ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

Computational Difficulty of Factoring Large Integers Using Generalize System Equations

Samaila Abdullahi[1], Sadiq Shehu[2], Tukur Shehu[3]

[1,2]Department of Mathematics, Faculty of Science, Sokoto State University, Sokoto Nigeria
[3]Department of Mathematics, School of Science,
Shehu Shagari College of Education, Sokoto Nigeria

Received: 26 January 2023; Accepted: 03 February 2023; Published: 28 February 2023

Abstract: The RSA algorithm is the foundation of a cryptosystem, which permits public key encryption and is frequently used to establish a secure connection, particularly when it is delivered over an unprotected network such as the internet. Let p and q be unbalance prime, we offer two novel attacks in this paper using prime power modulus $N = p^r q^s$. Our first results are based on the RSA equation $ex^2 - \phi(N)y^2 = 1$ e, N and $x, p, q, \varphi(N)$ are public key and private key tuples respectively. If $p \le q \le \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$, then $x < \sqrt{\frac{1}{2}(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}))}$ and $\frac{y^2}{x^2}$ can be obtained among the convergent of the continued fractions expansion of $\frac{e}{N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})}$ which lead to the factorization of moduli N. In second part we consider the generalize system of equation using the proper approximation of $\varphi(N)$ which allowed us to factored the prime power moduli $N_s = p_s^r q_s$ simultaneously in polynomial time.

Keywords: RSA Prime Power, Factorization, Polynomial time, Generalize system, Diophantine approximations, Continued fraction, convergent.

I. Introduction

Cryptanalysis is the science of studying information systems in order to learn more about the system's hidden elements. Even if the cryptography key is unknown, cryptanalysis is used to break into a cryptography security system and gain access to the content of encrypted messages. There are two sorts of keys in this category of cryptography: symmetric and asymmetric keys. Only one key can be disclosed for both encryption and decryption in symmetric cryptanalysis. Asymmetric cryptography is the subject of this study. The term "asymmetric" refers to the existence of two distinct keys. Because one of the keys can be provided to anybody while the private key is kept secret, this is also known as public key cryptography. When a cryptosystem's secure instances aren't utilised, a protocol failure occurs.

Ronal Revest was the one who came up with the concept of cryptosystem. The most frequently used asymmetric cryptographic technique, RSA, was devised by Adi Shamir and Leonard Adleman in 1977. The RSA public key cryptosystem, for example, is used to protect web traffic, email, remote login sessions, and electronic credit card payment systems. The integer factorization problem is RSA's underlying one-way function: multiplying two large primes is computationally simple, but factoring the resulting product is extremely difficult. The complexity of solving the so-called RSA problem is also well-known for RSA's security. Calculate the plaintext m using an RSA public key (e, N) and a ciphertext $c \equiv m^e \pmod{N}$, Because factoring modulus N leads to obtaining the private exponent d and solving the RSA problem, the RSA problem isn't any more difficult to solve than the integer factorization problem. The converse, on the other hand, is not evident. Rivest R.; Shamir, A.; Adleman, L. (1978).

The public modulus N = pq in the RSA cryptosystem is the product of two primes of the same bit size. The congruence is satisfied by the public and private exponents e and d, respectively.

$$ed \equiv 1 \pmod{\Phi(N)},$$

The Euler totient function $\Phi(N) = (p - 1)(q - 1)$ is used. In RSA, heavy exponentiations are needed for encryption, decryption signature, and signature verification. To reduce the encryption time or the signature verification time, one can use a small public exponent e such as 3 or $2^{16} + 1$.On the other hand to reduce the decryption time or the signature generation time, one can be tempted to use a small private exponent d. Many attacks show that using a very small private exponent is measure. Indeed, Wiener showed

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

in 1990 how to break RSA when $d < N^{0.25}$ using Diophantine approximations. The bound was improved by Boneh and Durfee 1999 to $d < N^{0.292}$ using Coppersmith's lattice based method.

1.2 RSA Cryptosystem Using Continued Fraction

Wiener (1999), presented an attack on RSA that solves the key equation and factor N if d is sufficiently small, namely $d < \frac{1}{3}N^{0.25}$. The 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 attack on RSA has been extended in many ways using the lattices reduction of the coppersmiths method.

