Malaysian Journal of Mathematical Sciences 13(S) April: 89–99 (2019)
Special Issue: 3rd International Conference on Mathematical Sciences and Statistics (ICMSS2018)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

A New Improved Bound for Short Decryption Exponent on RSA Modulus $N = pq$ using Wiener's Method

Abubakar, S. I. [1], Ariffin, M. R. K. * [1,2], and Asbullah, M. A.[1]

[1] *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*

E-mail: rezal@upm.edu.my
* *Corresponding author*

ABSTRACT

The use of short decryption exponent to mount an attack on RSA cryptosystem was first reported that the RSA modulus $N = pq$ is insecure if the private key $d < \frac{1}{3}N^{0.25}$. The private key d can be recovered from the convergents of the continued fraction expansion of $\frac{e}{N}$ which led to the factorization of N in polynomial time. Suppose $N_1 = N - \lceil [\frac{a^{\frac{j}{i}} + b^{\frac{j}{i}}}{(2ab)^{\frac{j}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{(2ab)^{\frac{1}{2j}}}]\sqrt{N}\rceil + 1$ where a, b, i, j are small positive integers less than $\log N$. In this paper, we present a new improved attack on RSA which is an extension of the recent bound of $d < 2\sqrt{2}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.25}$ that shows that the RSA modulus $N = pq$ can be easily recovered if the short decryption exponent $d < \sqrt{\frac{a^j + b^i}{2}}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.375}$. Thus, from the convergents of the continued fraction of $\frac{e}{N_1}$, the private key d can be recovered hence lead to the factorization of N in polynomial time.

Keywords: RSA, cryptanalysis, key equation, decryption, continued fraction.

1. Introduction

The RSA public-key cryptosystem is the most widely used public-key cryptosystem today invented by Rivest et al. (1978). The RSA key setup involves randomly selecting two large prime numbers p, q whose product $N = pq$ is termed as the RSA modulus. Then, we generate two integers e, d satisfying $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N) = (p-1)(q-1)$ is the Euler totient function of N. Hence, we have (e, N) as the public key pair that can be used in encrypting message and (d, p, q) as the private key tuple used in decrypting the ciphertext.

The security of RSA cryptosystem relies on the difficulty of solving the integer factorization problem (i.e. finding the prime factors of N). It is therefore recommended that for the RSA users to generates primes p and q in such a way that the problem of factoring $N = pq$ is computationally infeasible for an adversary to factor such modulus N (Rahman et al., 2018). Choosing p and q as strong primes has been recommended as a way of maximizing the difficulty of factoring RSA modulus N (Ghafar et al., 2018).

The main reason of using the short decryption exponent is to speed up the decryption process and reduce the decryption time. Wiener Wiener (1990) was the first to carryout an attack on RSA modulus $N = pq$ using continued fraction technique. As a result, the short decryption exponent d is insecure if $d < \frac{1}{3}N^{0.25}$. Recently, by using another proving technique, Asbullah and Ariffin (2019) proposed an extension of Wiener's work which RSA insecure when the secret exponent $d < \frac{1}{2}N^{0.25}$.

Our paper was motivated from the earlier work of a good approximation of $\phi(N)$ methodology in Asbullah and Ariffin (2015). We were also inspired by the improved method in Bunder and Tonien (2017) which showed that the RSA modulus $N = pq$ is insecure if the short decryption exponent $d < 2\sqrt{2}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.25}$. Bunder and Tonien (2017) used the continued fraction technique to recover d from the convergents of continued fraction of $\frac{e}{N-(1+\frac{3}{2\sqrt{2}})N^{\frac{1}{2}}+1}$. Suppose $N_1 < N - \left\lceil \left(\frac{a^{\frac{j}{i}}+b^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}} + \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$ where a, b , i and j are small positive integers less than $\log N$. In this paper, we present a new improved attack on RSA which is an extension of the recent bound of $d < 2\sqrt{2}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.25}$ that shows that the RSA modulus $N = pq$ can be easily recovered if the short decryption exponent $d < \sqrt{\frac{a^j+b^i}{2}}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.375}$. Thus, from the convergents of the continued fraction of $\frac{e}{N_1}$, the private key d can be recovered hence lead to the factorization of N in polynomial time.

The rest of the paper is organize as follows. Section 2 provides definitions and useful theorems that are needed in our work. Section 3 reports and proves useful lemmas and theorem to support our claims. We give an experiment result to show how the attack was efficiently carryout in Section 4. Finally, we conclude the paper in Section 5.

