Caliphate Journal of Science & Technology (CaJoST)

ISSN: 2705-313X (**PRINT**); 2705-3121 (**ONLINE**) **Research Article**

Article Info

Received: 13th January 2019

Revised: 4th March 2019

Accepted: 8th March 2019

[1]Department of Mathematics, Sokoto State University, Sokoto Nigeria
[2]Department of Mathematics, Usmanu Danfodiyo University, Sokoto Nigeria
[3]Department of Mathematics, Umaru Ali Shinkafi Polytechnic Sokoto

***Corresponding author's email:** sadiqshehuzezi@gmail.com,

Cite this: *CaJoST*, 2019, 1, 83-90

New Approach on RSA Prime Power N = p^2q using a Continued Fraction

Sadiq Shehu[1]*, Aminu A. Ibrahim[2], Buhari A. Ibrahim[3]

RSA Cryptosystem is an interesting area in mathematics. In this paper we propose two new approach on RSA prime power N = p^2q using continued fraction. Our first approach is based on the RSA equation $ed = 1 + k\phi(N)$ $where$ ϕ(N) = $(p^2-1)(q^2-1)$. Assuming that q < p < 2q, public key e < $(p^2-1)(q^2-1)$ and private key d < $\frac{1}{2}N^{1/3}$, we show that $\frac{k}{d}$ can be recovered among the convergent of the continued fraction expansion of $\frac{e}{N^{4/3}}$. Our Second approach is based on the same RSA equation and public key e. Assuming that q < p < 2q and approximation p_o^2 of p^2 $with$ $|p^2 - p_o^2| < \frac{1}{2}N^{2\alpha}$ and private key exponent d satisfies d < $N^{\frac{1-2\alpha}{2}}$, we show that $\frac{k}{d}$ can be recovered among the convergent of the continued fraction expansion of $\frac{e}{N^{4/3}+1-P}$.

Keywords: RSA prime power, Factorization, Diophantine approximations, Continued fractions, Convergent

1. Introduction

The RSA cryptosystem was created in 1977 [1]. It has become fundamental to e-commerce and is widely used to secure communication in the internet and ensure confidentiality and authenticity of e-mails. The RSA cryptosystem is based on the generation of two random prime numbers, p and q of equal bit-size and generation exponent d and e which are called public key and private key. The public key and the private key in this cryptosystem consist of the value N which is called the modulus where value e is called public exponent and d is called private exponent. That is the RSA cryptosystem setup involves randomly selecting two large prime numbers p, q whose product $N = pq$ is known as the RSA modulus and a public tuples (N, e) is used in encrypting message where e is generated and a private key tuples (N, d) which is used in decrypting the cipher text . The two parameters e, d have a relation in the form of $ed = 1(mod\emptyset(N))$ where $\phi(N) = (p-1)(q-1)$ is called Euler totient function of N.

RSA Algorithm can be generated by the following steps:

a) Generate a pair of large random prime number p and q.
b) Compute the modulus N i.e. $N = pq$.
c) Compute the $\phi(n) = (p-1)(q-1)$.
d) Choose an integer e such that 1< e < $\phi(N)$ and e is mutually prime to $\phi(N)$ i.e. e and $\phi(N)$ share no facter than one.
e) Compute d to satisfy the congruence relation $ed \equiv 1(mod\phi(N))$ i.e. $de = k\phi(N) + 1$ for some integer k where d is kept as the private key exponent.

2. Continued fraction

A continued fraction is important in many branches of mathematics. They arise naturally in long division and in the theory of approximation to real numbers by rationales. These objects that are related to number theory help us to find good approximations for real life constants. In mathematics, a continued fraction is an expression obtained through an iteration process of representing a number as the sum of its integer part and reciprocal of another number. In a finite continued fraction or (terminal continued fraction). The iteration/recursion is terminated after finitely many steps using an integer in lieu of another continued fraction. In contract, an infinite continued fraction is an infinite expression (Magnus 1962).

Definition 1.1 Continued fraction: A continued fraction expression of a number is formed by subtracting away the integer part of it and inverting the remainder and then repeating this process.

Definition 1.2 Finite continued fraction is a continued fraction with finite number of a terms donated by

$$a_o + \frac{1}{a_1 + \frac{1}{a_2 + \cdots \frac{1}{a_n}}} .$$

Definition 1.3 Infinite continued fraction is a continued fraction with infinite number of a terms donated by.

$$a_o + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}} .$$

RSA cryptosystem is a mathematical discipline that has a great application to various fields.

Wiener [2] presented an attack on RSA that solves the key equation and factors N if d is sufficiently small, namely d < $\frac{1}{3}N^{0.25}$. Wiener's attack consist on finding $\frac{k}{d}$ among the convergent of the continued fraction expansion of $\frac{e}{N}$ and then using $\frac{k}{d}$ to factor N. Wiener's attack on RSA has been extended in many ways using lattice reduction and Coppersmiths method.