M. J. Wiener (1990), described a polynomial time algorithm for breaking a typical (i.e. p and q are of the same size and e < n) RSA cryptosystem if the secret exponent d has at most one-quarter as many bits as the modulus n. From $ed \equiv 1 \pmod{\phi(n)}$, it follows that there is an integer k such that $ed - k\phi(n) = 1$. Since $\phi(n) \approx n$, we have that $\frac{k}{d} \approx \frac{e}{n}$. Wiener's attack is usually described in the following form If p < q < 2p, with e < n and $d < \frac{1}{3}\sqrt[4]{n}$, then d is the denominator of some convergent of the continued fraction expansion of $\frac{e}{n}$. Indeed, under these assumptions it is easy to show that

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

By the classical Legendre's theorem, $\frac{k}{d}$ is some convergent $\frac{p_m}{q_m}$ of the continue fraction expansion of $\frac{e}{n}$, and therefore d can be computed efficiently from the public key (n, e). Namely, the total number of convergent is of order O(log n), and each convergent can be tested in polynomial time.

In 2009 Nitaj, showed how to factor the RSA modulus $N = p\ q$, if (N, e), is a public key satisfying an equation

$eX - (N - (ap + bq - 1))Y = Z$ with small parameters X, Y and Z where $\frac{a}{b}$ is an unknown convergent of $\frac{q}{p}$ with $a \geq 1$.

Hence he consider the cases when the difference $|ap - bq|$ is small, ie, $|ap - bq| < (abN)^{\frac{1}{4}}$.

II. Literature Review

Theorem 1. Nitaj, (2009). Let $N = p\ q$ be an RSA modulus with unknown factors p, q such that 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 $|ap - bq| < (abN)^{\frac{1}{4}}$. Let e be a public exponent satisfying an equation $eX - (N - (ap + bq - 1))Y = Z$ with gcd(X,Y) = 1. Set $|ap + bq| = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}, if \quad 1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ and |Z|< inf $((abN)^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha})$, then N can be factored in polynomial time.

An Attack by Using the medium difference of $|ap - bq|$

In 2009 Nitaj, present the second attack based on the Elliptic Curve Method (ECM) which can find factors of about 52-digits. Assuming the efficiency of ECM, every step in this attack can be done in polynomial time and the number of convergents is bounded by O(log N). To express this fact, the term efficient is used.

Theorem 2. Nitaj, (2009). Let $N = p\ q$ be an RSA modulus with unknown factors p, q such that 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 $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$ and $b \leq 10^{52}$.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

Let e be a public exponent satisfying equation $eX-(N-(ap+bq))Y=Z$ with gcd(X,Y) = 1. Set $M=N-\frac{eX}{Y}$ and $|ap+bq|=N^{\frac{1}{2}+\alpha}$ with $0<\alpha<\frac{1}{2}, if \quad 1\le Y\le X<\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$ and |Z|< inf $(aN^{\frac{1}{4}},\ \frac{1}{2}N^{\frac{1}{2}-\alpha})Y$, then using ECM N can be factored in efficiently.

Furthermore using a combination of the continued fraction algorithm and Coppersmith's lattice based technique for solving polynomial equations, he showed that every exponent e in these classes yields the factorization of N. Moreover, proved that the number of such exponents is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon>0$ is arbitrarily small for large N. As it follows

Theorem 3. Let $N=p\ q$ be an RSA modulus with q < p < 2q and $|\ p-q\ |>\frac{\sqrt{N}}{2^{100}}$ the number of the exponents e satisfying $e=\left[X-(N-(pu+\frac{q}{u}))Y\right]+Z$ with $|\ u\ |>\frac{1}{2}q, \gcd(X,Y)=1,\ \ X\le Y<\frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}},\ |\ Z\ |<\frac{(p-q)N^{\frac{1}{4}}}{3(p+q)}-\frac{1}{2}$, where $\left|up-\frac{q}{u}\right|=N^{\frac{1}{2}+\alpha}$ is at least $N^{\frac{3}{4}-\varepsilon}$ where $\varepsilon>0$ is arbitrarily small for suitably large N.

