decryption algorithms are defined by $\mathrm{C} = \mathrm{M}^e \pmod{N}$, $\mathrm{M} = \mathrm{C}^d \pmod{N}$ respectively for each plain text $\mathrm{M} \in \mathbb{Z}_N$.

In the encryption/decryption process, RSA cryptosystem must do numerous power operations, thus the system takes a relatively great amount of time to process. Therefore, we want to reduce the decryption time or signature-generation time, as well as signature-verification time [10], [2]. One of the ways to reduce the time processing is to use the decryption exponent with small d. Unfortunately, since 1990, Wiener [14] showed that if $d < N^{1/4}$, we can recover d by using the pair of the modulus N and the encryption exponent e. Then, in 1999, Boneh and Durfee[9], taking the advantages of lattice reduction techniques, claimed that instance of RSA was not secure enough with $d < N^{0.292}$. Lattice attacks on RSA was firstly introduced by Coppersmith at Eurocrypt'96 [11] and then has been developed by many authors [6], [7]. Gaussian's lattice reductions or LLL algorithms can be used to recover the decryption exponent d in the case of small d. High dimension lattice attacks are based on LLL algorithm while low dimension lattice attacks are based on Gaussian lattice reduction algorithm.

In this paper, we consider experimentally two attacks on RSA in the case of $d < N^{1/4}$: the low dimension lattice attack using Gaussian algorithm and Wiener attack based on continued fraction expansion of $\frac{e}{N}$ with the purpose of determining which one is more effective. In addition, we want to point out the values of $\alpha \in (0, 1)$ such that in the case $d < \alpha N^{1/4}$, we can recover d from the pair (e, N) by using lattice attack.

II. Lattice attack and Wiener Attack

A. Lattice attacks

In [1], Phong Q. Nguyen presented a method to recover the private exponent d based on the solution of the shortest problem finding for two dimension lattice. Although he showed that by using two-dimension, $d < N^{1/4}$, this is only a heuristic. Suppose that p, q are two primes having the same bit-length. Since $ed \equiv 1 \pmod{\varphi(N)}$, there is a $k \in \mathbb{Z}$ such that $ed = 1 + k\varphi(N)$. Now, we consider 2-rank lattice L spanned by two vectors $\mathbf{u} = (e, \sqrt{N})$ and $\mathbf{v} = (N, 0)$, then L contains vector $\mathbf{t} = d \times \mathbf{u} - k \times \mathbf{v} = (ed - kN, d\sqrt{N})$. The norm of $\|\mathbf{t}\| = \sqrt{(ed - kN)^2 + (d\sqrt{N})^2} \approx d\sqrt{N}$, while $\sqrt{\mathrm{vol}(L)} = N^{3/4}$. Vector $\mathbf{t}$ may be the shortest vector if $d\sqrt{N} < \sqrt{\mathrm{vol}(L)} = N^{3/4}$. It means that $d < N^{1/4}$.

For finding $\mathbf{t}$, we apply Gaussian's lattice reduction algorithm [13] (Algorithm 1) to two vectors $\mathbf{u}$ and $\mathbf{v}$. The algorithm terminates and yields vectors $\mathbf{u}^*$ and $\mathbf{v}^*$, where $\|\mathbf{u}^*\| < \|\mathbf{v}^*\|$. It is noted that, vector $\mathbf{u}^*$ is the smallest non zero vector of lattice L. Gaussian's lattice reduction algorithm will terminate in at most $\left\lceil \log_{1+\sqrt{2}} \frac{\|\mathbf{u}\|}{\lambda_2} \right\rceil + 3$ iterations [12], where λ_2 is the second minima of L. If $\mathbf{u}^* = \pm\mathbf{t}$, our prediction is probably correct, and the value

978-0-7695-5045-9/13 $26.00 © 2013 IEEE
DOI 10.1109/ICCSA.2013.32

of the decryption exponent d can be computed, based on the vector $\mathbf{u}$.

