New Attacks on RSA with Modulus $N = p^2q$ Using Continued Fractions

New Attacks on RSA with Modulus $N = p^2q$ Using Continued Fractions

M A Asbullah[1] and M R K Ariffin[2]

[1,2]Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, 43400, Malaysia
[2]Department of Mathematics, Faculty of Sciences, Universiti Putra Malaysia, Serdang, 43400, Malaysia

E-mail: [1]ma_asyraf@upm.edu.my,[2]rezal@upm.edu.my

Abstract. In this paper, we propose two new attacks on RSA with modulus $N = p^2q$ using continued fractions. Our first attack is based on the RSA key equation $ed - \phi(N)k = 1$ where $\phi(N) = p(p-1)(q-1)$. Assuming that $q < p < 2q$, $2p^{5/3}|p^{1/3} - q^{1/3}| < \frac{1}{3}N^{\beta}$ and $d < N^{\frac{1-\beta}{2}}$, we show that $\frac{k}{d}$ can be recovered among the convergents of the continued fraction expansion of $\frac{e}{N-(2N^{2/3}-N^{1/3})}$. Our second attack is based on the equation $eX - \left(N - \left(ap^2 + bq^2\right)\right)Y = Z$ where a, b are positive integers satisfying $\gcd(a, b) = 1$, $|ap^2 - bq^2| < N^{1/2}$ and $ap^2 + bq^2 = N^{2/3+\alpha}$ with $0 < \alpha < \frac{1}{3}$. Given the conditions $|Z| < \frac{1}{3}N^{1/3+\alpha}Y$ and $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$, we show that one can factor $N = p^2q$ in polynomial time.

1. Introduction

Prior to 1970's, the encryption and decryption were done only in symmetrical ways. It is only until 1978, the RSA cryptosystem [13] went public and it is regarded now by the cryptographic community as the first realization of the public key cryptosystem. The security of RSA is based on the intractability to solve for the following four key equations; $N = pq$ for large primes p and q of the same size, the Euler totient $\phi(N) = (p-1)(q-1)$; the key equation $ed - \phi(N)k = 1$ such that e is known and finally the modular e^{th}-root problem $c \equiv m^e \pmod{N}$.

The RSA cryptosystem is likely to have faster decryption if the secret exponent d is relatively small. Nevertheless, in 1994 [10] observe that if d is small, say $d < N^{1/4}$ so by exploiting the key equation $ed - \phi(N)k = 1$, he establishes that using a mathematical tool, namely the continued fraction, then such secret exponent can efficiently be recovered. This is one of major concern to implement RSA appropriately, because the knowledge of secret exponent d lead to factoring N in polynomial time. Since then, many researchers have pursued the same direction (i.e. using convergent by continued fraction method, for instance ([5], [6], [14]) purposely to improve the bound $\delta > \frac{1}{4}$ for $d < N^{\delta}$. Besides the continued fraction approach, the usefulness of Coppersmith's theorem [7] widely applied for cryptanalyzing RSA key equations, such as ([1],[3],[8]). A survey on the mathematical cryptanalysis of the RSA cryptosystem can be found in [4].

As mentioned in [1] such that moduli of the form $N = p^2q$ are frequently used in cryptography and therefore they represent one of the most important cases. This assertion is confirmed by

the fact that many RSA-like cryptosystem are designed using such modulus. For example, ([9],[11],[12], [15]).

Our contribution. Hence, in this paper, we contribute two new attacks on RSA-type modulus of $N = p^2q$ using continued fractions. Our first attack is motivated from some previous attacks on RSA using a good approximation of $\phi(N) = p(p-1)(q-1)$. We observe that for $N = p^2q$ with $q < p < 2q$, if we use the term $N - (2N^{2/3} - N^{1/3})$ as an approximation of $\phi(N)$ satisfying the key equation $ed - \phi(N)k = 1$ then $\frac{k}{d}$ is one of a convergent of the continued fraction $\frac{e}{N-(2N^{2/3}-N^{1/3})}$ satisfying $2p^{5/3}|p^{1/3} - q^{1/3}| < \frac{1}{3}N^{\beta}$ and $d < N^{\frac{1-\beta}{2}}$.