Kuwakado *et al* [3] presented a scheme based on using RSA modulus N = pq and a singular cubic equation with equation $y^2 = x^2 + bx^2 \bmod N$ where a message M = (m_x ,m_y) is represented as a point on the singular cubic equation . In this system, the public exponent e and the private exponent d satisfy an equation of the form $de - k(p^2-1)(q^2-1)$.

Coppersmiths [4] presented a method which enables us to factor the modulus N = pq in time polynomial in its bit size provided that we know half of the bits of p. The original method is based in small roots of bivariate polynomial equations. He presented a variant which is based on uninvariate modular polynomial equations.

Takagi [5] proposed the first Multi-power RSA variant with a modulus of the form $N = p^s q$, where s > 1. Using Hensel lifting and Chinese remaindering, Takagi showed that decryption can be done much more efficiently as compared to normal RSA decryption.

Boneh and Durfee [6], introduced the small inverse problem and presented a substantial improvement over Wiener's bound. Their attack can recover the primes p, q in polynomial time provided that d < $N^{0.292}$. Their result is based on Coppersmith's technique for finding small solutions to modular polynomial equations. They present a weaker result which is valid for d < $N^{0.284}$. The used of short exponent encounters serious security problem in various instance of RSA. As the work that has been proposed by Howgrave-Graham and Seifert in [7] showed an extension of Wiener's attack that allows the RSA system to be insure in the presence of two decryption exponent (d_1,d_2) with d_1,d_2 <$N^{5/14}$. In the presence of three decryption exponent, they improved the bound to $N^{2/5}$.

De-weger. [8] proposed a generalization of Wiener attack on RSA De-weger extended Wiener bound $\frac{\sqrt{6\sqrt{2}}}{6}N^{1/4}$ to d < $\frac{N^{3/4}}{|p-q|}$ which is equivalent with Wiener bound for standard RSA that for $|p-q| = \partial(N^{1/2})$.

Blömer and May. [9], improved upon wiener's result by showing that every public exponent e satisfying an equation $ed - k\emptyset(N) = y$ with suitable bound for x and y yield the factorization of N. showed that using such exponent make RSA insure if N = pq with p – q = $CN^{1/2}$ for some constant $O < C \leq 1$ and $O \leq x \leq \frac{1}{3}\sqrt{\frac{\emptyset(N)}{e}}$ $\frac{N^{3/4}}{|p-q|}$ and $|Z| \leq \frac{p-q}{\emptyset(N)N^{1/4}}$ex .

Nassr *et al.* [10], showed that if N = pq be an RSA modulus with q < p < 2q. Suppose we know an approximation p_o of p with $|p - p_o| < \frac{1}{8}N^{\alpha}$ presented a continued fraction attack on RSA with a private exponent satisfying $d < N^{1-\alpha/2}$.

Maitra and Sarka [11], considered the case that p and 2q are too close. That means the difference between 2q and p is small. They used $N = \frac{3}{2}\sqrt{N}+1$ as a good approximation to $\phi(N)$ instead of N. Hence in their studied revealed that $\frac{k}{d}$ is one of the convergent of the continued fraction expansion of $\frac{e}{N-\frac{3}{2}\sqrt{N}+1}$.

Ariffin *et al* [12] showed that for any efficient algorithm able to factor the modulus $A_2 = p^2 q$ then such algorithm also to solve AA_{β} function.

Furthermore, they also proved that the $AA_{\beta}\, function$ can be solved if there exist algorithm that can solved the bivariate function hard problem.

AA_{β} Cryptosystem [13], Incorporating the hardness of factoring integer N = p^2q coupled with the square root problem as its cryptographic primitive which gives advantage for encryption without 'expansive' mathematically operation. Recently, by incorporating the modulus N = p^2q, a variant of Rabin cryptosystem successfully eliminated the decryption failure which was due to a 4-to-1 mapping Scenario.

Asbullah and Ariffin [14] proposed new attack on RSA types modulus N = p^2q using the term $N - (2N^{2/3} - N^{1/3})$ as a good approximation to $\phi(N)$ satisfying the equation $ed - k\phi(N) = 1$. Hence, they showed that $\frac{k}{d}$ is one of the convergent of the continued fraction expansion of $\frac{e}{N-(2^{2/3}-N^{1/3}}$ and later led to the factorization of N = p^2q in polynomial time .

Bunder and Tonien [15] **p**resented an attack that solves the former equation when d satisfies d < $\sqrt{\frac{2N^3-18N^2}{e}}$. The attack which is related to Wiener attack on RSA based on applying the continued fraction algorithm to find $\frac{k}{d}$ among the convergent of the continurd fraction expansion of $\frac{e}{N^2-\frac{9}{4}N+1}$.

Isah *et al*. [16] presented some result where they established that if the short decryption exponent $d < \sqrt{\frac{a^j+b^j}{2}}\left(\frac{N}{e}\right)^{1/2} N^{0.375}$ then $\frac{k}{d}$ can be found from the convergent of the continurd fraction expansion of $\frac{e}{N}$, where

N_1 = N$\left[\left(\frac{a^{j/i}+b^{j/i}}{(2ab)^{j/2i}} + \frac{a^{1/j}+b^{1/j}}{(2ab)^{1/2j}}\right)\sqrt{N}\right]$+1, and a, b, i, j are small positive integer less than log N which lead to the factorization of N in polynomial times.