Algorithm 1 Gaussian's lattice reduction algorithm $(\mathbf{u}, \mathbf{v})$

```
Input: A basis $[\mathbf{u}, \mathbf{v}]$
Output: A Gaussian reduced basis $[\mathbf{u}^*, \mathbf{v}^*]$
  repeat
    if $\|\mathbf{u}\| > \|\mathbf{v}\|$ then
      swap $\mathbf{u}$ and $\mathbf{v}$
    end if
    $\mu \leftarrow \langle \mathbf{u}, \mathbf{v} \rangle / \|\mathbf{u}\|^2$
    $\mathbf{v} \leftarrow \mathbf{v} - \lceil \mu \rfloor \mathbf{u}$    (where $\lceil x \rfloor = \lfloor x + \frac{1}{2} \rfloor$)
  until $\|\mathbf{u}\| < \|\mathbf{v}\|$
```

B. Wiener attack

In [5], [8], [3], they showed that if $p < q < 2p$, $e < pq$ and $d < N^{1/4}$, we can recover the decryption exponent d from the public pair (e, N) by using continued fraction expansion $\frac{e}{N}$.

Since $ed \equiv 1 \pmod{\varphi(N)}$, there is a $k \in \mathbb{Z}$ such that $ed = 1 + k\varphi(N)$. Hence, we have

$$\left| \frac{e}{\varphi(N)} - \frac{k}{d} \right| = \frac{1}{d\varphi(N)}$$

.

Accordingly we have $\frac{k}{d} \approx \frac{e}{\varphi(N)}$. Moreover, the modulus N is an approximation of $\varphi(N)$. Since then, we have $\frac{k}{d} \approx \frac{e}{n}$.

Because of $\varphi(N) = N - (p+q-1)$ and $p+q-1 < 3\sqrt{N}$, we have $|N - \varphi(N)| < 3\sqrt{N}$ and

$$\left| \frac{e}{N} - \frac{k}{d} \right| \leq \frac{3k}{d\sqrt{N}} < \frac{1}{2d^2}$$

So $\frac{k}{d}$ is a convergents of the continued fraction expansion of $\frac{e}{N}$

Let us define a continued fraction as following

$$\langle q_0, q_1, \cdots, q_m \rangle = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_m}}}} = f$$

The continued fraction representation of a positive rational number is calculated by using the Euclidean algorithm and is showed in algorithm 2.

To reconstruct fraction f from its continued fraction expansion, we use algorithm 3 with n_i and d_i being a sequence of numerators and denominates and $\gcd(n_i, d_i) = 1$ for $i = 1, 2, 3, \cdots, m$.

Wiener attack was also represented in [4]. Here, we reintroduce in the form of pseudo-code (Algorithm 4).

Algorithm 2 Fraction to continued fraction

```
Input: Numerator $a$ and denominator $b$
Output: Continued fraction $\langle q_0, q_1, \cdots, q_m \rangle$
  $q_0 \leftarrow \lfloor \frac{a}{b} \rfloor$
  $r_0 \leftarrow \frac{a}{b} - q_0$
  repeat
    $i \leftarrow i + 1$
    $q_i \leftarrow \left\lfloor \frac{1}{r_{i-1}} \right\rfloor$
    $r_i \leftarrow \frac{1}{r_{i-1}} - q_i$
  until $r_i = 0$
  $m \leftarrow i$
```

Algorithm 3 Continued fraction to fraction

```
Input: Continued fraction $\langle q_0, q_1, \cdots, q_m \rangle$
Output: Fraction $\frac{n_m}{d_m}$
  $n_0 = q_0$
  $d_0 = 1$
  $n_1 = q_0 q_1 + 1$
  $d_1 = q_1$
  for $i = 2 \rightarrow m$ do
    $n_i \leftarrow q_i n_{i-1} + n_{i-2}$
    $d_i \leftarrow q_i d_{i-1} + d_{i-2}$
  end for
```

III. Experiments

As [14], [8] predicted, if p and q are two large primes, which satisfy $p < q < 2p$, the decryption exponent d can be recovered from the public pair (e, N) when $d < N^{1/4}$. However, this is only a prediction. It means that there are many cases in which $d < N^{1/4}$ and d cannot be recovered from the public pair (e, N) by both of lattice attack using Gaussian's lattice reduction algorithm and Wiener attack using continued fraction expansion $\frac{e}{N}$.

In this section, we will experimentally demonstrate the following two statements:

1) Lattice attack is more effective than Wiener attack in recovering the private exponent d.
2) There is a coefficient $\alpha < 1$ such that for all $d < \alpha N^{1/4}$, the decryption exponent d is always recovered from the public pair (N, e).

The experiments are executed with the system of Intel processors of 2.2 GHz Core 2 Duo with 2 GB Memory. Gaussian's lattice reduction algorithm and continued fraction expansion $\frac{e}{N}$ were implemented by using Shoup's NTL [16]. All the experiments were executed with the data chosen randomly.

