Malaysian Journal of Science Special Issue (1) 2019: 67-73

ICMSS2018
3rd International Conference of Mathematical Sciences and Statistics
6th - 8th February 2018

ANOTHER PROOF OF WIENER'S SHORT SECRET EXPONENT

Muhammad Asyraf Asbullah[1*], Muhammad Rezal Kamel Ariffin[2]

[1,2]Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia.
[2]Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia.
*Corresponding author: ma_asyraf@upm.edu.my
Received: 29th Oct 2018 Revised: 29th Oct 2018 Accepted: 19th December 2018
DOI: https://doi.org/10.22452/mjs.sp2019no1.6

ABSTRACT Wiener's short secret exponent attack is a well-known crypt-analytical result upon the RSA cryptosystem using a Diophantine's method called continued fractions. We recall that Wiener's attack works efficiently on RSA with the condition that the secret exponent $d < \frac{1}{3}N^{\frac{1}{4}}$. Later, the upper bound was improved satisfying $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. In this work, we present another proof to Wiener's short secret exponent satisfying $d < \frac{1}{2}N^{\frac{1}{4}}$. We remark that our result is slightly better than the previously mentioned attacks.

Keywords: RSA cryptosystem, continued fractions, secret exponent, cryptanalysis, Wiener's theorem.

INTRODUCTION

From the beginning of time until 1970's, the technology for practicing secret communication, which is widely known as encryption and decryption, was always done in a symmetrical manner. In early 1978, the RSA cryptosystem (Rivest, R., Shamir, A. and Adleman, L, 1978) that was introduced (abbreviated accordingly to its creator; Rivest, Shamir, and Adleman) became a phenomenon in the world of secrecy of which was regarded as the first practical realization of the asymmetric cryptosystem as opposed to symmetric cryptosystem.

The core design of the RSA cryptosystem is based on the number-theoretic object called the integer factorization problem. The intractability to solve the said problems with current computational power is the source of its security (i.e. particularly in factoring of the form $N = pq$). Additionally, another source of security of RSA cryptosystem lies on the difficulty to solve the RSA key equation of the form $ed \equiv 1(\mathrm{mod}\phi(N))$ where $\phi(N) = (p-1)(q-1)$. Solving the RSA key equation meaning that the objective is to recover the unknown value of d, given only e and N. This will be the focus in this work.

For practicality purpose, the private exponent d of RSA decryption is tended to be made small, thus the RSA cryptosystem will have tremendous decryption speed. However, if d is upper bounded by $\frac{1}{3}N^{1/4}$,

then Wiener (Wiener M., 1990) observe that such secret exponent d can be easily solved in polynomial time. The observation is made based on the key equation $ed - \phi(N)k = 1$ and can be solved efficiently via continued fraction method.

The main idea behind Wiener's attack to solve for the parameter d that satisfy the inequality $\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$. In fact, a classical Legendre's theorem of continued fraction expansion shows that the value of $\frac{k}{d}$ could be efficiently obtained from the list of convergent of $\frac{e}{N}$. Thus, as the security of the RSA cryptosystem matters, it was proposed that such d must be generated by choosing an integer larger than $\frac{1}{3}N^{1/4}$ to resist Wiener's attack.

Afterward, (de Weger, B., 2002) demonstrated that the Legendre's theorem is satisfied upon $\left|\frac{e}{N-2N^{1/2}+1} - \frac{k}{d}\right|$. As a result, any secret integer d less than $\frac{N^{3/4}}{|p-q|}$ in no longer secure for RSA cryptosystem since $\frac{k}{d}$ effciently obtained from a convergent of the continued fraction $\frac{e}{N-2N^{1/2}+1}$. Note that (de Weger, B., 2002) considered the situation when p and q are too close (i.e.the difference of two primes, $|p-q|$ is small). Alternatively, even though p and q are not close, (Maitra, S. and Sarkar, S., 2008) considered the case of the primes p and $2q$ are too close. Furthermore, (Maitra, S. and Sarkar, S., 2008) showed that by replacing the $N - 2N^{1/2} + 1$ from the result in (de Weger, B., 2002) with $N - \frac{3}{\sqrt{2}}\sqrt{N} + 1$, then $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N-\frac{3}{\sqrt{2}}\sqrt{N}+1}$.