Theorem 2.2

Let x be a real positive number. If a and b are positive integers such that

$$\gcd(a,b) = 1 \; and$$

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$$

Then $\frac{a}{b}$ is one of the convergents of the continued fraction expansion of x.

3. Results

Lemma. 3.1

Let $N = p^2q$ to be an RSA modulus with $q < p < 2q$ then$2^{-2/3}N^{1/3} < q < N^{1/3} < p < 2^{1/3}N^{1/3}$ and $2N^{2/3} < p^2 + q^2 <(2^{2/3} + 2^{-4/3}\text{-}2^{1/6} +2)N^{2/3}$

Proof

Let $N = p^2q$

and $q < p < 2q$ (3.1)

Now, multiply by p^2 to both side of equation (3.1)

$We\ have\ \ p^2q < pp^2 < 2p^2q$ since $N = p^2q$ then

$N < p^3 < 2N$ (3.2)

Now, by taking cube root of the both side of equation (3.2) we have

$\sqrt[3]{N} < p < \sqrt[3]{2}\sqrt[3]{N} \Rightarrow\ N^{1/3} < p < 2^{1/3}N^{1/3}$ (3.3)

Taking the square of both side of equation (3.3) we get

$N^{2/3} < p^2 < 2^{2/3}N^{2/3}$ (*)

Since $N = p^2q \Rightarrow p^2 = \frac{N}{q}$ (3.4)

Now using equation (3.4) into (*)

$N^{2/3} < \frac{N}{q} < 2^{2/3}N^{2/3}$

Taking the reciprocal we have that

$\Rightarrow \frac{1}{2^{2/3}N^{2/3}} < \frac{q}{N} < \frac{1}{N^{2/3}}$

Now multiply through by N

$\frac{N}{2^{2/3}N^{2/3}} < \frac{qN}{N} < \frac{N}{N^{2/3}}$

$\frac{N}{2^{2/3}N^{2/3}} < q < \frac{N}{N^{2/3}}$

$\frac{1}{2^{2/3}N^{-1/3}} < q < \frac{1}{N^{-1/3}}$

Hence, $2^{-2/3}N^{1/3} < q < N^{1/3}$ (3.5)

Secondly Observe that

$(p^2+q^2)^2 = (p^2-q^2)^2+4N^{4/3}$ (3.6)

$\therefore (p^2+q^2)(p^2+q^2) = (p^2-q^2)(p^2-q^2)+ 4N^{4/3}$

$p^4+p^2q^2+p^2q^2+q^4 = p^4-p^2q^2-p^2q^2+q^4+4N^{4/3}$

$\therefore p^4+2p^2q^2+q^4 = p^4-2p^2q^2+q^4+4N^{4/3}$

But since $N = p^2q$

$p^4+2Nq+q^4 = p^4-2Nq+q^4+4N^{4/3}$

But from equation (3.5) $q < N^{1/3}$

$p^4+2NN^{1/3}+q^4 = p^4-2NN^{1/3}+q^4+4N^{4/3}$

$\Rightarrow p^4+2N^{4/3}+q^4 = p^4-2N^{4/3}+q^4+4N^{4/3}$

$left\ handside = right\ handside$

$(p^2+q^2)^2 = (p^2-q^2)^2+4N^{4/3}$

Then it follows that $(p^2-q^2)^2+4N^{4/3} > 0+4N^{4/3}$ where $(p^2-q^2)^2>0$

$(p^2+q^2)^2) > 4N^{4/3} \Rightarrow (p^2+q^2) > \sqrt{4}\sqrt{N^{4/3}}$

$Then\ (p^2+q^2) > 2\sqrt{N^{4/3}} = 2N^{\frac{4}{6}}$

$p^2+q^2 > 2N^{2/3}$ (**)

Recall equation (3.3) and multiply through by -1

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

$\Rightarrow -N^{1/3} < -q < -2^{-2/3}N^{1/3}$ (3.7)

Add equation (3.3) and (3.7)

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

But since $(p^2+q^2)^2 = (p^2-q^2)^2 + 4N^{4/3}\ from\ equation\ (3.6)$

$(p^2-q^2)^2+4N^{4/3} = (2^{2/3}N^{2/3}-2^{-4/3}N^{2/3})^2+4N^{4/3}$

$\Rightarrow (p^2+q^2)^2 = (2^{2/3}N^{2/3}-2^{-4/3}N^{2/3})^2+4N^{4/3}$

$= (2^{2/3}N^{2/3}-2^{-4/3}N^{2/3})(2^{2/3}N^{2/3}-2^{-4/3}N^{2/3})+4N^{4/3}$

$= (2^{4/3}N^{4/3}-2^{-2/3}N^{4/3}-2^{-2/3}N^{4/3}+2^{-8/3}N^{4/3}+4N^{4/3})$

$= (2^{4/3}-2^{-2/3}-2^{-2/3}+2^{-8/3}+4)\ N^{4/3}$

$= (2^{4/3}-\left(\frac{1}{2^{\frac{2}{3}}}+\frac{1}{2^{\frac{2}{3}}}\right)+2^{-8/3}+4)\ N^{4/3}$