The second attack is extending the result of [3] for $N = p^2q$ and e satisfying the variant equation $eX - (N - (ap^2 + bq^2))Y = Z$ where a, b are positive integers with $\gcd(a, b) = 1$ such that $|ap^2 - bq^2| < N^{1/2}$, $ap^2 + bq^2 = N^{2/3+\alpha}$ with $0 < \alpha < \frac{1}{3}$. We show tha if $|Z| < \frac{1}{3}N^{1/3+\alpha}Y$ and $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$, then N can be factored in polynomial time using the second attack.

The rest of this paper is organized as follows. In Section 2 we give an introductory to continued fraction and some previous result regarding to the RSA cryptanalytic method using continued fraction. Section 3 and Section 4 give details around our two approaches, respectively. Finally, Section 5 concludes this paper.

2. Preliminaries

We start with the definition and an important theorem regarding to a continued fraction. We then provide some previous results on cryptanalyzing RSA utilizing such theorem. In this work, the symbol $\phi(N)$ is a notation for Euler totient function for its respective modulus N.

2.1. Continued Fraction

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

$$R = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N} - \{0\}$ for $i \geq 1$. The numbers $a_0, a_1, a_2, \dots$ are called the partial quotients. We use the notation $R = [a_0, a_1, a_2, \dots]$. For $i \geq 1$ the rational $r_i/s_i = [a_0, a_1, a_2, \dots]$ are called the convergents of the continued fraction expansion of R. If $R = \frac{a}{b}$ is a rational number with $\gcd(a, b) = 1$, then the continued fraction expansion is finite.

There are various results and applications of continued fraction. A key role in all our arguments is played by the following result.

Theorem 1 (Legendre). Let a, b, x, y be integer such that $\gcd(a, b) = \gcd(x, y) = 1$. Suppose $|\frac{a}{b} - \frac{x}{y}| < \frac{1}{2y^2}$. Then $\frac{x}{y}$ is a convergent of the continued fraction expansion of $\frac{a}{b}$.

2.2. Previous Attacks On RSA Using Good Approximation of $\phi(N)$

In this section we provide some previous attacks on RSA using the convergents of good approximations of $\phi(N)$.

2.2.1. Wiener's Attack Firstly, let us consider the public exponent e and the private exponent d of an RSA instance related by the key equation $ed - k\phi(N) = 1$ rewritten as

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

Suppose that $\left|\frac{e}{\phi(N)} - \frac{k}{d}\right| < \frac{1}{2d^2}$. Then by Theorem 1, $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{\phi(N)}$. However, the value of $\phi(N)$ is unknown. Suppose we replace $\phi(N)$ with any known value φ such that it is an approximation of $\phi(N)$ and satisfies $\left|\frac{e}{\varphi} - \frac{k}{d}\right| < \frac{1}{2d^2}$. This idea was firstly introduced by Wiener [10]. Since the fact that φ is approximate to N, then he uses $\varphi = N$ which is publicly known. With the additional condition $d < \frac{1}{3}N^{1/4}$, he shows that $\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$, which by Theorem 1 implies that $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$. This leads to the following result.

Theorem 2 [10]. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < \phi(N)$ and d be a public and private exponent, respectively. If $d < \frac{1}{3}N^{1/4}$, then $\left|\frac{e}{\phi(N)} - \frac{k}{d}\right| < \frac{1}{2d^2}$.

2.2.2. de Weger's Generalization

Later, de Weger [5] observes that if the difference between two RSA primes (i.e. $|p-q|$) is small, then $N-2\sqrt{N}+1$ is a better approximation to $\phi(N)$ instead of N. Replacing $\varphi = N-2\sqrt{N}+1$, combining with $\varphi > \frac{3}{4}N$,$N > 8d$ then $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N-2\sqrt{N}+1}$ which is satisfying the Theorem 1, as stated in the following result.