In 2009 Chen et al. generalize the result of Benne de Weger (2002) and Maitra and Sakar (2008), 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 $b(a^2+1)q-a(b^2+1)(aq-bp)>0$. Let $|aq-bp|<N^{\gamma}$ they showed that $N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1$ is a better approximation to $\varphi(N)$ instead of $N.$ and $\frac{k}{d}$ is a convergent from the continued fraction expansion of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1}$.

Theorem 4. Chen et al., (2009). Let $N=pq$ be an RSA modulus with q < p < 2q, $N\ >8d$ and $|aq-bp|<N^{\gamma}$ Let $e<\varphi(N)$ and $d<N^{\delta}$ be a public and private exponent, respectively. If $\delta<\frac{3}{4}-\gamma,$ then

$$\left|\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1}-\frac{k}{d}\right|<\frac{1}{2d^2},$$

Ariffin *et al*. (2013) showed that for any efficient algorithm able to factor the modulus $A_2=p^2q$ 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 (Asbullah and Ariffin, 2014),** 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 eliminate the decryption failure which was due to a 4-to-1 mapping Scenario.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

Asbullah and Ariffin (2015) 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 *et al.* (2016) an attack is presented 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*. (2018) 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

III. Some Important Results

Lemma 3.1

Let $\mu = p^r q$ be a prime power moduli with unbalance prime numbers p and q, if $q < p < \lambda q$ for $r, \lambda < 2$ then

$\lambda^{\frac{-r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}} < p < \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$ and

$\phi(N) = N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})$

$q < p < \lambda q$

$p^r q < p^r p < \lambda p^r q$

$N < p^{r+1} < \lambda N$

$N^{\frac{1}{r+1}} < p < \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$ .....(1)

But $q = \frac{N}{p^r}$

From (1)

$N^{\frac{1}{r+1}} < p^r < \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

$$\frac{N}{N^{\frac{r}{r+1}}} < \frac{N}{p^r} < \frac{N}{\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}}}$$

$$\lambda^{\frac{-r}{r+1}} N^{\frac{1-r}{r+1}} < q < N^{\frac{1-r}{r+1}}$$

$$\lambda^{\frac{-r}{r+1}} N^{\frac{r}{r+1}} < q < N^{\frac{1}{r+1}} \text{..}(2)$$

From (1) and (2) we've

$$\lambda^{\frac{-r}{r+1}} N^{\frac{1}{r+1}} < q < N^{\frac{1}{r+1}} < p < \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$$

Therefore

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

$$\begin{aligned}
&= p^{r-1}(pq - p - q + 1) \\
&= p^{r-1}pq - p^{r-1}p - p^{r-1}q + p^{r-1} \\
&= p^{r-1+1}q - p^{r-1+1} - p^{r-1}q + p^{r-1} \\
&= p^r q - p^r - p^{r-1}q + p^{r-1}
\end{aligned}$$

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

when $p \square q \square \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$

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

$$\begin{aligned}
&= N - (p^r + p^{r-1}q - p^{r-1}) \\
&= N - ((\lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})^r + (\lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})^{r-1}(\lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}) - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}) \\
&= N - (\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} + \lambda^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}(\lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}) - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}) \\
&= N - (\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} + \lambda^{\frac{r-1}{r+1}+\frac{1}{r-1}} N^{\frac{r-1}{r+1}+\frac{1}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}) \\
&= N - (\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} + \lambda^{\frac{r-1+1}{r+1}} N^{\frac{r-1+1}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}) \\
&= N - (\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} + \lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})
\end{aligned}$$

$$\phi(N) = N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})$$

$$\Rightarrow N - \phi(N) = (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})$$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

Theorem

Let $N = p^r q$ be a prime power moduli where p and q are unbalance prime with $q < p < \lambda q$ for $r, \lambda > 2$ and $1 < e < \phi(N) < N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})$ Satisfying the equation $ex^2 - \phi(N)y^2 = 1$ where e, N and $d, p, q, \phi(N)$ are public key and private key tuples respectively. If $p \square q \square \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$, then $x < \sqrt{\frac{1}{2}(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}))}$ and $\frac{y^2}{x^2}$ can be obtained among the convergent of the continued fractions expansion of $\frac{e}{N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})}$ which lead to the factorization of moduli N.