$= (2^{4/3}-\frac{2}{2^{\frac{2}{3}}}+2^{-8/3}+4)\ N^{4/3}$

$= (2^{4/3}-2\times 2^{-2/3}+2^{-8/3}+4)\ N^{4/3}$

$= (2^{4/3}-2^{-2/3+1}+2^{-8/3}+4)\ N^{4/3}$

$= (2^{4/3}-2^{1/3}+2^{-8/3}+4)\ N^{4/3}$

$(p^2+q^2)^2 = (2^{4/3}-2^{1/3}+2^{-8/3}+4)\ N^{4/3}$

$\Rightarrow p^2+q^2 = (2^{4/6}-2^{1/6}+2^{-8/6}+4^{1/2})\ N^{4/6}$

$p^2+q^2 = (2^{2/3}-2^{1/6}+2^{-4/3}+2)\ N^{2/3}$ (3.8)

$p^2+q^2 < (2^{2/3}-2^{1/6}+2^{-4/3}+2)\ N^{2/3}$

Finally, by comparing equation (**) and (3.8) we have that

$2N^{2/3} < p^2+q^2 < (2^{2/3}-2^{1/6}+2^{-4/3}+2)\ N^{2/3}$.

Theorem: **3.2**

Let $N = p^2q$ be an RSA modulus with $q < p < 2q$ let e < $(p^2-1)(q^2-1)$ be a public exponent and *d* be the corresponding private key if $d < \frac{1}{2}N^{1/3}$ then we can find the factorization of N in polynomial time.

Proof

We write the equation ed = 1+k$[(p^2-1)(q^2-1)] = (Nq+1-(p^2+q^2))$.

But since N= p^2q and ed = 1+k$(Nq+1-(p^2+q^2))$ then by lemma 3.1 $q < N^{1/3}$

ed = 1+k$\left(NN^{1/3}+1-(p^2+q^2)\right)$

ed = 1+k$\left(N^{4/3}+1-(p^2+q^2)\right) \Rightarrow$ ed = 1 + k $N^{4/3}+k-k(p^2+q^2)$

e$d-kN^{4/3}$ = 1$-k(p^2+q^2-1)$

Now divided through by $N^{4/3}d$

$\frac{ed}{dN^{4/3}}-\frac{kN^{4/3}}{dN^{4/3}} = \frac{1-k(p^2+q^2-1)}{N^{4/3}d} \Rightarrow \frac{e}{N^{4/3}}-\frac{k}{d} = \frac{1-k(p^2+q^2-1)}{N^{4/3}d}$

$\left|\frac{e}{N^{4/3}}-\frac{k}{d}\right| = \frac{|1-k(p^2+q^2-1)|}{N^{4/3}d} \Rightarrow \left|\frac{e}{N^{4/3}}-\frac{k}{d}\right| = \frac{k(p^2+q^2-1)-1}{N^{4/3}d}$

$= \frac{k(p^2+q^2-1)}{N^{4/3}d} - \frac{1}{N^{4/3}d} < \frac{k(p^2+q^2-1)}{N^{4/3}d}$ which show that

$\left|\frac{e}{N^{4/3}} - \frac{k}{d}\right| < \frac{k(p^2+q^2-1)}{N^{4/3}\ d}$ (3.9)

But since we let e < $(p^2-1)(p^2-1)$ and $ed-1$ = k$(p^2-1)(p^2-1)$ them we write

$\frac{ed-1}{(p^2-1)(p^2-1)} = \frac{k\,(p^2-1)(p^2-1)}{(p^2-1)(p^2-1)}$

$k = \frac{ed-1}{(p^2-1)(p^2-1)} = \frac{ed}{(p^2-1)(p^2-1)} - \frac{1}{(p^2-1)(p^2-1)} < \frac{ed}{(p^2-1)(p^2-1)}$ which shows that

$k < \frac{ed}{p^2-1)(p^2-1)}$ but since we let e < $(p^2-1)(p^2-1)$

$\Longrightarrow k < \frac{k\,(p^2-1)(p^2-1)}{(p^2-1)(p^2-1)} = d$. Hence

$k < d$ (3.10)

Using equation (3.10) into (3.9) we get

$\left|\frac{e}{N^{4/3}} - \frac{k}{d}\right| < \frac{d(p^2+q^2-1)}{N^{4/3}d} = \frac{(p^2+q^2-1)}{N^{4/3}} = \frac{p^2+q^2}{N^{4/3}} - \frac{1}{N^{4/3}} < \frac{p^2+q^2}{N^{4/3}}$ (3.11)

by lemma 3.1 $p^2+q^2 > 2N^{2/3}$

$\left|\frac{e}{N^{4/3}} - \frac{k}{d}\right| < \frac{p^2+q^2}{N^{4/3}} = \frac{2N^{2/3}}{N^{4/3}} = \frac{2}{N^{4/3-2/3}} = \frac{2}{N^{2/3}}$