Theorem 3 [5]. Let $N = pq$ be an RSA modulus with $q < p < 2q$ with $N > 8d$ and $|p-q| < N^{\beta}$. Let $e < \phi(N)$ with $\phi(N) > \frac{3}{4}N$ and $d < N^{\delta}$ be a public and private exponent, respectively. If $\delta < \frac{3}{4} - \beta$, then $\left|\frac{e}{N-2\sqrt{N}+1} - \frac{k}{d}\right| < \frac{1}{2d^2}$.

2.2.3. Maitra and Sarkar's Attack

In [5], de Weger considered the situation that p and q are too close. This implies that $p-q$ is small. Later on, Maitra and Sarkar [14] consider the case that p and $2q$ are too close. This means that $|2q-p|$ is small. Assuming this, they showed that $N-\frac{3}{\sqrt{2}}\sqrt{N}+1$ is a better approximation to $\phi(N)$ instead of N.

Replacing $\varphi = N-\frac{3}{\sqrt{2}}\sqrt{N}+1$ with $N > 8d$, [14] shows that $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N-\frac{3}{\sqrt{2}}\sqrt{N}+1}$ satisfying Theorem 1, as follows.

Theorem 4 [14]. Let $N = pq$ be an RSA modulus with $q < p < 2q$ with $N > 8d$ and $|2q-p| < N^{\gamma}$. Let $e < \phi(N)$ and $d < N^{\delta}$ be a public and private exponent, respectively. If $\delta < \frac{3}{4} - \gamma$, then $\left|\frac{e}{N-\frac{3}{\sqrt{2}}\sqrt{N}+1} - \frac{k}{d}\right| < \frac{1}{2d^2}$.

2.2.4. Chen et.al's Attack

In 2009, Chen et al. [6] generalize the result of [5] and [14] using the difference between two multiples of primes $|aq-bp|$ with $a > b$ and assuming that the ratio of the RSA primes $\frac{p}{q}$ is close to a simple fraction $\frac{b}{a}$ such that $(b(a^2+1)q-a(b^2+1)p)(aq-bp)) > 0$. Let $|aq-bp| < N^{\gamma}$. Replacing $\varphi = N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1$, [6] shows that $\frac{k}{d}$ can be obtained from the continued fraction expansion of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1}$ which is satisfying the Theorem 1. The work of [6] obtain the same result as [5] if $a = b = 1$, and get the same result as [14] when $\frac{b}{a} = \frac{1}{2}$. We present the result of [6] as follows.

Theorem 5 [6]. Let $N = pq$ be an RSA modulus with $q < p < 2q$ with $N > 8d$ and $|aq - bp| < N^{\gamma}$. Let $e < \phi(N)$ and $d < N^{\delta}$ be a public and private exponent, respectively. If $\delta < \frac{3}{4} - \gamma$, then $\left| \frac{e}{N - \frac{a+b}{\sqrt{ab}}\sqrt{N}+1} - \frac{k}{d} \right| < \frac{1}{2d^2}$.

3. Our First Attack

In this section we prove our first attacks. We begin with a simple lemma fixing the sizes of the prime factor of the RSA modulus.

Lemma 1. Let $N = p^2q$ with $q < p < 2q$. Then

$$2^{-1/3}N^{1/3} < q < N^{1/3} < p < 2^{1/3}N^{1/3}.$$

Proof. Suppose $q < p < 2q$. Multiplying by p^2, we get $N < p^3 < 2N$. Hence $N^{1/3} < p < 2^{1/3}N^{1/3}$. Multiplying $q < p < 2q$ by q^2, we get $q^3 < N < 2q^3$ implies $2^{-1/3}N^{1/3} < q < N^{1/3}$. This terminates the proof. ■

Let $N = p^2q$. Then

$$\phi(N) = p(p-1)(q-1) = p^2q - p^2 - pq + p = N - (p^2 + pq - p).$$

The following result gives a interval for $N - \phi(N) = p^2 + pq - p$ in terms of N. It shows that if $p \approx q$, then $N - \left(2N^{2/3} - N^{1/3}\right)$ is a good approximation to $\phi(N)$, while if $p \approx 2q$, then $N - \left(\left(2^{2/3} + 2^{-1/3}\right)N^{2/3} - 2^{1/3}N^{1/3}\right)$ is a good approximation to $\phi(N)$.

