Extending Wiener's Attack Using Rsa Prime Power Moduli Of The Form $N = p^r q$

Zaid I.[1], Muhammad A. H[2], Abubakar T. U.[3], Shehu S.[1], Bello U.[2], Abdullahi A. W.[2]

[1]Department of Mathematics, Faculty of Science, Sokoto State University, Sokoto, Nigeria.

[2]Department of Science, Mathematics Unit, State Collage of Basic and Remedial Studies, Sokoto, Nigeria.

[3]Department of Mathematics, Shehu Shagari College of Education, Sokoto, Nigeria.

DOI: 10.29322/IJSRP.11.09.2021.p11762
http://dx.doi.org/10.29322/IJSRP.11.09.2021.p11762

Abstract

In this paper, we considered the RSA prime power moduli $N = p^r q$ for $r \geq 2$ with the key equation $ed - k\varphi(N) = 1$. We presented a new attack which is an extension of Wiener's attack where we used $p^r + p^{r-1}q - p^{r-1} = \left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$ and obtained $d < \frac{N^{1/(r+1)}}{\sqrt{\left(2^{(2r+1)/(r+1)} + 2^{r/(r+1)}\right)N^{1/(r+1)} - 2^{2r/(r+1)}}}$. The result showed that $\frac{k}{d}$ is one of the convergence of the continued fraction expansion of $\frac{e}{N}$ which lead to factorization of N in polynomial time.

Keywords: Prime power, Factorization, Attack, Encryption, Decryption, Euler Toitient function, and Continued fraction.

1. Introduction

The most popular public key cryptosystem in use today is the RSA cryptosystem, introduced by Rivest, Shamir and Adleman (Dujella, 2004). Its security is based on the fact that it is hard to control or deal with as it involves large integer factorization problem and since then it has been extensively used for many applications in the government as well as commercial domain, which include e-banking, secure telephone, smart cards, and communications in different types of networks (Dubey et. al, 2014).

The first attack on small decryption exponent was reported by Wiener in 1990. He showed that RSA is insecured if the small decryption exponent $d < \frac{1}{3}N^{1/4}$ using the continued fractions method to recover d from the convergents of the continued fractions expansion $\frac{e}{N}$. Since then, many attacks on short

decryption exponents emerged, which improved the bound (Wiener, 1990 as reported by Ariffin M. R. K, et. al. (2019).

As described in Boneh and Durfee (2000), schemes with modulus of the form N = $p^r q$ are more susceptible to attacks that leak bits of p than the original RSA-scheme. Using Coppersmith's method for solving univariate modular equations, they showed that it suffices to know a fraction of $\frac{1}{r+1}$ of the MSBs of p to factor the modulus, as reported by Shehu, S. and Ariffin, M. R. K. (2017).

de Weger (2002) proposed a cryptosystem that used the prime difference method to carry out an attack on RSA modulus $N = pq$, where he proved that if $d < \frac{N^{3/4}}{|p-q|}$, then the RSA cryptosystem is considered to be unsecured where primes $p\ and\ q$ have the same bit-length.

Maitra and Sarka (2008) considered RSA-type schemes with modulus $N = p^r q$ for $r \geq 2$, and presented two new attacks for small secret exponent d. Both approaches were applications of Coppersmith's method for solving modular univariate polynomial equations. From these new attacks they directly derive partial key exposure attacks, that is attacks when the secret exponent is not necessarily small but when a fraction of the secret key bits is known to the attacker, as reported by Ariffin M. R. K, et. al. (2019).

Shehu and Ariffin (2017) presented three new attacks on Prime Power $N = p^r q$ using good approximation of $\varphi(N)$ and continued fraction they showed that $\frac{k}{d}$ can be recovered among the convergence of the continued fraction expansion of $\frac{e}{N-2N^{\frac{r}{r+1}}+N^{\frac{r-1}{r+1}}}$ and that one can factor the modulus $N = p^r q$ in polynomial time.

It is in view of this, the paper proposes new attack on RSA variant $N = p^r q$ using continued fraction method. We consider $p^r + p^{r-1}q - p^{r-1} = \left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$ which lead to factorization of N in polynomial time.

2.0 Preliminaries

We begin with definitions and important results concerning the continued fractions, Division Algorithm, Greatest Common Divisor (GCD) and Euler Totient function as well as some useful lemmas needed for the attack.