A. Comparative Lattice attack and Wiener attack

Experimental method as follows: Let i be an iteration number and execute following algorithm i times.

Algorithm 4 Wiener attack algorithm

```
Input: Public key $(e, N)$
Output: Secret key $d$
  $\langle q'_0, q'_1, \cdots, q'_m \rangle \leftarrow \frac{e}{N}$ (using algorithm 2)
  for $i = 0 \rightarrow m$ do
    $\frac{n_i}{d_i} \leftarrow \langle q'_0, q'_1, \cdots, q'_i \rangle$ (using algorithm 3)
    $\frac{k}{dg} \leftarrow \begin{cases} \langle q'_0, q'_1, \cdots, q'_i + 1 \rangle & \text{if } i \text{ is even} \\ \langle q'_0, q'_1, \cdots, q'_i \rangle & \text{if } i \text{ is odd} \end{cases}$
    $\varphi(N) \leftarrow \left\lceil \frac{edg}{k} \right\rfloor$
    $g \leftarrow edg \bmod k$
    if $\varphi(N) = 0$ then
      increment $i$ and restart the loop
    end if
    $\alpha \leftarrow \frac{pq-(p-1)(q-1)+1}{2}$
    $\beta \leftarrow \alpha^2 - pq$
    if $\beta$ is not a square number then
      increment $i$ and restart the loop
    end if
    $d \leftarrow dg/g$
  end for
```

- For each iteration step, generate a pair of different prime (p, q), which have the same 32-bit of length satisfying $p < q < 2p$.
- With each pair of generated primes (p, q), choose all decryption exponent d in the range $\left(1, \lfloor N^{1/4} \rfloor\right)$, and compute the corresponding encryption exponent e satisfying $ed \equiv 1 \pmod{\varphi(N)}$. Pair (e, N) is the public key and d is private key.

After using the public key (e, N) generated as the description above and two algorithms introduced in section II to compute a private key d', we check if d' is exactly the corresponding private key d, which is generated at the same time with the public key (e, N)?

In this paper, we run both algorithms to compute d', with the value of iteration number i being 500. After each time running, we count the number of time that $d' = d$ (denoting YES), and the number of time that $d' \neq d$ (denoting NO), executing time in milliseconds (denoting TIME) and the percentage of $d' = d$ (YES) over all (denoting Percent of YES). Table I shows the comparison results between lattice and Wiener attack. It can be seen clearly that lattice attack is more effective than Wiener attack, and the running time of lattice attack is also shorter than the one of Wiener attack.

In this experiment, an interesting phenomenon of lattice attack is the case of $d < \alpha N^{1/4}$ with $\alpha = \frac{1}{\sqrt{4+2\sqrt{2}}} \approx \frac{3}{8}$, the private key d seems to be always recovered properly. The question is whether α is exactly $\frac{3}{8}$ or α can be greater (as we affirm in 2 of section III). The next section will answer this question.

	Lattice attack	Wiener attack
YES	6030474	905792
NO	2174281	11902990
TIME (ms)	3048521	14518535
Percent of YES (%)	73.49	7.07

Table I
THE COMPARISON BETWEEN LATTICE ATTACK AND WIENER ATTACK

B. Empirical coefficient of α

When $\alpha = \frac{1}{\sqrt{4+2\sqrt{2}}} \approx \frac{3}{8}$, for each $d < \alpha N^{1/4}$ the vector $\mathbf{t}$ is always the shortest vector by using Gaussian's lattice reduction algorithm.

Indeed, by the previous experiment for lattice attack with the iteration number $i = 500$, we always recover the corresponding private key d when $d < \alpha N^{1/4}$ if $\alpha = \frac{3}{8}$. In table II, we can see that in the range $1 < d < \lfloor \frac{3}{8} N^{1/4} \rfloor$, where $\lfloor x \rfloor$ is an integer satisfying $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, the private key d is always recovered, or $d' \neq d$ (NO) is always 0.