Lemma 2. Let $N = p^2q$ with $q < p < 2q$. Then

$$2N^{2/3} - N^{1/3} < N - \phi(N) < \left(2^{2/3} + 2^{-1/3}\right)N^{2/3} - 2^{1/3}N^{1/3}.$$

Proof. Suppose $N = p^2q$ with $q < p < 2q$. We have $N - \phi(N) = p^2 + pq - p = p^2 + \frac{N}{p} - p$. Define the function f such that $f(p) = p^2 + \frac{N}{p} - p$. Then, the derivative is such that

$$f'(p) = 2p - \frac{N}{p^2} - 1 = 2p - q - 1 > 0.$$

Then the function f is strictly increasing for the interval of p, that is $(N^{1/3}, 2N^{1/3})$ by Lemma 1. Hence $f\left(N^{1/3}\right) < f(p) < f\left(2N^{1/3}\right)$, which leads to

$$2N^{2/3} - N^{1/3} < p^2 + pq - p < \left(2^{2/3} + 2^{-1/3}\right)N^{2/3} - 2^{1/3}N^{1/3}.$$

Since $p^2 + pq - p = N - \phi(N)$, this terminates the proof. ■

Lemma 3. Let $N = p^2q$ and $\phi(N) = N - (p^2 + pq - p)$ with $q < p < 2q$. Then

$$\left| N - \left(2N^{2/3} - N^{1/3}\right) - \phi(N) \right| < 2p^{5/3}|p^{1/3} - q^{1/3}|.$$

Proof. Let $N = p^2q$. Using $\phi(N) = p(p-1)(q-1) = p^2q - p^2 - pq + p = N - (p^2 + pq - p)$, we get

$$\begin{aligned}\left|N - \left(2N^{2/3} - N^{1/3}\right) - \phi(N)\right| &= \left|p^2 + pq - p - \left(2N^{2/3} - N^{1/3}\right)\right| \\ &= \left|p^2 + pq - p - \left(2\left(p^2q\right)^{2/3} - \left(p^2q\right)^{1/3}\right)\right| \\ &= |p^{1/3} - q^{1/3}| \times p^{2/3}\left(p + p^{2/3}q^{1/3} - p^{1/3}q^{2/3} - 1\right) \\ &< |p^{1/3} - q^{1/3}| \times p^{2/3}\left(p + p^{2/3}q^{1/3}\right) \\ &< |p^{1/3} - q^{1/3}| \times p^{2/3} \times 2p \\ &= 2p^{5/3}|p^{1/3} - q^{1/3}|.\end{aligned}$$

This terminates the proof.■

Theorem 6. Let $N = p^2q$ with $q < p < 2q$. Let $1 < e < \phi(N) < N - \left(2N^{2/3} - N^{1/3}\right)$ satisfying $ed - k\phi(N) = 1$ for some unknown integers $\phi(N), d, k$. Assume $\phi(N) > \frac{2}{3}N$ and $N > 6d$. Let $2p^{5/3}|p^{1/3} - q^{1/3}| < \frac{1}{3}N^{\beta}$ and $d < N^{\delta}$. If $\delta < \frac{1-\beta}{2}$ then $\left|\frac{e}{N-\left(2N^{2/3}-N^{1/3}\right)} - \frac{k}{d}\right| = \frac{1}{2d^2}$.