2.1 Continued Fraction Expansion

A continued fraction is an expression of the form:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_m + \ddots}}} = [a_0,\ a_1, \dots,\ a_m,\ \dots]$$

where a_0 is an integer and a_m are positive integers for $m \geq 1$. The a_m are called the partial quotients of the continued fraction, (Shehu and Ariffin, 2017).

That is, continued fraction expansion of a number is formed by subtracting away the integer part of it and inverting the remainder and then repeating this process till it terminates. For example,

$$\frac{649}{200} = 3 + \frac{49}{200}$$

$$= 3 + \frac{1}{\frac{200}{49}}$$

$$= 3 + \frac{1}{4 + \frac{4}{49}}$$

$$= 3 + \frac{1}{4 + \frac{\frac{1}{49}}{4}}$$

$$= 3 + \frac{1}{4 + \frac{1}{12 + \frac{1}{4}}}$$

$$= 3 + \frac{1}{4 + \frac{1}{12 + \frac{\frac{1}{4}}{1}}}$$

Thus, the convergent of the fraction $\frac{649}{200}$ is $[\frac{49}{200}, \frac{4}{49}, \frac{1}{4}]$

Theorem 2.1 (Legendre): Let $x \in \mathbb{R}$ and $\frac{p}{q}$ be a rational fraction such that $\gcd(p, q) = 1$ and $q < b$ if $x = \frac{a}{b}$ with $\gcd(a, b) = 1$. If $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$ then $\frac{p}{q}$ is a convergent of the continued fraction expansion of x (Shehu and Ariffin, 2017).

2.2 Division algorithm

Given a and $b \in \mathbb{Z}$, with $b > 0$ there are unique integers c and d with the properties $a = bc + d$ and $0 \leq d < b$

Theorem 2.2 The Euclidean algorithm:

Suppose a and b are integers which are not both zero then there exists a unique integer $_c$ w satisfying the conditions

$$c > 0, \quad c|a, \quad c|b, \text{ and if } d|a \text{ and } d|b \text{ then } d|c.$$

2.3 Greatest Common Divisor *(GCD)*

Let $a, b \in \mathbb{Z}$, not both zero, then the unique number c given by Theorem 2.2 is called the greatest common divisor, or GCD, of $a \text{ and } b$.

2.4 The Euler Totient Function

The Euler function ϕ is given by

$$\phi(n) = \text{the number of integers } a \text{ satisfying } 1 \leq a \leq n \text{ and } (a, n) = 1.$$

that is, if $n > 1, \phi(n)$ is the number of positive integers less than n which are coprime to n.

-(Rose, 1987)

2.5 Wiener's attack on RSA

A well-known attack on RSA with low secret-exponent d was given by Wiener (Wiener, 1990). Wiener showed that using continued fractions, one can efficiently recover the secret exponent d from the public key (N, e) as long as $d < \frac{1}{3}N^{1/4}$. For $N = pq$ with $q < p < 2q$, we present below Wiener's attack.

Weiner uses this useful lemma:

Lemma 2.1: Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then

$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}$ and $2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}$

Wiener's Theorem: Let $N = pq$ with $q < p < 2q$, let $d < \frac{1}{3}N^{1/4}$. Given public key (N, e) with $ed \equiv 1 \ mod\varphi(N)$, attacker can efficiently recover d.

Proof:

Using RSA key equation:

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

Dividing the above equation by $d\varphi(N)$, we have:

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

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

We have $\varphi(N) = (p-1)(q-1)$

$$= pq - p - q + 1$$

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

$$\Rightarrow N - \varphi(N) = p + q - 1$$

For which $N - \varphi(N) > 0$ and $p + q - 1 < 2q + q - 1$ (since $p < 2q$)

$$\Rightarrow \quad 0 < N - \varphi(N) \text{ and } p + q - 1 < 3q - 1 < 3q$$

But $N = pq > q^2$, we have that $q < \sqrt{N}$, hence:

$$p + q - 1 < 3\sqrt{N}$$

But $\left|\frac{e}{N}-\frac{k}{d}\right| = \left|\frac{ed-kN}{dN}\right|$

But $ed = 1 + k\varphi(N)$

$$\Longrightarrow \left|\frac{ed-kN}{dN}\right| = \left|\frac{1+k\varphi(N)-kN}{dN}\right|$$

$$= \left|\frac{1+k[\varphi(N)-N]}{dN}\right|$$

$$= \left|\frac{1+k(p+q-1)}{dN}\right|$$

$$< \frac{3k\sqrt{N}}{dN}$$

$$< \frac{3k}{d\sqrt{N}}$$

Since $k < d$, we have: $\left|\frac{e}{N}-\frac{k}{d}\right| < \frac{3}{\sqrt{N}}$