Proof

Using of result of lemma (3.1) where $p \square q \square \lambda^{\frac{1}{r+1}} \mu^{\frac{1}{r+1}}$ for $\lambda > 2$, the equation $ex^2 - \phi(N)y^2 = 1$ with $g < d(x^2, y^2) = 1$ can be rewritten as follows

$$ex^2 - \phi(N)y^2 = 1$$
$$ex^2 - y^2(p^{r-1}(p-1)(q-1)) = 1$$
$$ex^2 - y^2(p^{r-1}(pq - p - q + 1)) = 1$$
$$ex^2 - y^2(p^{r-1}pq - p^{r-1}p - p^{r-1}q + p^{r-1}) = 1$$
$$ex^2 - y^2(N - p^r - p^{r-1}q + p^{r-1}) = 1$$
$$ex^2 - y^2(N - (p^r + p^{r-1}q - p^{r-1})) = 1$$
$$ex^2 - y^2(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})) = 1$$

Divide both side by $x^2(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}))$ we get

$$\frac{ex^2}{x^2(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}))} - \frac{y^2(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}))}{x^2(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}))}$$

$$\left| \frac{e}{N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}})} - \frac{y^2}{x^2} \right| = \left| \frac{1}{x^2(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}))} \right|$$ also using the Euler's theorem we have

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

$$\frac{2(x^4)}{2x^2} < \frac{x^2(N - (2\lambda^{\frac{r}{r+1}} N^{\frac{r}{r+1}} - \lambda^{\frac{1}{r+1}} N^{\frac{1}{r+1}}))}{2x^2}$$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

$$x^2 < \frac{1}{2}(N-(2\lambda^{\frac{r}{r+1}}N^{\frac{r}{r+1}}-\lambda^{\frac{1}{r+1}}N^{\frac{1}{r+1}}))$$

$$x < \sqrt{\frac{1}{2}(N-(2\lambda^{\frac{r}{r+1}}N^{\frac{r}{r+1}}-\lambda^{\frac{1}{r+1}}N^{\frac{1}{r+1}})}$$

Hence $\frac{y^2}{x^2}$ can be fund among the convergent of the continued fractions expansion of $\frac{e}{N-(2\lambda^{\frac{r}{r+1}}N^{\frac{r}{r+1}}-\lambda^{\frac{1}{r+1}}N^{\frac{1}{r+1}}),}$

Which lead to computing $ex^2-\phi(N)y^2=1$ as $\phi(N)=\frac{ex^2-1}{y^2}$ and $p^{r-1}=gcd(\phi(N),N)$ with $g=\frac{N}{p^{r-1}}$ for $r>2.$

This completes the proof.

Algorithm 1

1. Initialization : $N=p^rq$ with $q<p<\lambda q$ and public keys (N,e) satisfying theorem
2. Choose r,λ to be suitable small position integers where $r,\lambda>2$.
3. For any (r,λ) do
4. Complete $\frac{x^2}{y^2}$ from the continued fraction expansion of $N-(2\lambda^{\frac{r}{r+1}}N^{\frac{r}{r+1}}-\lambda^{\frac{1}{r+1}}N^{\frac{1}{r+1}})$
5. Complete $\phi(N)=\frac{ex^2-1}{y^2}$
6. Complete $p^{r-1}=gcd(N,\frac{ex^2-1}{y^2})$
7. $1< p^{r-1}<N$,then $q=\frac{N}{p^r}$
8. Return prime p and q

Lemma 4.0

Generalize system of Equation using the Proper Approximation of $\phi(N).$

In this section for $r,\lambda>2$ we present another attack of two instance of factoring j prime power moduli $Ns=p_s^r\phi_s$ for $s=1,\ 2\ldots\ldots j$ using the system of equation of the form $e_sx^2-\lambda(N_s)y_s^2=1$ and $e_sx_s^2-\lambda(N)y^2=1$.