Proof. We transform the equation $ed - k\phi(N) = 1$ to

$$ed - k(N - (p^2 + pq - p)) = 1$$

$$ed - k(N - (N - \phi(N))) = 1$$

$$ed - k(N - (2N^{2/3} - N^{1/3}) + (2N^{2/3} - N^{1/3}) - (N - \phi(N)) = 1$$

$$ed - k(N - (2N^{2/3} - N^{1/3})) = 1 - k(N - \phi(N) - (2N^{2/3} - N^{1/3}))$$

Dividing by $d(N - (2N^{2/3} - N^{1/3}))$, on the right hand side we get

$$\begin{aligned}\left|\frac{e}{N - (2N^{2/3} - N^{1/3})} - \frac{k}{d}\right| &= \left|\frac{e}{N - (2N^{2/3} - N^{1/3})} - \frac{e}{\phi(N)} + \frac{e}{\phi(N)} - \frac{k}{d}\right| \\ &\leq \left|\frac{e}{N - (2N^{2/3} - N^{1/3})} - \frac{e}{\phi(N)}\right| + \left|\frac{e}{\phi(N)} - \frac{k}{d}\right| \\ &\leq e\left|\frac{\phi(N) - (N - (2N^{2/3} - N^{1/3}))}{\phi(N)(N - (2N^{2/3} - N^{1/3}))}\right| + \left|\frac{ed - k\phi(N)}{\phi(N)d}\right| \\ &\leq e\left|\frac{\phi(N) - (N - (2N^{2/3} - N^{1/3}))}{\phi(N)(N - (2N^{2/3} - N^{1/3}))}\right| + \left|\frac{ed - k\phi(N)}{\phi(N)d}\right| \\ &\leq e\left|\frac{N - (2N^{2/3} - N^{1/3}) - \phi(N)}{\phi(N)(N - (2N^{2/3} - N^{1/3}))}\right| + \left|\frac{ed - k\phi(N)}{\phi(N)d}\right|\end{aligned}$$

Since $e < N - (2N^{2/3} - N^{1/3})$ and $ed - k\phi(N) = 1$, then we have $\left|\frac{e}{N-(2N^{2/3}-N^{1/3})} - \frac{k}{d}\right| < \left|\frac{N-(2N^{2/3}-N^{1/3})-\phi(N)}{\phi(N)} + \frac{1}{\phi(N)d}\right|$. Using $2p^{5/3}|p^{1/3} - q^{1/3}| < \frac{1}{3}N^{\beta}, d < N^{\delta}$ and $\phi(N) > 4d$, we get

$$\left|\frac{N-(2N^{2/3}-N^{1/3})-\phi(N)}{\phi(N)}+\frac{1}{\phi(N)d}\right| < \frac{1}{2}N^{\beta-1}+\frac{1}{4d^2}$$
$$< \frac{1}{2}N^{\beta-1}+\frac{1}{2}N^{-2\delta}$$

In order to satisfy the Theorem 1, it is suffice when we take $\beta-1<-2\delta$, then $\delta<\frac{1-\beta}{2}$.■

Corollary 1. Consider Theorem 6. If the unknown integer d be discovered from the continued fraction expansion of $\frac{e}{N-(2N^{2/3}-N^{1/3})}$, then N can be factored in polynomial time.

Proof. Suppose we obtained the secret exponent d according to Theorem 6. Observe that from the relation of $\frac{ed-1}{k}=\phi(N)=p(p-1)(q-1)$, therefore computing $\gcd(\frac{ed-1}{k},N)$ should give the prime p.■

Hence, we design the following algorithm to further recovering the prime factorization of the modulus $N=p^2q$.

Algorithm 1.

INPUT: The public key modulus (N,e) satisfying $N=p^2q$ and Theorem 6.
OUTPUT: The prime factors p,q.

1. Compute the continued fraction $\frac{e}{N-(2N^{2/3}-N^{1/3})}$.
2. For each convergent $\frac{k_i}{d_i}$ of $\frac{e}{N-(2N^{2/3}-N^{1/3})}$, compute $\phi(N)_i=\frac{ed_i-1}{k_i}$.
3. Compute $g=\gcd(\phi(N)_i,N)$.
4. If $1<g<N$, then stop.

4. Our Second Attack

In this section we describe our second attack which is based on the work of Nitaj [3]. We extend the method to the modulus $N=p^2q$ instead of $N=pq$. We firstly provide Nitaj's result as follows.