$\Rightarrow \left|\frac{e}{N^{4/3}} - \frac{k}{d}\right| < \frac{2}{N^{2/3}} = 2N^{-2/3}$

$\left|\frac{e}{N^{4/3}} - \frac{k}{d}\right| < 2N^{-2/3}$ (3.12)

Now suppose$d < \frac{\sqrt{4}}{4}N^{2/6}$, taking the square of the both side

$d^2 < \frac{4}{16}N^{2/3} \Longrightarrow d^2 < \frac{1}{4}N^{2/3} \Longrightarrow \frac{4}{N^{2/3}} < \frac{1}{d^2} \Rightarrow 4N^{-2/3} < \frac{1}{d^2}$

$= \frac{1}{2}\,4N^{-2/3} < \frac{1}{2d^2} \Rightarrow 2N^{-2/3} < \frac{1}{2d^2}$ (3.13)

$\left|\frac{e}{N^{4/3}} - \frac{k}{d}\right| < 2N^{-2/3} < \frac{1}{2d^2}$

$\left|\frac{e}{N^{4/3}} - \frac{k}{d}\right| < \frac{1}{2d^2}$.

Then by Theorem 2.2 $\frac{k}{d}$ *is one of the convergents of the continued fraction expansion of* $\frac{e}{N^{4/3}}$.

Theorem 3.3

Let N= p^2q *be an RSA* modulus with $q < p < 2q$ Suppose we know an approximation p_o^2 of p^2 with $|p^2 - p_o^2| < \frac{1}{2}N^{2\alpha}$ let e be a public exponent if the corresponding private exponent d satisfies $d < N^{\frac{1-2\alpha}{2}}$ then N can be factored in time polynomial in log N.

Proof

Let $c^2 = \frac{1}{2}$ Suppose we know $p_o^2 > N^{1/3}$ and $\alpha \ni |p^2 - p_o^2| < c^2N^{2\alpha}$ then by absolute value we have $-c^2N^{2\alpha} < |p^2 - p_o^2| < c^2N^{2\alpha}$ (3.14)

By separating equation (3.14) we have

$-c^2N^{2\alpha} < |p^2 - p_o^2|$

and $|p^2 - p_o^2| < c^2N^{2\alpha}$ (3.15)

So if we add (3.15) together we get

$-c^2N^{2\alpha} < |p^2 - p_o^2| \Rightarrow -c^2N^{2\alpha} < |p^2| - |p_o^2|$

$-c^2N^{2\alpha} < p^2 - p_o^2 \Rightarrow p_o^2 - c^2N^{2\alpha} < p^2$ (3.16)

And $|p^2| - |p_o^2| < c^2N^{2\alpha} \Rightarrow p^2 - P_O^2 < c^2N^{2\alpha} \Rightarrow P^2 < p_o^2 + c^2N^{2\alpha}$ (3.17)

by comparing (3.16) and (3.17) we have

$p_o^2 - c^2N^{2\alpha} < p^2 < p_o^2 + c^2N^{2\alpha}$ (3.18)

But since $N = p^2q \Rightarrow p^2 = \frac{N}{q}$ (3.19)

Using (3.19) into (3.18)

$p_o^2 - c^2N^{2\alpha} < \frac{N}{q} < p_o^2 + c^2N^{2\alpha}$ Which can be rewrite as

$\frac{1}{p^2+c^2N^{2\alpha}} < \frac{q}{N} < \frac{1}{p^2-c^2N^{2\alpha}} \Rightarrow \frac{N}{p^2+c^2N^{2\alpha}} < \frac{qN}{N} < \frac{N}{p^2-c^2N^{2\alpha}} = \frac{N}{p^2+c^2N^{2\alpha}} < q < \frac{N}{p^2-c^2N^{2\alpha}}$ (3.20)

Using the result of lemma 3.1 and (3.20) we get

$\frac{Nq}{p^2+c^2N^{2\alpha}} < q^2 < \frac{Nq}{p^2-c^2N^{2\alpha}}$ (3.21)

Substituting (3.21) into (3.20)

$\frac{NN^{1/3}}{p^2+c^2N^{2\alpha}} < q^2 < \frac{NN^{1/3}}{p^2-c^2N^{2\alpha}} \Rightarrow \frac{N^{4/3}}{p^2+c^2N^{2\alpha}} < q^2 < \frac{N^{4/3}}{p^2-c^2N^{2\alpha}}$ (3.22)

Then it follows that by adding equation (3.18) and (3.22)

$p_o^2 + \frac{N^{4/3}}{p^2+c^2N^{2\alpha}} - c^2N^{2\alpha} < p^2 + q^2 < p_o^2 + \frac{N^{4/3}}{p^2-c^2N^{2\alpha}} + c^2N^{2\alpha}$ (3.23)