Motivated from the earlier work of (de Weger, B., 2002) and (Maitra, S. and Sarkar, S., 2008) of utilizing a good approximation of $\phi(N)$ methodology, (Asbullah, M. A. and Ariffin, M. R. K., 2015) extended such cryptanalysis technique to the RSA modulus of type $N = p^2q$. A recent survey of RSA-like cryptosystems that implement such modulus can be found in (Asbullah, M. A. and Ariffin, M. R. K., 2014; Asbullah, M. A. and Ariffin, M. R. K., 2016c). The continued fraction technique is also widely used for algebraic cryptanalysis such as in (Asbullah, M. A. and Ariffin, M. R. K., 2016a) and (Asbullah, M. A. and Ariffin, M. R. K., 2016b)

We recall that Wiener's attack works efficiently on RSA with the condition that the secret exponent $d < \frac{1}{3}N^{\frac{1}{4}}$. Later, Nitaj (Nitaj, A., 2013) revisited the Wiener's theorem and proof. As a result, the upper bound was improved satisfying $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. In this work, we present another proof to Wiener's short secret exponent satisfying $d < \frac{1}{2}N^{\frac{1}{4}}$. We remark that our result is slightly better than the previously mentioned attacks in (Wiener M., 1990) and (Nitaj, A., 2013).

This paper was written in five main sections. In Section 2 we give definitions and useful theorems that are needed in our work. Section 3 provides mathematical proof of our result. We illustrate two numerical examples to show how the attack was conducted and performance analysis by comparing with Wiener's (Wiener M., 1990) and Nitaj's (Nitaj, A., 2013) attack's, respectively in Section 4. Finally, in Section 5 we end with a conclusion of our work.

PRELIMINARIES

In this section, we state the definition of continued fraction and useful theorems that form the basis for this paper. These include the result from (Wiener M., 1990) and (Nitaj, A., 2013).

Definition 2.1 (Continued fraction) *Each rational number x can be written as an expression of the form*

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \ddots}}}$$

A simple way to show the above expression is by the form $x = [a_0, a_1, a_2 \ldots a_n]$. We define that the i^{th} term from the list of the continued fraction to be $[a_0, a_1, a_2, \ldots, a_i]$ for $i \geq 0$.

An important result on continued fractions that will be used is the following theorem.

Theorem 2.2 (Legendre's Theorem) *Suppose x is written in its continued fraction expansion $[a_0, a_1, a_2, \ldots]$ form. If $y, z \in \mathbb{Z}$ and coprime such that*

$$|x - \frac{y}{z}| < \frac{1}{2z^2}$$

then $\frac{y}{z}$ is a rational number amongst the continued fraction's convergent of x.

Suppose $N = pq$ is an RSA modulus where the bit-length of the primes p and q are in the same size (i.e. $q < p < 2q$). Such condition will be used throughout this paper.

Theorem 2.3 (Wiener's Theorem) *Let e be an RSA public exponent and d be the RSA private exponent satisfying the relation $ed - k\phi(N) = 1$. Let $d < \frac{1}{3}N^{\frac{1}{4}}$, then the integer k and d appeared the continued fraction's convergent of $\frac{e}{N}$.*

Later, Nitaj (2013) refine the bound of d as stated in the following theorem.

Theorem 2.4 (Nitaj, A., 2013). *The integer k and d can be obtained from the convergent of the continued fraction of $\frac{e}{N}$, if $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$.*

OUR RESULT

In comparison to the (Wiener M., 1990) and (Nitaj, A., 2013) bounds of which $d < \frac{1}{3}N^{1/4}$ and $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$, respectively, our bound is fixed to $d < \frac{1}{2}N^{1/4}$. We begin with the following lemma.

Lemma 3.1 *Suppose we have the prime factors p and q with $q < p < 2q$ and let $N = pq$ be the RSA modulus. Then*

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

and

$$p + q > 2N^{1/2}$$

Proof. The first statement is straight forward. Now, we provide the proof for the second statement. Observe the relation of $(p + q)^2 = (p - q)^2 + 4N$. Thus, directly gives $p + q > 4N > 2N^{1/2}$.

We prove our main result as follows.

Theorem 3.2 *Suppose $ed - \phi(N)k = 1$ be the RSA key equation. If $d < \frac{1}{2}N^{1/4}$, then the*

secret value of k and d are easily recovered from the continued fraction's convergent of $\frac{e}{N}$.