Theorem 7. Let $N=pq$ with $q<p<2q$. Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ with $a\geq 1$ and $|ap-bq|<\frac{1}{2}N^{1/2-\alpha}$. Let e be a public exponent satisfying the equation $eX-(N-(ap+bq))Y=Z$ with $\gcd(X,Y)=1$. Set $ap+bq=N^{1/2+\alpha}$ with $0<\alpha<\frac{1}{2}$. If $|Z|<N^{1/2+\alpha}X$ and $1\leq Y\leq X<\frac{1}{2}N^{1/4-\alpha/2}$, then N can be factored in polynomial time.

Proof. Refer [[3], Theorem 3].

We are now ready to give our second attack. Let the integer closest x denoted as [x].

Lemma 4. Let $N=p^2q$ with $q<p<2q$. Let a,b be integers with $\gcd(a,b)=1$. Let $ap^2+bq^2=N^{2/3+\alpha}$ with $\alpha<\frac{1}{3}$. If $|ap^2+bq^2-S|<\frac{1}{3}N^{1/3-\alpha}$ then $abq=\left[\frac{S^2}{4N}\right]$.

Proof. Set $S = ap^2 + bq^2 + x$. Observe that

$$\begin{aligned}(ap^2 - bq^2)^2 &= (ap^2)^2 - 2(ap^2bq^2) + (bq^2) \\ &= (ap^2)^2 + 2(ap^2bq^2) - 2(ap^2bq^2) - 2(ap^2bq^2) + (bq^2) \\ &= (ap^2 + bq^2)^2 - 4(ap^2bq^2) \\ &= (ap^2 + bq^2)^2 - 4abqN.\end{aligned}$$

Hence we get

$$(ap^2 - bq^2)^2 = (ap^2 + bq^2)^2 - 4abqN. \tag{1}$$

Now, consider

$$\begin{aligned}S^2 - 4abqN &= (ap^2 + bq^2 + x)^2 - 4abqN \\ &= (ap^2 + bq^2)^2 + 2x(ap^2 + bq^2) + x^2 - 4abqN.\end{aligned}$$

Using (1), we can rewrite the above equation as

$$S^2 - 4abqN = (ap^2 - bq^2)^2 + 2x(ap^2 + bq^2) + x^2. \tag{2}$$

Suppose $|ap^2 - bq^2| < N^{1/2}$. Hence, using $|x| < \frac{1}{3}N^{1/3-\alpha}$, then (2) becomes

$$\begin{aligned}|S^2 - 4abqN| &< (N^{1/2})^2 + 2|x|N^{2/3+\alpha} + x^2 \\ &< N + 2(\frac{1}{3}N^{1/3-\alpha})N^{2/3+\alpha} + (\frac{1}{3}N^{1/3-\alpha})^2 \\ &= N + \frac{2}{3}N + \frac{1}{9}N^{2/3-2\alpha} \\ &= N(1 + \frac{2}{3} + \frac{1}{9}N^{-1/3-2\alpha}) \\ &< 2N\end{aligned}$$

Thus, we have $|S^2 - 4abqN| < 2N$. If we divide $|S^2 - 4abqN|$ by $4N$, then $\frac{S^2}{4N} - abq < \frac{2N}{4N} = \frac{1}{2}$. It follows that $abq = \left\lfloor \frac{S^2}{4N} \right\rfloor$. ■

Lemma 5. Let $N = p^2q$ with $q < p < 2q$. Let a, b be integers with $\gcd(a, b) = 1$ such that $ap^2 + bq^2 = N^{2/3+\alpha}$ with $\alpha < \frac{1}{3}$. Let e be a public exponent satisfying the equation $eX - (N - (ap^2 + bq^2))Y = Z$ with $\gcd(X, Y) = 1$. If $|Z| < \frac{1}{3}N^{1/3+\alpha}Y$ and $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$, then $\frac{Y}{X}$ is a convergent of continued fraction $\frac{e}{N}$.