Theorem 4.1

Let $Ns=p_s^rq_s$ be the unbalance prime power moduli and suppose that $1<e_s<\phi(N_s)<N_s-(\lambda_s^{\frac{r}{r+1}}N_s^{\frac{r}{r+1}}-\lambda_s^{\frac{1}{r+1}}N_s^{\frac{1}{r+1}})$ for $r,\lambda>2$ and $s=1,\ 2\ldots\ldots j$ let (e_s,Ns)

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

and $(x, p_s, q_s, \phi(N))$ be public and private key tuples respectively let N= max $\{Ns\}$, if there exist positive integer $x, y_s < N^{\xi}$ for all $\xi = \frac{j-\gamma j(r+1)}{(r+1)(1+2j)}$ with $0 < \xi \le 1$, such that $e_s x^2 - \phi(N_s) y^2 = 1$, then j prime power moduli $N_s = p_s^r q_s$ can be factored simultaneously in polynomial time.

Proof

Suppose that $N_s = p_s^r q_s$ with $r \ge 2$ and $s = 1, 2, ..., j$. Also assume that $N = max\{N_s\}$, and $x, y_s < N^{\xi}$ then the equation $e_s x^2 - y_s^2(\phi(N_s) = 1$ can be as follows

$$e_s x^2 - y_s^2(\phi(N_s) = 1$$

$$e_s x^2 - y_s^2(p_s^{r-1} q_s(p_s - 1)(q_s - 1)) = 1$$

But $\phi(N_s) = N_s - (2\lambda_s^{\frac{r}{r+1}} N_s^{\frac{r}{r+1}} - \lambda_s^{\frac{1}{r+1}} N_s^{\frac{1}{r+1}})$ and $N_s - \phi(N_s) = (2\lambda_s^{\frac{r}{r+1}} N_s^{\frac{r}{r+1}} - \lambda_s^{\frac{1}{r+1}} N_s^{\frac{1}{r+1}})$

Let $K = 2\lambda_s^{\frac{r}{r+1}} N_s^{\frac{r}{r+1}} - \lambda_s^{\frac{1}{r+1}} N_s^{\frac{1}{r+1}}$

$$\Rightarrow e_s x^2 - y_s^2(N_s - (2\lambda_s^{\frac{r}{r+1}} N_s^{\frac{r}{r+1}} - \lambda_s^{\frac{1}{r+1}} N_s^{\frac{1}{r+1}}) = 1$$

$$\Rightarrow e_s x^2 - y_s^2(N_s - K + K - (N_s - \phi(N_s)) = 1$$

$$\Rightarrow e_s x^2 - y_s^2(N_s - K) = 1 - y_s^2(N_s - \phi(N_s) - K)$$

$$\Rightarrow \left| \frac{e_s}{N_s - k} x^2 - y_s^2 \right| = \left| \frac{1 - y_s^2(N_s - \phi(N) - K)}{N_s - K} \right|$$

If $N = max\{N_s\}$, and $x, y_s < N^{\xi}$ be unknown positive integers with $|N_s - \phi(N_s) - K| < N^{\gamma}$ for $0 < \gamma < 1$ and $|N_s - K| > N_s^{\frac{1}{r+1}}$

$$\frac{1 - y_s^2(N_s - \phi N_s) - K)}{N_s - K} < \frac{1 + y_s^2(N_s - \phi N_s) - K)}{N_s - K}$$

$$< \frac{1 + (N_s^{\xi})^2 (N_s^{\gamma})}{N^{\frac{1}{r+1}}}$$

$$< \frac{1 + N_s^{2\xi} N_s^{\gamma}}{N^{\frac{1}{r+1}}}$$

$$< N^{2\xi} + \gamma - \frac{1}{r+1}$$

$$\therefore \left| \frac{e_s}{N_s - K} x^2 - y_s^2 \right| < N^{2\xi} + \gamma - \frac{1}{r+1}$$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

To show that the unknown integer x and j integer y_s lead to the factorization of the moduli $N_s = p_s^r q_s$ we let