Proof. Let $ed - \phi(N)k = 1$ be the RSA key equation. Thus, such equation can be transformed as follows.

$$ed - k(N + 1 - p - q) = 1$$

$$ed - Nk = 1 - k(p + q - 1) \qquad (1)$$

Divides both sides of (1) by Nd and take the modulus sign, thus we have

$$\begin{aligned}\left|\frac{e}{N} - \frac{k}{d}\right| &= \left|\frac{1 - k(p + q - 1)}{Nd}\right| \\ &= \left|\frac{k(p + q - 1) - 1}{Nd}\right| \\ &< \frac{k(p + q - 1)}{Nd} \qquad (2)\end{aligned}$$

Let the public RSA exponent $e < \phi(N)$, then rearranging $ed - \phi(N)k = 1$ we have

$$k = \frac{ed - 1}{\phi(N)} < \frac{ed}{\phi(N)} < d$$

Thus (2) straightforward gives

$$< \frac{p + q}{N}$$

For the Theorem 2.2 to work, it is adequate to show that $\frac{p+q}{N} < \frac{1}{2d^2}$.

Hence, by making the secret value d as the subject and plugging in the condition of Lemma 3.1, we have the following result

$$\begin{aligned}d &< \left(\frac{N}{2(p + q)}\right)^{1/2} \\ &< \left(\frac{N}{2(2N^{1/2})}\right)^{1/2} \\ &= \frac{1}{2}N^{1/4}\end{aligned}$$

COMPARATIVE ANALYSIS AND EXAMPLES

Table 1 compare our result in Section 3 with Wiener (1990) and Nitaj's (2013), respectively. The result, as shown in Table 1, indicate that regarding the attack and finding the secret parameter d, our result significantly improves the previous bound, which extends the Wiener's Theorem by 16.7%. While a comparison of with Nitaj's theorem reveals slight betterment, which is improves significantly by 1.5%.

Table 1: Comparison of the bounds on d for RSA modulo $N = pq$

Reference	Bounds for d
(Wiener M., 1990)	$d < \frac{1}{3}N^{\frac{1}{4}} \approx 0.333N^{\frac{1}{4}}$
(Nitaj, A., 2013)	$d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}} \approx 0.485N^{\frac{1}{4}}$
Our work	$d < \frac{1}{2}N^{\frac{1}{4}} \approx 0.500N^{\frac{1}{4}}$

Next, we provide algorithm workflow for factoring finding d and k based on Theorem 3.2 as follows.

Algorithm 4.1 Algorithm for factoring finding d and k based on Theorem 3.2

Input: The public key modulus (N, e)
Output: The secret value d and k

1. Compute the continued fraction of $\frac{e}{N}$.
2. For each convergent $\frac{k\prime}{d\prime}$ of $\frac{e}{N}$, compute $N' = \frac{ed\prime-1}{k\prime}$.
3. For N' be an integer, proceed to Step 4. Else, repeat Step 2.
4. Compute $ed(\mathrm{mod}\ N')$.
5. Output the $d = d'$ and $k = k'$ if $ed' \equiv 1(\mathrm{mod}\ N')$. Else, repeat Step 2.

Turning now to the numerical examples on our result. Consider an RSA modulus N and an RSA public key e as follows.

$N = 13783853195340239094605568589512849083 3$

$e = 11720373558924246698770660273596633861 7$

Example 4.1 *As an illustration of Theorem 3.2, suppose we find a list of the continued fraction expansion of $\frac{e}{N}$ using Algorithm 2. Let the above values of N and e satisfy all the requirements of Theorem 3.2. Hence, we will have a list of the continued fraction expansion of $\frac{e}{N}$ as follows.*

$$\left[0,1,\frac{5}{6},\frac{6}{7},\frac{142}{167},\cdots,\frac{572547398}{673349637},\frac{1438826739}{1692145429},\cdots\right]$$

We find that the secret the integer k and d are amongst the list the convergents of $\frac{e}{N}$. For each convergent $\frac{k\prime}{d\prime}$ of $\frac{e}{N}$, compute $N' = \frac{ed\prime-1}{k\prime}$. In fact, $\frac{k\prime}{d\prime} = \frac{1438826739}{1692145429}$ gives the integer

$N' = 13783853195340239092257454009741219702 8.$

Next, since $ed' \equiv 1(\mathrm{mod}N')$, thus according to Algorithm 2, we obtained $d = d' = 1692145429$ and $k = k' = 1438826739.$