Proof. Set $ap^2 + bq^2 = N^{2/3+\alpha}$ with $\alpha < \frac{1}{3}$. Rearrange the equation $eX - (N - (ap^2 + bq^2))Y = Z$ as

$$eX - NY = Z - (ap^2 + bq^2)Y. \tag{3}$$

Now, suppose $|Z| < \frac{1}{3}N^{1/3+\alpha}Y$ and $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$. If we divide (3) by NX then we get

$$\begin{aligned}\left|\frac{e}{N}-\frac{Y}{X}\right| &= \left|\frac{Z}{NX}-\frac{(ap^2+bq^2)Y}{NX}\right| \\ &\leq \left|\frac{Z}{NX}\right|+\frac{(ap^2+bq^2)Y}{NX} \\ &\leq \left|\frac{Z}{NX}\right|+\frac{(ap^2+bq^2)X}{NX} \\ &< \frac{\frac{1}{3}N^{1/3+\alpha}X}{NX}+\frac{N^{2/3+\alpha}X}{NX} \\ &< N^{-2/3+\alpha}+N^{-1/3+\alpha} \\ &< 2N^{-1/3+\alpha}\end{aligned}$$

Observe that, for $X < \frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$ then $\left|\frac{e}{N}-\frac{Y}{X}\right| < \frac{1}{2X^2}$. Hence by Theorem 1, $\frac{Y}{X}$ is a convergent of continued fraction $\frac{e}{N}$.■

Theorem 8. Let $N = p^2q$ with $q < p < 2q$. Let a, b be integers with $\gcd(a, b) = 1$ such that such that $|ap^2 - bq^2| < N^{1/2}$. Let e be a public exponent satisfying the equation $eX - (N - (ap^2 + bq^2))Y = Z$ with $\gcd(X, Y) = 1$. Set $ap^2 + bq^2 = N^{2/3+\alpha}$ with $\alpha < \frac{1}{3}$. If $|Z| < \frac{1}{3}N^{1/3+\alpha}Y$ and $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$, then N can be factored in polynomial time.

Proof. Suppose $|Z| < \frac{1}{3}N^{1/3+\alpha}Y$ and $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$ with $\gcd(X, Y) = 1$. Hence by Lemma 5, $\frac{Y}{X}$ is a convergent of continued fraction $\frac{e}{N}$. Rearrange (3) as $(ap^2+bq^2)Y-NY+eX = Z$. Dividing by Y, we get

$$(ap^2 + bq^2) - N + \frac{eX}{Y} = \frac{Z}{Y}. \tag{4}$$

Set $S = \frac{N-eX}{Y}$. Then (4) can be written as $(ap^2 + bq^2) - S = \frac{Z}{Y}$. Hence, we have $|(ap^2 + bq^2) - S| = \frac{|Z|}{Y} < |Z| < \frac{1}{3}N^{1/3+\alpha}$. By Lemma 4, if $|ap^2 - bq^2| < N^{1/2}$ and $|ap^2 + bq^2 - S| < \frac{1}{3}N^{1/3-\alpha}$ then $\left\lfloor \frac{S^2}{4N} \right\rfloor = abq$. It follows that we obtained $q = \gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right)$.■

According to Theorem 8, we design the following algorithm to obtain the prime factor of $N = p^2q$ as follows.

Algorithm 2.

INPUT: The public key modulus (N, e) satisfying $N = p^2q$ and Theorem 6.
OUTPUT: The prime factors p, q.

1. Compute the continued fraction $\frac{e}{N}$.
2. For each convergent $\frac{Y}{X}$ of $\frac{e}{N}$, compute $S = \frac{N-eX}{Y}$.
3. Compute $\left\lfloor \frac{S^2}{4N} \right\rfloor$.
4. Compute $h = \gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right)$.
5. If $1 < h < N$, then stop.

5. Conclusion

This paper shows two new attacks on RSA-type modulus of $N = p^2q$ using continued fractions. The first attack we note that $1 < e < \phi(N) < N - (2N^{2/3} - N^{1/3})$ is a good approximation of $\phi(N)$ leading to get d satisfying $2p^{5/3}|p^{1/3} - q^{1/3}| < \frac{1}{3}N^{\beta}$ and $d < N^{\delta}$. With this result, we come up with an algorithm for factoring $N = p^2q$, as we described in Algorithm 1.