$\varepsilon = N^{2\xi+\gamma-\frac{1}{r+1,}}$ and $0 < \gamma < 1$

With

$$\xi = \frac{j - \gamma j(r+1)}{(r+1)(1+2j)}$$

$$N^{\xi}\varepsilon^{j} = N^{\xi}(N^{2\xi+\gamma-\frac{1}{r+1}})^{j}$$

$$= N^{\xi++2\xi j+\gamma j-\frac{1}{r+1}}$$

$$= (1)^{j}$$

$$\Rightarrow \xi + 2\xi j + \gamma j - \frac{j}{r+1} = 0$$

$$\xi + 2\xi j = \frac{j}{r+1} - \gamma j$$

$$\xi(1+2j) = \frac{j - \gamma j(r+1)}{r+1}$$

$$\xi = \frac{j - \gamma j(r+1)}{(r+1)(1+2j)}$$

From the theorem (2.4) above we can say write

$(1)^{j} < 2\frac{w(\omega-3)}{4}.3^{w}$ for $w \geq 2$ which shows that $N^{\xi}\xi^{j} < 2\frac{w(w-3)}{4}.3^{\omega}$ and hence if $x < N^{\xi}$ then

$x < 2\frac{w(w-3)}{4}.3^{\omega}\varepsilon^{-\omega}$ for $s = 1,\ 2\ldots\ldots j$

$$\therefore \left|\frac{e_s}{N_s - K}x^2 - y_s^2\right| < \varepsilon.$$

Since the inequality above satisfies the condition of theorem 2.4, then the decryption exponent

x and j integers y_s for $s = 1,\ 2\ldots\ldots j$. can be obtain by using the lattice basis reduction techniques which allow the following computations.

$$\frac{e_s x^2 - 1}{y_s^2} = \phi(N_s)$$

$$p_s^{r-1} = \gcd(\phi(N_s)N_s)$$

$$q_s = \frac{N_s}{p_s^r}$$

Which leads to the factorization of j prime power moduli N_s for $s = 1,\ 2\ldots\ldots j$ in polynomial time. Next we let

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

$$H_1 = \frac{e_1}{N_1 - 2\lambda_1^{\frac{r}{r+1}} N_1^{\frac{r}{r+1}} - \lambda_1^{\frac{1}{r+1}} N_1^{\frac{1}{r+1}}}$$

$$H_2 = \frac{e_2}{N_2 - 2\lambda_2^{\frac{r}{r+1}} N_2^{\frac{r}{r+1}} - \lambda_2^{\frac{1}{r+1}} N_2^{\frac{1}{r+1}}}$$

$$H_3 = \frac{e_3}{N_3 - 2\lambda_3^{\frac{r}{r+1}} N_3^{\frac{r}{r+1}} - \lambda_3^{\frac{1}{r+1}} N_3^{\frac{1}{r+1}}}$$

with the lattice L spanned by the matrix,

$$W = \begin{vmatrix} 1 & -[T(H_1)] & -[T(H_2)] & -[T(H_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{vmatrix}$$

where T is define as

$$\text{T}=\left[3^{\omega+1} \times 2 \frac{(\omega+1)(\omega-4)}{4} \times \varepsilon^{-\omega-1} \right] \text{ for } w \geq 2.$$

Algorithm 2

1. initialization : the public key tuple (N_s, e_s, ξ, γ) satisfying theorem 3.3
2. choose $r, \lambda > 2$ $N = max\{Ns\}$, for $s = 1, 2 \ldots\ldots j$
3. For any $(r, \lambda, N, \xi, \gamma)$ do
4. $\xi = N^{2\xi} + T - \frac{1}{r+1,}$
5. $T = \left[3^{\omega+1} \times 2 \frac{(\omega+1)(\omega-4)}{4} \times \varepsilon^{-\omega-1} \right]$ for $\omega \geq 2$
6. End for co
7. From the lattice L spanned by the matrix W apply the iii algorithms to L, result to the reduced basis matrix K.
8. For any (ω, K) do
9. $R = \omega^1$
10. $C = RK$
11. End for
12. Compute $\phi(N_s) = \frac{e_s x - 1}{y_s^2}$
13. $p_s^{r-1} = \gcd(\phi(N_s), N_s)$
14. $q_s = \frac{N_s}{p_s^r}$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

15. Return the prime factors (p_s, q_s)

Theorem 3.4

Support $N_S = P_s^r q_s$ be prime moduli with $q < p < \lambda q$ for $r, \lambda > 2$ and $s = 1,\ 2 \ldots\ldots j$. Where p and q are unbalance prime factors. Let (e_s, N_s) and $\left(x, N_S, p_s, q_s, \phi(N_s)\right)$ be public key pair and private key pair respectively such that $1 < e_s < \phi(N_s)$ satisfies $e_s x_s^2 - y^2\phi(N_s) = 1$. Let $N = \min\{N_S\}$ and $e = \min(e_s) = N\hat{}$ be the public exponent. If there exit unknown integers $x_s, y^2 < N^{\xi}$ where $\xi = \dfrac{j - \gamma j(r+1)}{(r+1)(1+2j)}$ for $0 < \varepsilon < 2$ then p_s and q_s can be recover as the factors of the prime power moduli N_s simultaneously in polynomial time.