Let $P = p^2 + q^2$ be define as a mean value then equation (3.23) becomes

$p_o^2 + \frac{N^{4/3}}{p^2+c^2N^{2\alpha}} - c^2N^{2\alpha} < P < p_o^2 + \frac{N^{4/3}}{p^2-c^2N^{2\alpha}} + c^2N^{2\alpha}$ (3.24)

From equation (3.24) we get

$p_o^2 + \frac{N^{4/3}}{p^2+c^2N^{2\alpha}} - c^2N^{2\alpha} < P \; and$ (3.25)

$P < p_o^2 + \frac{N^{4/3}}{p^2-c^2N^{2\alpha}} + c^2N^{2\alpha}$ (3.26)

Adding (3.24) and (3.26) since we let $P = p^2 + q^2 \; to \; be \; define \; as \; a \; mean \; value$

$P = \frac{1}{2}\left(2p_o^2 + \frac{N^{4/3}}{p_o^2+c^2N^{2\alpha}} - c^2N^{2\alpha} + c^2N^{2\alpha} + \frac{N^{4/3}}{p_o^2-c^2N^{2\alpha}}\right)$

$= \frac{1}{2}\left(2p_o^2 + \frac{N^{4/3}}{p_o^2+c^2N^{2\alpha}} + \frac{N^{4/3}}{p_o^2-c^2N^{2\alpha}}\right)$

$= \frac{1}{2}\left(2p_o^2 + \frac{N^{4/3}(p_o^2-c^2N^{2\alpha})+N^{4/3}(p_o^2+c^2N^{2\alpha})}{(p_o^2+c^2N^{2\alpha})(p_o^2-c^2N^{2\alpha})}\right)$

$= \frac{1}{2}\left(2p_o^2 + \frac{N^{4/3}p_o^2-N^{4/3}c^2N^{2\alpha}+N^{4/3}p_o^4+N^{4/3}c^2N^{2\alpha}}{p_o^4-p_o^2c^2N^{2\alpha}+p_o^2c^2N^{2\alpha}-c^4N^{4\alpha}}\right)$

$= \frac{1}{2}\left(2p_o^2 + \frac{N^{4/3}p_o^2+N^{4/3}p_o^2}{p_o^4-c^4N^{4\alpha}}\right)$

$P = \frac{1}{2}\left(2p_o^2 + \frac{2N^{4/3}p_o^2}{p_o^4-c^4N^{4\alpha}}\right) = \left(\left(p_o^2 + \frac{N^{4/3}p_o^2}{p_o^4-c^4N^{4\alpha}}\right)\right)$

$= p_o^2 + \frac{N^{4/3}p_o^2}{p_o^4-c^4N^{4\alpha}}$ (3.27) we can rewrite

$P = p^2 + q^2 \;\; as \;\; p^2 + q^2 - P > 0$

Therefore equation ((3.27) becomes

$p_o^2 + \frac{N^{4/3}}{p^2+c^2N^{2\alpha}} - c^2N^{2\alpha} < p^2 + q^2 - P < p_o^2 + \frac{N^{4/3}}{p^2-c^2N^{2\alpha}} + c^2N^{2\alpha}$

$p^2 + q^2 - P < \frac{1}{2}\left(p_o^2 + \frac{N^{4/3}}{p^2-c^2N^{2\alpha}} + c^2N^{2\alpha} - p_o^2 - \frac{N^{4/3}}{p^2+c^2N^{2\alpha}} + c^2N^{2\alpha}\right)$

$|p^2 + q^2 - P| < \left(\frac{1}{2}\left(\frac{N^{4/3}}{p_o^2 - c^2N^{2\alpha}} - \frac{N^{4/3}}{p_o^2 + c^2N^{2\alpha}} + 2c^2N^{2\alpha}\right)\right)$

$= \frac{1}{2}\left(\frac{N^{4/3}(p_o^2+c^2N^{2\alpha})-N^{4/3}(p_o^2-c^2N^{2\alpha})}{(p_o^2+c^2N^{2\alpha})(p_o^2-c^2N^{2\alpha})} + 2c^2N^{2\alpha}\right)$

$= \frac{1}{2}\left(\frac{N^{4/3}p_0^2+N^{4/3}c^2N^{2\alpha}-N^{4/3}p_o^2+N^{4/3}c^2N^{2\alpha}}{(p_o^4+p_o^2c^2N^{2\alpha}-p_o^2c^2N^{2\alpha}-c^2N^{2\alpha})} + 2c^2N^{2\alpha}\right)$

$= \frac{1}{2}\left(\frac{N^{4/3}c^2N^{2\alpha}+N^{4/3}c^2N^{2\alpha}}{p_o^4-c^4N^{4\alpha}} + 2c^2N^{2\alpha}\right)$

$= \frac{1}{2}\left(\frac{2N^{4/3}c^2N^{2\alpha}}{p_o^4-c^4N^{4\alpha}} + 2c^2N^{2\alpha}\right)$