Concerning to the second attack with e satisfying the equation $eX - (N - (ap^2 + bq^2))Y = Z$ such that $|ap^2 - bq^2| < N^{1/2}$, then we show that this result also can find the primes factor of N in polynomial time fulfilling the condition $ap^2 + bq^2 = N^{2/3+\alpha}$ with $0 < \alpha < \frac{1}{3}$, $|Z| < \frac{1}{3}N^{1/3+\alpha}Y$ and $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{6}-\frac{\alpha}{2}}$.

Acknowledgement
The authors would like to thank the Ministry of Education, Malaysia for research funding. The authors also would like to thank Prof. Dr. Abderrahmane Nitaj from the Laboratoire de Mathématiques, Université de Caen, France, for valuable comments and discussion.

References

[1] May A 2004 Secret exponent Attacks on RSA-type schemes with moduli $N = p^r q$ In PKC 2004 *LNCS* **2947** Springer-Verlag pp. 218-230.
[2] Menezes A, van Oorschot C, and Vanstone 1997 *A Handbook of Applied Cryptography* CRC Press Washington.
[3] Nitaj A 2009 Cryptanalysis of RSA using the Ratio of the Primes In Preneel B. (ed.): Progress in Cryptology-AFRICACRYPT 2009 *LNCS* **5580** Springer-Verlag pp. 98-115.
[4] Nitaj A 2013 *Diophantine and Lattice Cryptanalysis of the RSA Cryptosyste*m Springer-Verlag pp. 139-168.
[5] de Weger B 2002 Cryptanalysis of RSA with Small Prime Difference *Applicable Algebra in Engineering Communication and Computing* **13**(1) pp. 1728.
[6] Chen C Y, Hsueh C C and Lin Y F 2009 A Generalization of de Wegers Method In the *5th IAS/IEEE International Conference on Information Assurance and Security (IAS 2009)* pp. 344-347.
[7] Coppersmith D 1997 Small Solutions to Polynomial Equations and Low Exponent RSA Vulnerabilities *J. of Cryptology* **10**(4) Springer-Verlag pp. 233-260.
[8] Blömer J and May A 2004 A Generalized Wiener Attack on RSA *Practice and Theory in Public Key Cryptography PKC 2004 LNCS* **2947** Springer-Verlag pp. 113.
[9] Asbullah M A and Ariffin M R K 2014 Rabin-*p* Cryptosystem: Practical and Efficient Method for Rabin based Encryption Scheme *arXiv preprint (2014).* Available at http://arxiv.org/abs/1411.4398.
[10] Wiener M J 1990 Cryptanalysis of Short RSA Secret Exponents *IEEE Trans. on Information Theory* **IT-36** pp. 553-558.
[11] Nishioka M, Satoh H and Sakurai K 2001 Design and Analysis of Fast Provably Secure Public-Key Cryptosystems based on a Modular Squaring *Information Security and CryptologyICISC 2001 LNCS* **2288** Springer-Berlin Heidelberg pp 81-102.
[12] Ariffin M R K, Asbullah M A, Abu N A and Mahad Z 2013 A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of $N = p^2q$ *Malaysian Journal of Mathematical Sciences* **7**(S) pp. 19-37.
[13] Rivest R L, Shamir A and Adleman L M 1978 A Method for Obtaining Digital Signatures and Public-Key Cryptosystems *Comm. of the ACM* **21**(2) pp. 120-126.
[14] Maitra S and Sarkar S 2008 Revisiting Wieners Attack - New Weak Keys in RSA *ISC 2008 LNCS* **5222** Springer-Verlag pp. 228-243.
[15] Takagi T 1998 Fast RSA-type Cryptosystem Modulo $p^k q$. *Advances in Cryptology Crypto98 LNCS* **1462** Springer-Verlag pp. 318 326.