2. 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 (1990) and Bunder and Tonien (2017).

Definition 2.1. *(Continued Fraction) The continued fraction of a real number x is an expression of the form*

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \ddots}}} = [a_0, a_1, \ldots, a_n, \ldots],$$

This expression is often used in the form of $x = [a_0, a_1, a_2....]$. Any rational number $\frac{a}{b}$ can be expressed as a finite continued fraction $x = [a_0, a_1, a_2....a_m]$. For $i \geq 0$, we define the i^{th} convergent of the continued fraction $[a_0, a_1, a_2, ...]$ to be $[a_0, a_1, a_2, ..., a_i]$. Each convergent is a rational number.

Note that, the continued fraction technique also widely used for algebraic cryptanalysis such as in Asbullah and Ariffin (2014, 2016) and Abubakar et al. (2018). An important result on continued fractions that will be used is the following theorem.

Theorem 2.1. (Legendre) Asbullah et al. (2016) Let $x = [a_0, a_1, a_2, \ldots]$ be the continued fraction expansion of x. If y and z are coprime integers such that

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

then $\frac{y}{z}$ is a convergent of x.

Theorem 2.2. *(Wiener's Theorem Wiener (1990)) Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < \phi(N)$ be a public exponent and d be the corresponding private exponent. If $d < \frac{1}{3}N^{\frac{1}{4}}$, then one can factor N in polynomial time.*

Theorem 2.3. *(Bunder and Tonien (2017)) Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < \phi(N)$ be a public exponent and the relation $ed - k\phi(N) = 1$ be satisfied where $k \in Z$. If $d < 2\sqrt{2}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.25}$, then $\frac{k}{d}$ is a convergent of $\frac{e}{N-(1+\frac{3}{2\sqrt{2}})N^{\frac{1}{2}}+1}$.Thus the secret information p, q, d, k can be recovered from the public information (e, N) where $\phi(N) = \frac{ed-1}{k}$.*

3. Main Results

In this section, we present a new cryptanalytic result via $\phi(N)$ approximation given by $N - \left\lceil \left(\frac{a^{\frac{j}{i}}+b^{\frac{j}{i}}}{(2ab)^{\frac{j}{2i}}} + \frac{a^{\frac{1}{j}}+b^{\frac{1}{j}}}{(2ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$. This approximation of $\phi(N)$ enables us to extend the bound of susceptible decryption exponent given by $d < \sqrt{\frac{a^j+b^i}{2}}(\frac{N}{e})^{\frac{1}{2}} N^{0.375}$. In this section, we also prove two lemmas and a theorem that are used to carryout our attack on RSA modulus $N = pq$ as follows.

Lemma 3.1. *If a and b are positive integers less than $\log N$ and p and q are prime numbers such that $a > b$ and $ap^j - bq^j \neq 0$ and $N = pq$, then $\phi(N) < N - \left\lceil \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}} \sqrt{N} \right\rceil + 1$ for $2 < i < j$.*

Proof. Let $(ap^j - bq^j)(bp^j - aq^j) > 0$, then we get

$$abp^{2j} - a^2p^jq^j - b^2p^jq^j + abq^{2j} > 0$$

$$ab(p^{2j} + q^{2j}) > (a^2 + b^2)p^jq^j$$

Adding $2abp^jq^j$ to both sides we have:

$$ab(p^{2j} + 2p^jq^j + q^{2j}) > (a^2 + 2ab + b^2)p^jq^j$$

$$(p^j + q^j)^2 > \frac{(a+b)^2p^jq^j}{ab}$$

$$p^j + q^j > \frac{(a+b)(p^jq^j)^{\frac{1}{2}}}{\sqrt{ab}}$$

Since $(p+q)^j > p^j + q^j$, then

$$p + q > \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}}\sqrt{N}$$

Then $\phi(N) < N - \left\lceil \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}}\sqrt{N} \right\rceil + 1$ □

Lemma 3.2. *If a and b are small positive integers and p and q are prime numbers such that $a^j p^i - b^j q^i \neq 0$ and $N = pq$ is RSA modulus satisfying the condition $e < \phi(N)$, then $\phi(N) > N - \left\lceil \frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}}\sqrt{N} \right\rceil + 1$, for $2 < i < j$ and $a > b$.*

Proof. Let $(a^j p^i - b^j q^i)(b^j p^i - a^j q^i) < 0$, then we get

$$a^j b^j p^{2i} - a^{2j} p^i q^i - b^{2j} p^i q^i + a^j b^j q^{2i} < 0$$
$$a^j b^j (p^{2i} + q^{2i}) < (a^{2j} + b^{2j}) p^i q^i$$