Using Legendre's theorem, $\left|x-\frac{a}{b}\right| < \frac{1}{2b^2}$

We have: $\left|\frac{e}{N}-\frac{k}{d}\right| < \frac{1}{2d^2}$

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

$$\Longrightarrow \frac{3}{\sqrt{N}} < \frac{1}{3d^2}$$

$$\Longrightarrow 9d^2 < \sqrt{N}$$

$$\Longrightarrow d^2 < \frac{\sqrt{N}}{9}$$

$$\Longrightarrow d < \frac{1}{3}N^{1/4}$$

2.6 Some Useful Lemmas

We will use the following Lemmas in our proof of new attack.

Lemma 2.2: (Shehu and Araffin, 2017), let $N = p^r q$ be an RSA prime power modulus with $q < p < 2q$.

Then $2^{-r/(r+1)}N^{1/(r+1)} < q < N^{1/(r+1)} < p < 2^{1/(r+1)}N^{1/(r+1)}$.

Proof:

For $N = p^r q \Rightarrow q = \frac{N}{p^r}$

$$\Rightarrow \frac{N}{p^r} < p < 2\left(\frac{N}{p^r}\right)$$

$$\Rightarrow N < p^{r+1} < 2N$$

$$\Rightarrow N^{1/(r+1)} < p < 2^{1/(r+1)}N^{1/(r+1)} \quad (2.1)$$

Taking reciprocal of the above equation:

$$\Rightarrow \frac{1}{N^{1/(r+1)}} < \frac{1}{p} < \frac{1}{2^{1/(r+1)}N^{1/(r+1)}}$$

$$\Rightarrow \frac{1}{2^{r/(r+1)}N^{r/(r+1)}} < \frac{1}{p^r} < \frac{1}{N^{r/(r+1)}}$$

Multiplying by N:

$$\Rightarrow \frac{N}{2^{r/(r+1)}N^{r/(r+1)}} < \frac{N}{p^r} < \frac{N}{N^{r/(r+1)}}$$

$$\Rightarrow 2^{-r/(r+1)}N^{1-r/(r+1)} < q < N^{1-r/(r+1)}$$

$$\Rightarrow 2^{-r/(r+1)}N^{1/(r+1)} < q < N^{1/(r+1)} \quad (2.2)$$

Combining equation (2.1) and (2.2):

$$2^{-r/(r+1)}N^{1/(r+1)} < q < N^{1/(r+1)} < p < 2^{1/(r+1)}N^{1/(r+1)}$$

Lemma 2.3: Let $N = p^r q$ be an RSA prime power modulus with $q < p < 2q$, $2^{-r/(r+1)}N^{1/(r+1)} < q < N^{1/(r+1)} < p < 2^{1/(r+1)}N^{1/(r+1)}$. Then

$p^r + p^{r-1}q - p^{r-1} = \left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$, for $r \geq 2$.

Proof:

Using $\varphi(N) = p^{r-1}(p-1)(q-1)\ for\ N = p^r q$

We have:

$$p^{r-1}(p-1)(q-1) = (p^r - p^{r-1})(q-1)$$

$$= p^r q - p^{r-1}q - p^{r-1} + p^{r-1}$$

$$= N - (p^r + p^{r-1}q) + p^{r-1}$$

$$\Rightarrow\ p^r + p^{r-1}q - p^{r-1} = N - p^{r-1}(p-1)(q-1)$$

This terminate the proof.