Interval of d	YES	NO
$\left(1, \lfloor \frac{3}{8} N^{1/4} \rfloor\right]$	3076387	0

Table II
RESULT OF LATTICE ATTACK WITH $d < \alpha N^{1/4}$ WHERE $\alpha = \frac{3}{8}$

Can we enlarge the value of α? And why? To answer these questions, we tried to do experiments dividing the interval $\frac{3}{8} < d < N^{1/4}$ into sub-intervals. Firstly, $\frac{3}{8} < d < N^{1/4}$ is divided into two sub-intervals: $\lfloor \frac{3}{8} N^{1/4} \rfloor < d \leq \lfloor \frac{1}{2} N^{1/4} \rfloor$ and $\lfloor \frac{1}{2} N^{1/4} \rfloor < d \leq \lfloor N^{1/4} \rfloor$. Let $X = \left(\lfloor \frac{3}{8} N^{1/4} \rfloor, \lfloor \frac{1}{2} N^{1/4} \rfloor\right]$ and $Y = \left(\lfloor \frac{1}{2} N^{1/4} \rfloor, \lfloor N^{1/4} \rfloor\right]$. In the experiment process, we see that the number $d' = d$ (YES) of the interval X is more than the one of the interval Y, and number $d' \neq d$ (NO) of the interval X is less than the one of the interval Y. This suggests that the probability for recovering d in the interval X will be higher than in the interval Y. Therefore, we continue to divide the interval X into four sub-intervals $X_1 = \left(\lfloor \frac{3}{8} N^{1/4} \rfloor, \lfloor \frac{13}{32} N^{1/4} \rfloor\right]$, $X_2 = \left(\lfloor \frac{13}{32} N^{1/4} \rfloor, \lfloor \frac{7}{16} N^{1/4} \rfloor\right]$, $X_3 = \left(\lfloor \frac{7}{16} N^{1/4} \rfloor, \lfloor \frac{15}{32} N^{1/4} \rfloor\right]$ and $X_4 = \left(\lfloor \frac{15}{32} N^{1/4} \rfloor, \lfloor \frac{1}{2} N^{1/4} \rfloor\right]$. Running the attack, we see that in the sub-interval $X_1 \cup X_2$, the private key d is always recovered, but starting from the sub-interval $X_3 \cup X_4$, the private key d is not always recovered, In other words, this prediction is only a heuristic, reflected in the number of $d' \neq d$ (NO) being greater than 0 (see table II).

Similarly, with the interval Y, we also divide into sub-intervals $Y_1 = \left(\lfloor \frac{1}{2} N^{1/4} \rfloor, \lfloor \frac{5}{8} N^{1/4} \rfloor\right]$,

$Y_2 = \left(\lfloor\frac{5}{8}N^{1/4}\rfloor, \lfloor\frac{3}{4}N^{1/4}\rfloor\right]$, $Y_3 = \left(\lfloor\frac{3}{4}N^{1/4}\rfloor, \lfloor\frac{13}{16}N^{1/4}\rfloor\right]$, $Y_4 = \left(\lfloor\frac{13}{16}N^{1/4}\rfloor, \lfloor\frac{7}{8}N^{1/4}\rfloor\right]$ and $Y_5 = \left(\lfloor\frac{7}{8}N^{1/4}\rfloor, \lfloor N^{1/4}\rfloor\right]$.

The experiment results are showed in the table IV. Combining table III with table IV, we see that with $\frac{7}{16}N^{1/4} < d < N^{1/4}$, lattice attack cannot recover the private key d, or in other words, it is only a heuristic. However, the private key d can still exactly be recovered in many cases.

Interval of d	YES	NO
$(\lfloor\frac{3}{8}N^{1/4}\rfloor, \lfloor\frac{13}{32}N^{1/4}\rfloor]$	256431	0
$(\lfloor\frac{13}{32}N^{1/4}\rfloor, \lfloor\frac{7}{16}N^{1/4}\rfloor]$	256398	0
$(\lfloor\frac{7}{16}N^{1/4}\rfloor, \lfloor\frac{15}{32}N^{1/4}\rfloor]$	253600	2800
$(\lfloor\frac{15}{32}N^{1/4}\rfloor, \lfloor\frac{1}{2}N^{1/4}\rfloor]$	237644	18804

Table III
RESULT OF LATTICE ATTACK WITH $\alpha N^{1/4} < d < \beta N^{1/4}$ WHERE $\alpha = \frac{3}{8}, \beta = \frac{1}{2}$

Interval of d	YES	NO
$(\lfloor\frac{1}{2}N^{1/4}\rfloor, \lfloor\frac{5}{8}N^{1/4}\rfloor]$	779828	245758
$(\lfloor\frac{5}{8}N^{1/4}\rfloor, \lfloor\frac{3}{4}N^{1/4}\rfloor]$	563897	461778
$(\lfloor\frac{3}{4}N^{1/4}\rfloor, \lfloor\frac{13}{16}N^{1/4}\rfloor]$	215882	296901
$(\lfloor\frac{13}{16}N^{1/4}\rfloor, \lfloor\frac{7}{8}N^{1/4}\rfloor]$	174568	338259
$(\lfloor\frac{7}{8}N^{1/4}\rfloor, \lfloor N^{1/4}\rfloor]$	215824	809843