$= \frac{N^{4/3}c^2N^{2\alpha}}{p_o^4-c^4N^{4\alpha}} + c^2N^{2\alpha}$

$\Rightarrow |p^2 + q^2 - P| < \frac{N^{4/3}c^2N^{2\alpha}}{p_o^4-c^4N^{4\alpha}} + c^2N^{2\alpha}$ (3.28)

Recall equation (3.18)

$p_o^2 - c^2N^{2\alpha} < p^2 < p_o^2 + c^2N^{2\alpha}$ and by lemma 3.1 we have $N^{1/3} < p < 2^{1/3}N^{1/3}$ we get

$N^{2/3} < p^2 < 2^{2/3}N^{2/3}$ (3.29)

Suppose that $N^{2/3} < p_o^2 - c^2N^{2\alpha}$ and $p_o^2 + c^2N^{2\alpha} < 2^{2/3}N^{2/3}$

$p_o^2 - c^2N^{2\alpha} > N^{2/3}$ Square of the both side we have $p_o^4 - c^4N^{4\alpha} > N^{4/3}$

If $p_o^2 - c^2N^{2\alpha} > N^{2/3}$ then $p_o^2 + c^2N^{2\alpha} < N^{2/3}$ therefore equation (3.28) becomes

$|p^2 + q^2 - P| < \frac{N^{4/3}c^2N^{2\alpha}}{p_o^4-c^4N^{4\alpha}} + c^2N^{2\alpha}$

$\Rightarrow \; |p^2 + q^2 - P| < \frac{N^{4/3}c^2N^{2\alpha}}{N^{4/3}} + c^2N^{2\alpha} = 2c^2N^{2\alpha}$ (3.30)

From RSA equation

$ed = 1 + k[(p^2 - 1)(q^2 - 1)]$

But $(p^2 - 1)(q^2 - 1) = p^2q^2 - p^2 - q^2 + 1$

$= Nq + 1 - (p^2 + q^2)$

Since $N = P^2q \; and \; q < N^{1/3}$ by lemma 3.1 we write

$(p^2 - 1)(q^2 - 1) = N^{4/3} + 1 - (p^2 + q^2)$

$= N^{4/3} + 1 - P$

$\Rightarrow ed - k(N^{4/3} + 1 - (p^2 + q^2) = 1$

$ed - k\left(N^{4/3} + 1 - P\right) = 1 + k(P - p^2 - q^2)$ (3.31)

And $N^{4/3} + 1 - (p^2 + q^2) = N^{4/3} + 1 - P$

$p^2 + q^2 = P \Rightarrow P - p^2 - q^2$

$ed - k\left(N^{4/3} + 1 - P\right) = 1 + k(P - p^2 - q^2)$ (3.32)

Divide through by $\left(N^{4/3} + 1 - P\right)d \; from \; (3.32)$ to get

$\frac{ed}{(N^{4/3}+1-P)d} - \frac{k(N^{4/3}+1-P)}{(N^{4/3}+1-P)d} = \frac{1+k(P-p^2-q^2)}{(N^{4/3}+1-P)d}$

$\Rightarrow \frac{e}{(N^{4/3}+1-P)} - \frac{k}{d} = \frac{1+k(P-p^2-q^2)}{(N^{4/3}+1-P)d}$

$\left|\frac{e}{(N^{4/3}+1-P)} - \frac{k}{d}\right| = \frac{|1+k(P-p^2-q^2)|}{(N^{4/3}+1-P)d} < \frac{1+k|P-p^2-q^2|}{(N^{4/3}+1-P)d} \leq \frac{(1+k)|P-p^2-q^2|}{(N^{4/3}+1-P)d}$ (3.33)

Since $ed = 1 + k[(p^2 - 1)(q^2 - 1)]$ then

$$k = \frac{ed-1}{(p^2-1)(q^2-1)} < d \; and \; 1 + k \leq d \quad (3.34)$$

Substituting (3.34) into (3.33) we have

$$\left|\frac{e}{(N^{4/3}+1-P} - \frac{k}{d}\right| < \frac{d|P-p^2-q^2|}{(N^{4/3}+1-P)d}$$

$$< \frac{|P-p^2-q^2|}{(N^{4/3}+1-P)} \quad (3.35)$$

Since from (3.30) we have that $|p^2 + q^2 - P| < 2c^2N^{2\alpha}$ also

$P = p^2 + q^2 \Rightarrow P - p^2 - q^2 \implies p^2+q^2 - P$ then (3.35) become

$\left|\frac{e}{(N^{4/3}+1-P} - \frac{k}{d}\right| < \frac{|p^2+q^2-P|}{(N^{4/3}+1-P)} \implies \left|\frac{e}{(N^{4/3}+1-P} - \frac{k}{d}\right| < \frac{2c^2N^{2\alpha}}{(N^{4/3}+1-P)}$ (3.36)