Using $2^{-r/(r+1)}N^{1/(r+1)} < q < N^{1/(r+1)} < p < 2^{1/(r+1)}N^{1/(r+1)}$

Let $p \approx 2^{1/(r+1)}N^{1/(r+1)}$ $and\ q \approx 2^{-r/(r+1)}N^{1/(r+1)}$

$$\Rightarrow p^r + p^{r-1}q - p^{r-1} = N - \left(2^{1/(r+1)}N^{1/(r+1)}\right)^{r-1}\left(2^{1/(r+1)}N^{1/(r+1)} - 1\right)\left(2^{-r/(r+1)}N^{1/(r+1)} - 1\right)$$

$$= N - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}\left(2^{1/(r+1)}N^{1/(r+1)} - 1\right)\left(2^{-r/(r+1)}N^{1/(r+1)} - 1\right)$$

$$= N - \left(2^{r/(r+1)}N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}\right)\left(2^{-r/(r+1)}N^{1/(r+1)} - 1\right)$$

$$= N - \left(N - 2^{r/(r+1)}N^{r/(r+1)} - 2^{-1/(r+1)}N^{r/(r+1)} + 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}\right)$$

$$= N - N + 2^{r/(r+1)}N^{r/(r+1)} + 2^{-1/(r+1)}N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$$

$$= \left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$$

Hence, $p^r + p^{r-1}q - p^{r-1} = \left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$ (2.3)

3.0 Our New Attack

Let $N = p^r q$ be an RSA prime power moduli with $q < p < 2q,\ 1 < e < \varphi(N),\ p^r + p^{r-1}q - p^{r-1} = \left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$ and $\frac{k}{d}$ is among the convergence of the continued fraction expansion of $\frac{e}{N}$, then $d < \frac{N^{1/(r+1)}}{\sqrt{\left(2^{(2r+1)/(r+1)} + 2^{r/(r+1)}\right)N^{1/(r+1)} - 2^{2r/(r+1)}}}$, for $r \geq 2$.

Proof:

Using RSA key equation $ed - k\varphi(N) = 1,$ we have

$$ed - kp^{r-1}(p-1)(q-1) = 1$$

$$i.e. \qquad ed - k(p^r - p^{r-1})(q-1) = 1$$

$$\Rightarrow \quad ed - k(p^r q - p^r - p^{r-1}q + p^{r-1}) = 1$$

$$\Rightarrow \quad ed - k(N - p^r - p^{r-1}q + p^{r-1}) = 1$$

$$\Rightarrow \quad ed - kN + k(p^r + p^{r-1}q - p^{r-1}) = 1$$

$$\Rightarrow \quad ed - kN = 1 - k(p^r + p^{r-1}q - p^{r-1})$$

Dividing both sides by Nd:

$$\left|\frac{ed}{Nd} - \frac{kN}{Nd}\right| = \frac{|1 - k(p^r + p^{r-1}q - p^{r-1})|}{Nd} < \frac{k(p^r + p^{r-1}q - p^{r-1})}{Nd}$$

$$\Rightarrow \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{k(p^r + p^{r-1}q - p^{r-1})}{Nd} \tag{3.1}$$

but $\dfrac{k}{d} < 1$

$$\Rightarrow \frac{k(p^r + p^{r-1}q - p^{r-1})}{Nd} < \frac{(p^r + p^{r-1}q - p^{r-1})}{N}$$

$$Hence, \qquad \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{p^r + p^{r-1}q - p^{r-1}}{N} \tag{3.2}$$

From equation (2.3)

$$p^r + p^{r-1}q - p^{r-1} = \left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$$

$$\Rightarrow \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{\left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}}{N}$$

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

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

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

$$< \frac{\left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)}{N^{1/(r+1)}} - \frac{2^{(r-1)/(r+1)}}{N^{2/(r+1)}}$$

$$< \frac{\left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{1/(r+1)} - 2^{(r-1)/(r+1)}}{N^{2/(r+1)}}$$

Using Legendre's equation $\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$