Table IV
RESULT OF LATTICE ATTACK WITH $\alpha N^{1/4} < d < N^{1/4}$ WHERE $\alpha = \frac{1}{2}$

IV. CONCLUSIONS

In this paper, by doing experiments, we can conclude that the lattice attack is more effective than the Wiener attack when being used to recover the private key d from the pair of public key (e, N).

During the experiment, it is also showed that there is a coefficient $\alpha < 1$ such that $d < \alpha N^{1/4}$ so that we can always recover the private key d from the pair of public key (e, N). To be specific, we indicate that with $\alpha = \frac{1}{\sqrt{4+2\sqrt{2}}} \approx \frac{3}{8}$, d is always exactly recovered from $\mathbf{t} = \left(ed - kN, d\sqrt{N}\right)$ by using Gaussian's lattice reduction algorithm. Basing on these results, we want to determine and prove that coefficient α is correct in theory. Here, when we enlarge the interval $d < \frac{7}{16}N^{1/4}$, the private key d is also recovered. In this particular case of the interval $\frac{7}{16}N^{1/4} < d < N^{1/4}$, recovering the private key d is not always possible.

An open question to end this paper: what are the needed and sufficient conditions to recover the private key d by lattice attack using Gaussian's lattice reduction algorithm?

REFERENCES

[1] Nguyen, Phong Q. *Public-key cryptanalysis.* Recent Trends in Cryptography. Contemporary Mathematics 477 (2008).

[2] Sun, Hung-Min, and Cheng-Ta Yang. *RSA with balanced short exponents and its application to entity authentication.* Public Key Cryptography-PKC 2005 (2005): 199-215.

[3] Dujella, Andrej. *Continued fractions and RSA with small secret exponent.* arXiv preprint cs/0402052 (2004).

[4] Render, Elaine L. *A Survey of Attacks on the RSA Cryptosystem, with Implementations in Java.* (2004).

[5] Smart, Nigel Paul. *Cryptography: an introduction*. New York: McGraw-Hill, 2003.

[6] Hinek, M. Jason, Mo King Low, and Edlyn Teske. *On some attacks on multi-prime RSA.* In Selected Areas in Cryptography, pp. 385-404. Springer Berlin Heidelberg, 2003.

[7] Hinek, M. Jason. *Low public exponent partial key and low private exponent attacks on multi-prime RSA*. PhD diss., University of Waterloo, 2002.

[8] Boneh, Dan, Ron Rivest, Adi Shamir, and Len Adleman. *Twenty years of attacks on the RSA cryptosystem.* Notices of the AMS 46, no. 2 (1999): 203-213.

[9] Boneh, Dan, and Glenn Durfee. *Cryptanalysis of RSA with private key d less than N 0.292.* In Advances in Cryptology-EUROCRYPT'99, pp. 1-11. Springer Berlin/Heidelberg, 1999.

[10] Sun, Hung-Min, Wu-Chuan Yang, and Chi-Sung Laih. *On the design of RSA with short secret exponent.* Advances in Cryptology-ASIACRYPT'99 (1999): 150-164.

[11] Coppersmith, Don. *Finding a small root of a bivariate integer equation; factoring with high bits known.* In Advances in Cryptology-EUROCRYPT96, pp. 178-189. Springer Berlin/Heidelberg, 1996.

[12] Schnorr, C. P. *Gittertheorie und Kryptographie.* Ausarbreitung, Johann-Wolfgang-Goethe-Universit at, Frankfurt/Main (1994).

[13] Valle, Brigitte. *Gauss' algorithm revisited.* Journal of Algorithms 12, no. 4 (1991): 556-572.

[14] Wiener, Michael J. *Cryptanalysis of short RSA secret exponents.* Information Theory, IEEE Transactions on 36, no. 3 (1990): 553-558.

[15] Rivest, Ronald L., Adi Shamir, and Len Adleman. *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM 21, no. 2 (1978): 120-126.

[16] Shoup, V. *Number Theory C++ Library (NTL) version 3.6.* Can be obtained at http://www. shoup. net/ntl.