Example 4.2 *Let we consider an RSA modulus*

$N = 13783853195340239094605568589512849083 3$

as the same as in Example 4.1, but with different value e' as follows;

$e' = 78079823056802569754144973506355376043$

Computing the continued fraction expansion of $\frac{e\prime}{N}$ will give the following list;

$$\left[0,1,\frac{1}{2},\frac{4}{7},\frac{13}{23},\cdots,\frac{47970613}{84685116},\frac{969859519}{1712145431},\cdots\right]$$

We find that the secret the integer k and d are amongst the list the convergents of $\frac{e\prime}{N}$. In fact, in this example we obtained $\frac{k}{d} = \frac{969859519}{1712145431}$. From here, one can verified that $e'd' \equiv 1(\mathrm{mod}N')$ holds.

Let us compare the integers d and k with the upper bound of d provided by applying the Wiener's Theorem and Nitaj's Theorem attacks to the same problem. As shown in the Example 4.1, we obtained the secret parameter $d = 1692145429$, which is much larger than Wiener's upper bound (i.e. $d < 1142145426$) and Nitaj's bound (i.e. $d < 1663506620$), respectively.

Referring to the Example 4.2, the attack presented in this example use a much larger value of d yet our attack still finds such secret integer d. Note that, our attack works with the maximal value d less than 1713218139 for the respective N in both examples. Again, the secret integer d from Example 2 is much larger than Wiener's upper bound (i.e. $d < 1142145426$) and Nitaj's bound (i.e. $d < 1663506620$), respectively. Hence, this is in a good agreement with our theoretical result, which is mathematically proven in Theorem 3.2 and as reported in Table 1.

CONCLUSION

Note that Wiener's attack works efficiently on RSA with the condition that the secret exponent $d < \frac{1}{3}N^{\frac{1}{4}}$, which was using a Diophantine's method called continued fractions. Later, the upper bound was improved in Nitaj, A., 2013 satisfying $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. In this work, we present another proof of using continued fraction method that shows a way to obtain the secret exponent d efficiently, satisfying $d < \frac{1}{2}N^{\frac{1}{4}}$. We conclude that our result is slightly better than the previously mentioned attacks, in term of both theoretically and practically, via numerical examples.

ACKNOWLEDGMENT

The present research was partially supported by the Putra Grant - Putra Young Initiative (IPM) -GP-IPM-2017-9519200.

REFERENCES

Asbullah, M. A. and Ariffin, M. R. K. (2014). Comparative Analysis of Three Asymmetric Encryption Schemes Based Upon the Intractability of Square Roots Modulo $N = p^2q$. *4th International Cryptology and Information Security Conference 2014 (CRYPTOLOGY2014)* 24-26 June 2014, Putrajaya, 86-99.

Asbullah, M. A. and Ariffin, M. R. K. (2015). New Attack on RSA with Modulus $N = p^2q$ Using Continued Fractions, *Journal of Physics* **622** 191-199.

Asbullah, M. A. and Ariffin, M. R. K. (2016a) Analysis on the AA_β Cryptosystem. *5th International Cryptology and Information Security Conference 2016 (Cryptology2016)*, 31 May-2 June 2016, Sabah, Malaysia, 41-48.

Asbullah, M. A. and Ariffin, M. R. K. (2016b). Analysis on the Rabin-p cryptosystem. *4th International Conference on Fundamental and Applied Sciences (ICFAS2016). AIP Conf. Proc.* **1787** 080012-1 - 080012-8

Asbullah, M. A. and Ariffin, M. R. K. (2016c). Design of Rabin-like cryptosystem without decryption failure. *Malaysian Journal of Mathematical Sciences* **10 (S)** 1 - 18.

de Weger, B. (2002). Cryptanalysis of RSA with Small Prime Difference *Applicable Algebra in Enginering, Commnication and Computing AAECC* **13** 17-28.

Maitra, S. and Sarkar, S. (2008). Revisiting Wiener's Attack- New Weak Keys in RSA. *11th International Conference on Information Security ISC* Taipei.

Nitaj, A. (2013). Diophantine and lattice cryptanalysis of the RSA cryptosystem *In Artificial Intelligence, Evolutionary Computing and Metaheuristics* Springer Berlin Heidelberg 139-168.

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

Wiener M. (1990). Cryptanalysis of Short RSA Secret Exponents *IEEE Trans. Inform. Theory* 36 **3** 553-558.