We have: $\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$

$$\Rightarrow \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{\left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{1/(r+1)} - 2^{(r-1)/(r+1)}}{N^{2/(r+1)}} < \frac{1}{2d^2}$$

$$< \frac{\left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{1/(r+1)} - 2^{(r-1)/(r+1)}}{N^{2/(r+1)}}(2d^2) < 1$$

$$\Rightarrow \quad 2d^2 < \frac{N^{2/(r+1)}}{\left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{1/(r+1)} - 2^{(r-1)/(r+1)}}$$

$$\Rightarrow \quad d^2 < \frac{N^{2/(r+1)}}{2\left[\left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{1/(r+1)} - 2^{(r-1)/(r+1)}\right]}$$

$$< \frac{N^{2/(r+1)}}{\left(2^{r/(r+1)+1} + 2^{-1/(r+1)+1}\right)N^{1/(r+1)} - 2^{(r-1)/(r+1)+1}}$$

$$< \frac{N^{2/(r+1)}}{\left(2^{(r+r+1)/(r+1)} + 2^{(-1+r+1)/(r+1)}\right)N^{1/(r+1)} - 2^{(r-1+r+1)/(r+1)}}$$

$$< \frac{N^{2/(r+1)}}{\left(2^{(2r+1)/(r+1)} + 2^{r/(r+1)}\right)N^{1/(r+1)} - 2^{2r/(r+1)}}$$

$$\Rightarrow \quad d < \sqrt{\frac{N^{2/(r+1)}}{\left(2^{(2r+1)/(r+1)} + 2^{r/(r+1)}\right)N^{1/(r+1)} - 2^{2r/(r+1)}}}$$

$$\Rightarrow \quad d < \frac{N^{1/(r+1)}}{\sqrt{\left(2^{(2r+1)/(r+1)} + 2^{r/(r+1)}\right)N^{1/(r+1)} - 2^{2r/(r+1)}}}, \text{for } r \geq 2$$

Proposed Algorithm:

Input: an RSA prime modulus $N = p^r q$ with $q < p < 2q$, and public key (e, N)

Output: The private key (N, d).

1: **Choose** two random and distinct n - bit strong primes (p, q).

2: **for each** pair of the form (p, q) **do**

3: $N : p^r q$

4: $\varphi(N) := p^{r-1}(p-1)(q-1)$

5: f**or** $p^r + p^{r-1}q - p^{r-1} = \left(2^{r/(r+1)} + 2^{-1/(r+1)}\right)N^{r/(r+1)} - 2^{(r-1)/(r+1)}N^{(r-1)/(r+1)}$ do

6: compute the continued fraction expansion of $\frac{e}{N}$

7: **for** every convergent $\frac{k}{d}$ of $\frac{e}{N}$, compute $\varphi(N) = \frac{ed-1}{k}$

8: **compute** $d < \frac{N^{1/(r+1)}}{\sqrt{\left(2^{(2r+1)/(r+1)} + 2^{r/(r+1)}\right)N^{1/(r+1)} - 2^{2r/(r+1)}}}$, for $r \geq 2$

9. **end** if

10: **return** the public key pair (N, e) and the private key pair (N, d).

4.0 Conclusion

This paper presented a new attack on the RSA prime power moduli $N = p^r q$. In the attack, we used continued fractions expansions and showed that $\frac{k}{d}$ can be recovered among the convergences of the continued fraction expansion of $\frac{e}{N}$ and discovered a decryption exponent $d < \frac{N^{1/(r+1)}}{\sqrt{\left(2^{(2r+1)/(r+1)} + 2^{r/(r+1)}\right)N^{1/(r+1)} - 2^{2r/(r+1)}}}$, for $r \geq 2$. Hence, the RSA prime power moduli $N = p^r q$ can be factored in polynomial time.

References

Ariffin M. R. K. et. al. (2019), *New Cryptanalytic Attack on RSA Modulus N = pq Using Small Prime Difference Method.* https://www.mdpi.com/2410-387X/3/1/2/htm

de Weger, B. (2002), *Cryptanalysis of RSA with small prime difference*, Applicable Algebra in Engineering, Communication and Computing, Vol. 13(1), pp. 17-28.

Dubey, M.K. et. al. (2014). *Cryptanalytic Attacks and Countermeasures on RSA.* In proceedings of the Third International Conference on Soft Computing for Problem Solving; Springer: New Delhi, India, pp. 805–819.

Dujella A. (2004). Continued fractions and RSA with small secret exponent, Tatra Mt. Math. Publ. 29.

Rose, H. E. (1987), *A Course in Number Theory*. Oxford Science Publications.

Shehu, S. and Ariffin M. R. K. (2017). *New attacks on prime power $N = p^r q$ using good approximation of $\varphi(N)$*.Malysia Journal of Mathematical Sciences 11(S); pp 121 -138.

Wiener, M. (1990). *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory, Vol. 36, pp. 553-558.