Adding $2a^j b^j p^i q^i$ to both sides we have

$$a^j b^j (p^i + q^i)^2 < (a^j + b^j)^2 p^i q^i$$
$$(p^i + q^i)^2 < \frac{(a^j + b^j)^2}{a^j b^j} N^i$$
$$p^i + q^i < \frac{a^j + b^j}{(ab)^{\frac{j}{2}}} N^{\frac{i}{2}}$$

Since $p^i + q^i < (p+q)^i$, then

$$p + q < \frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}}\sqrt{N}$$

$\phi(N) > N - \left\lceil \frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}}\sqrt{N} \right\rceil + 1$ □

Theorem 3.1. *Let p and q be distinct prime numbers and let $N = pq$ be RSA modulus where (N, e) are public key pair with condition $e < \phi(N)$. If $d < \sqrt{\frac{a^j + b^i}{2}} (\frac{N}{e})^{\frac{1}{2}} N^{0.375}$ and $N_1 < N - \left\lceil \left(\frac{a^{\frac{j}{i}} + b^{\frac{j}{i}}}{(2ab)^{\frac{j}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{(2ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$, for $2 < j < i$ then one of the convergents $\frac{k}{d}$ can be found from continued fraction expansion of $\frac{e}{N_1}$ which leads to the factorization of RSA modulus N in polynomial time.*

Proof. From Lemmas 3.1 and 3.2, let:

$$\phi_1 = N - \left\lceil \frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}}\sqrt{N} \right\rceil + 1$$

$$\phi_2 = N - \left\lceil \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}}\sqrt{N} \right\rceil + 1$$

Let N_1 be the midpoint of interval of $[\phi_1, \phi_2]$. Then:

$$\begin{aligned}
N_1 &= \frac{1}{2}[\phi_1 + \phi_2] \\
&= N - \left\lceil \left(\frac{(a+b)^{\frac{j}{i}}}{(2ab)^{\frac{j}{2i}}} + \frac{(a+b)^{\frac{1}{j}}}{(2ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1 \\
&< N - \left\lceil \left(\frac{a^{\frac{j}{i}} + b^{\frac{j}{i}}}{(2ab)^{\frac{j}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{(2ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1
\end{aligned}$$

Also let:

$$\begin{aligned}
N_2 &= (\phi_2 - \phi_1) \\
&= N - \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}}\sqrt{N} + 1 - (N - \frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}}\sqrt{N} + 1) \\
&= \left(\frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}} - \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}} \right) \sqrt{N}
\end{aligned}$$

Taking $|\phi(N) - N_1| < \frac{2}{3}(N_2)$, then we have:

$$|\phi(N) - N_1| < \frac{2}{3}(\phi_2 - \phi_1)$$

Using the RSA key equation $ed = 1 + k\phi(N)$, for some $k \in Z$, it gives:

$$\begin{aligned}
ed - k\phi(N) &= 1 \\
|\frac{e}{\phi(N)} - \frac{k}{d}| &= \frac{1}{d\phi(N)}
\end{aligned}$$

Taking N_1 to be an approximation of $\phi(N)$ yields:

$$\begin{aligned}
\left| \frac{e}{N_1} - \frac{k}{d} \right| &= \left| \frac{e}{N_1} - \frac{e}{\phi(N)} + \frac{e}{\phi(N)} - \frac{k}{d} \right| \\
&= \left| \frac{e}{N_1} - \frac{e}{\phi(N)} \right| + \left| \frac{e}{\phi(N)} - \frac{k}{d} \right| \\
&\leq \frac{|e\phi(N) - eN_1|}{N_1\phi(N)} + \frac{ed - k\phi(N)}{d\phi(N)} \\
&\leq e\frac{|(\phi(N) - N_1)|}{N_1\phi(N)} + \frac{1}{d\phi(N)}
\end{aligned}$$

$$\left|\frac{e}{N_1} - \frac{k}{d}\right| < e\frac{|(\phi(N) - N_1)|}{N_1\phi(N)} + \frac{1}{d\phi(N)} \tag{1}$$

But $e < \phi(N)$, $|\phi(N) - N_1| < \frac{2}{3}(\phi_2 - \phi_1)$ and $d = \frac{1+k\phi(N)}{e}$. Plugging these conditions into inequality (1) yields:

$$\begin{aligned}\left|\frac{e}{N_1} - \frac{k}{d}\right| &< e\frac{2(\phi_2 - \phi_1)}{3\phi(N)N_1} + \frac{e}{\phi(N)(1 + k\phi(N))}\\ &< e\frac{2(\phi_2 - \phi_1)}{3\phi^2(N)} + \frac{e}{\phi^2(N)}\\ &< \frac{2(\phi_2 - \phi_1) + 3}{3\phi(N)}\end{aligned}$$