Also by lemma 3.1, we have that $p^2 + q^2 > 2N^{2/3}$

but since $P = p^2 + q^2 \Rightarrow P > 2N^{2/3}$ then for $N \geq 14$

$N^{4/3} + 1 - P > N^{4/3} + 1 - 2N^{2/3} > 2N$ then it follows that

$$\left|\frac{e}{(N^{4/3}+1-P} - \frac{k}{d}\right| < \frac{2c^2N^{2\alpha}}{2N} = \frac{c^2N^{2\alpha}}{N} = c^2N^{2\alpha-1}$$

$$c^2N^{2\alpha-1} < \frac{1}{2d^2} \Rightarrow 2c^2N^{2\alpha-1} < \frac{1}{d^2}$$

$$d^2\,2c^2N^{2\alpha-1} < 1$$

$$d^2 < \frac{1}{2c^2N^{2\alpha-1}} \Rightarrow d < \frac{1}{\sqrt{2c^2}N^{\frac{2\alpha-1}{2}}} \Rightarrow d < \frac{1}{\sqrt{2c^2}}N^{\frac{1-2\alpha}{2}}$$

But since $c^2 = 1/2 \quad Then\ d < \frac{1}{\sqrt{2^{\frac{1}{2}}}}N^{\frac{1-2\alpha}{2}} \Rightarrow d < \frac{1}{\sqrt{1}}N^{\frac{1-2\alpha}{2}}$

Hence, $d < N^{\frac{1-2\alpha}{2}}$. Notice that when $\alpha = \frac{1}{4}$ the bound is $d < N^{1/4}$ as expected in wiener's approach.

4. Conclusion

For N = p²q we have shown that $\frac{k}{d}$ can be recovered among the convergent of the continued fraction expansion of $\frac{e}{N^{4/3}}$ based on the RSA equation $ed = 1 + k\phi(N)\ where\ \phi(N) = (p^2 - 1)(q^2 - 1)$ with assumption that q < p < 2q, public key e < $(p^2 - 1)(q^2 - 1)$ and private key d < $\frac{1}{2}N^{1/3}$. Using the same RSA equation and e been a public key, with the approximation $p_o^2\ of\ p^2\ that\ is\ |p^2 - p_o^2| < \frac{1}{2}N^{2\alpha}$ and private key exponent d satisfies d < $N^{\frac{1-2\alpha}{2}}$, we proved that $\frac{k}{d}$ can be recovered among the convergent of the continued fraction expansion of $\frac{e}{N^{4/3}+1-P}$. Hence we used convergent of the continued fraction to compute $\phi(N)$ which lead to the successful factorization of RSA prime power $N = p^2q$.

Conflict of Interest

The authors declare no conflict of interest.

References

[1]. Rivest,R. L., Shamir,A., and Adleman, L. (1977). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126.

[2]. Wiener, M. (1990). Cryptanalysis of Short RSA Secret Exponents. *IEEE Trans. Inform. Theory*, 36 : 553–558.

[3]. Kuwakado, H. Koyama, K. and Tsuruoka, Y.(1995). A new RSA-type scheme based on singular cubic curves $y^2 = x^3 + bx^2$ (mod n), *IEICE Transactions on Fundamentals, 78 :* 27-33.

[4]. Coppersmith, D. (1997). Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *Journal of Cryptology*, 10 : 233-260.

[5]. Takagi, T. (1998). Fast RSA-Type Cryptosystem Modulo pkq. *Advances in Crytology-CRYPTO* 1462:318-326.

[6]. Boneh, D. and Durfee, G. (1999). Cryptanalysis of RSA with private key d less than $N^{0.292}$. *Advance in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science,* 1592:1–11.

[7]. Howgrave-Graham, N. (1997). Finding small roots of univariate modular equations revisited. *In IMA International Conference on Cryptography and Coding*, 131–142

[8]. De Weger, B. (2002). Cryptanalysis of RSA With Small Prime Difference. *Applicable Algebra in Engineering, Communication and Computing,* 13:17–28.

[9]. Blömer, J. and May, A. (2004). A Generalized Wiener Attack on RSA. *In Public Key Cryptography (PKC 2004),* 2947: 1–13. Springer-Verlag. https://doi.org/10.1007/BF01195180

[10]. Nassr, D. I., Bahig, H. M., Bhery, A., and Daoud, S. S. (2008). A new RSA vulnerability using continued fractions. In *Proceeding of AICCSA.* 694-701.

[11]. Maitra, S. and Sarkar, S. (2008). Revisiting Wieners Attack-New Weak Keys In RSA. *InInformation Security Springer-Verlag*, 228–243.Magnus, A. Math Z (1962) 78: 361.

[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**: 19-37.

[13]. 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 The 4th International Cryptology and Information Security Conference* 86–99.

[14]. 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.

[15]. Bunder, M, Tonien, J. (*2016).* A new Improved attack on RSA, *Proceedings of the 5th International Cryptology and Information Security Conference.*

[16]. Isah, S. A., Asbullah, M. A., and Ariffin, M. R. K. (2018). A New Improved Bound for Short Decryption Exponent on RSA Modulus N = pq Using Wiener's Method. In *3rd International Conference on Mathematical Sciences and Statistics* UPM,Malaysia.