Also, taking $\frac{2\left(\frac{(a+b)^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}} - \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}}\right)+3}{3\phi(N)} < \frac{e}{N^{\frac{7}{4}}(a^j+b^i)}$ and applying continued fraction theorem gives:

$$\begin{aligned}\frac{e}{N^{\frac{7}{4}}(a^j + b^i)} &< \frac{1}{2d^2}\\ \frac{e}{N^{\frac{7}{4}}(a^j + b^i)} &< \frac{1}{2d^2}\\ d &< \sqrt{\frac{a^j + b^i}{2}}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.375}\end{aligned}$$

□

Our new bound $d < \sqrt{\frac{a^j+b^i}{2}}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.375}$ is an improvement on the work of Bunder and Tonien (2017) whose bound is $d < 2\sqrt{2}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.25}$.

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

Author(s)	Bounds for d
Wiener (1990)	$d < \frac{1}{3}N^{0.25}$
De Weger (2002)	$d < \frac{N^{\frac{3}{4}}}{\lvert p-q\rvert}$
Nitaj (2013)	$d < \frac{\sqrt{6\sqrt{2}}}{6}N^{0.25}$
Bunder and Tonien (2017)	$d < 2\sqrt{2}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.25}$
Our result	$d < \sqrt{\frac{a^j+b^i}{2}}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.375}$

From Table(1) one can observe that our bound $d < \sqrt{\frac{a^j+b^i}{2}}\left(\frac{N}{e}\right)^{\frac{1}{2}} N^{0.375}$ is consider to be greater than the aforementioned bounds.

4. Numerical Result

In this section, we give a numerical example to illustrates how the attack works.

Table 2: Algorithm for factoring $N = pq$ based on Theorem 3.1

```
INPUT: The tuple $(N, e)$ and the value $a, b, i, j$ satisfying Theorem 3.1
OUTPUT: The prime factors $p$ and $q$.
1. Compute $N_1 < N - \left\lceil \left( \frac{a^{\frac{j}{i}} + b^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}} + \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$ .
2. Compute the continued fraction of $\frac{e}{N_1}$.
3. For each convergent $\frac{k}{d}$ of $\frac{e}{N_1}$ compute $N' = \frac{ed-1}{k}$.
4. Compute $N - N' + 1$.
5. Solve the quadratic equation $X^2 - (N - N' + 1)X + N$.
6. Output the roots of the equation as $p$ and $q$.
```

Example 4.1. *In what follows, we give a numerical example to show how the attack works.*

$$\begin{aligned} \textit{Let } N &= 5265653757185996710045551788402196725555642452432500175631391179725714328242 3 \\ e &= 4312889619331195815496301034026806166886782203723547353247431309725983794396 9 \end{aligned}$$

where $a = 3$, $b = 2$, $j = 4, i = 3$ *and taken continued fraction expansion of* $\frac{e}{N - \left\lceil \left(\frac{a^{\frac{j}{i}} + b^{\frac{j}{i}}}{(2ab)^{\frac{j}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{(2ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1}$ *we get the following:*

$$[0, 1, 4, 1, 1, 8, 1, 6, 12, 9, 2, 1, 9, 3, 1, 1, 8, 4, 5, 1, 6, 1, 1, 4, 2, 1, 1, 8, 3, 1, 13,$$

$$2, 3, 1, 6, 7, 3, 2, 1, 2, 2, 2, 4, 6, 2, 4, 3, 3, 13, 9, 2, 2, 2, 2, 1, 5, 12, 1, 758,$$

$$2, 60, 6, 2, 1, 1, 1, 2, 4, 1, 3, 1, 3, 7, 2, 123, 9, 1, 1, 3, 1, 4, 2, 2, 26, 5, 9, 2, 1, 2,$$

$$1, 3, 1, 2, 1, 1, 1, 2, 1, 28, 4, 22, 1, 7, 4, 2, 2, 2, 2, 2, 2, 1, 2, 9, 3, 137, 1, 2, 1, 2,$$

$$2, 1, 17, 9, 1, 6, 2, 1, 14, 2, 1, 2, 2, 3, 7, 1, 9, 2, 1, 3, 1, 1, 1, 4, 1, 3, 1, 23]$$

Also taking the convergents of continued fraction expansion of $\frac{e}{N - \left\lceil \left(\frac{a^{\frac{j}{i}} + b^{\frac{j}{i}}}{(2ab)^{\frac{j}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{(2ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1}$ *yields the following:*

$$[0, 1, \frac{4}{5}, \frac{5}{6}, \cdots, \frac{16518333807348465121}{20167413069246359606}, \frac{40004797970066937235}{48842292135734192929}, \cdots,]$$

Taking $\frac{k}{d} = \frac{400047979700669937235}{48842292135734192929}$ *and computing* $\phi(N) = \frac{ed-1}{k}$

$$\phi(N) = 52656537571859967100455517884021967255088402895347\\ 714789700733955831043328320$$

$$N - \phi(N) + 1 = 468021628977286966613177841426099954104$$

Finally, solving the quadratic equation for x below

$$x^2 - (N - \phi(N) + 1)x + N = 0$$

will lead to the factorization of N *in polynomial time.*

$$x_1 = p = 279885902780420619755064053216198237143$$

$$x_2 = q = 188135726196866346858113788209901716961$$

The example given above shows that the convergent $\frac{k}{d}$ can be found from continued fraction expansion of $\frac{e}{N_1}$ which enables us to find prime factors p and q of RSA modulus N. Also our result shows that the short decryption exponent found is greater than the Bunder's (2017) bound of $d < 2\sqrt{2}(\frac{N}{e})^{\frac{1}{2}}N^{0.25}$, that is $2\sqrt{2}(\frac{N}{e})^{\frac{1}{2}}N^{0.25} < d < \sqrt{\frac{a^j+b^j}{2}}(\frac{N}{e})^{\frac{1}{2}}N^{0.375}$, that is

$$4.734237550^{19} < 48842292135734192929 < 4.536881742 \times 10^{29}.$$

5. Conclusion

In this paper, it has been established that a new improved attack on Wiener (1990), Nitaj (2013) bound was carryout successfully which is also an extension of Bunder and Tonien (2017) result. The paper uses continued fraction method to recover the private exponent d from the convergents of the continued fraction of $\frac{e}{N - \left\lceil \left(\frac{a^{\frac{j}{i}} + b^{\frac{j}{i}}}{(ab)^{\frac{j}{2i}}} + \frac{(a+b)^{\frac{1}{j}}}{(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1}$. This would not have been possible if we were forced to use the continued fraction expansion to obtained $\frac{k}{d}$ as suggested by Wiener (1990), Nitaj (2013) and Bunder and Tonien (2017), thus this indicates that our usage of $\frac{e}{N_1}$ is significant.

6. Acknowledgment

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

References

Abubakar, S. I., Ariffin, M. R. K., and Asbullah, M. A. (2018). A New Simultaneous Diophantine Attack Upon RSA Moduli $N = pq$. In *6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)*, page 119.

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

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(1):191–199.

Asbullah, M. A. and Ariffin, M. R. K. (2016). Analysis on the AA_β cryptosystem. In *5th International Cryptology and Information Security Conference (CRYPTOLOGY2016)*, pages 41–48.

Asbullah, M. A. and Ariffin, M. R. K. (2019). Another Proof Of Wiener's Short Secret Exponent. *Malaysian Journal of Science*, 1(1):62–68.

Asbullah, M. A., Ariffin, M. R. K., and Mahad, Z. (2016). Analysis on the Rabin-p cryptosystem. In *AIP Conference Proceedings*, volume 1787, page 080012. AIP Publishing.

Bunder, M. W. and Tonien, J. (2017). New attack on the rsa cryptosystem based on continued fractions.

De Weger, B. (2002). Cryptanalysis of rsa with small prime difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17–28.

Ghafar, A. H. A., Ariffin, M. R. K., and Asbullah, M. A. (2018). Extending Pollard Class of Factorable RSA Modulus. In *6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)*, page 103.

Nitaj, A. (2013). Diophantine and lattice cryptanalysis of the rsa cryptosystem. In *Artificial Intelligence, Evolutionary Computing and Metaheuristics*, pages 139–168. Springer.

Rahman, N. N. A., Ariffin, M. R. K., Asbullah, M. A., and Yunos, F. (2018). New Vulnerability on System of $N_i = p_i^2 q_i$ using Good Approximation of $\phi(N)$. In *6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)*, page 139.

Rivest, R. L., 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. J. (1990). Cryptanalysis of short rsa secret exponents. *IEEE Transactions on Information theory*, 36(3):553–558.