Proof

Suppose that $N_S = P_s^r q_s$ for $r > 2$ and $s = 1,\ 2 \ldots\ldots j$ be j prime power moduli such that $q < p < \lambda q$. Let $N = \min\{N_S\}$ and $y_s < N^{\xi}$ then for $e_s x_s^2 - y^2\phi(N_s) = 1$, we obtained $e_s x_s^2 - y^2(p_s^{r-1} q_s (p_s - 1)(q_s - 1)) = 1$

$$e_s x_s^2 - y^2(N_s - (2\lambda_s^{\frac{r}{r+1}} N_s^{\frac{r}{r+1}} - \lambda_s^{\frac{1}{r+1}} N_s^{\frac{1}{r+1}})) = 1$$
$$e_s x_s^2 - y^2(N_s - K + K - (N_s - \phi(N_s))) = 1$$
$$e_s x_s^2 - y^2(N_s - K) = 1 - y^2(N_s - \phi(N_s) - K)$$
$$\left|\frac{N_s - K}{e_s} y^2 - x_s^2\right| = \left|\frac{1 - y^2(N_s - \phi(N_s) - K)}{e_s}\right|$$

If $N = \min\{N_S\}$ and $x_s^2, y^2 < N^{\xi}$ be the unknown positive integers with $\left|N_s - \phi(N_s) - K\right| < N^{\gamma}$ for $0 < \gamma < 1$ and

$e = \min e_1 = N^{\beta}$ then $\left|\dfrac{N_s - K}{e_s} y^2 - x_s^2\right| < \dfrac{1 + N^{\xi}(N^{\gamma})}{N^{\beta}}$

$$< N^{\xi + \gamma - \beta}$$

To prove the existence of the unknown integers y and j integer x_s we let $\varepsilon = N^{\xi+\gamma-\beta}$ for $0 < \gamma, \beta < 1$ and $\xi = \dfrac{\beta j - \tau j}{(1+j)}$

$$N^{\xi}\varepsilon^j = N^{\xi}(N^{\xi+\gamma-\beta})^j = (1)^j$$
$$= N^{\xi + \xi j + \gamma j - \beta j}$$
$$= (1)^j$$

Which satisfied the theorem (2.4). therefore $(1)^j < 2\dfrac{\omega(\omega-3)}{4}.3^{\omega}$ for $w \geq 2$ which implies $N^{\xi}\varepsilon^j < 2\dfrac{\omega(\omega-3)}{4}3^{\omega}$ and if then $y < 2\dfrac{\omega(\omega-3)}{4}3^{\omega}.\varepsilon^{-\omega}$ for

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

$s = 1, 2, ... j$

$$\left| \frac{N_s K}{e_s} y^2 - x_s^2 \right| < \varepsilon$$

Hence we can obtain the stated unknown integer x and y_s for $s = 1, 2, ... j$ using the following computation

$$\frac{e_s x_s^2 - 1}{y^2} = \phi(N_s)$$

$$p_s^{r-1} = gcd(\phi(N_s), N_s)$$

$$q_s = N_s \Big/ p_s^r$$

Which yield the factorization of j prime power moduli $N_s = p_s^r q_s$ for $r > 2$ and $s = 1, 2, ... j$, in polynomial time.

Let :

$$H_{1,1} = \frac{N_1 - 2\lambda_1^{\frac{r}{r+1}} N_1^{\frac{r}{r+1}} - \lambda_1^{\frac{1}{r+1}} N_1^{\frac{1}{r+1}}}{e_1}$$

$$H_{1,2} = \frac{N_2 - 2\lambda_2^{\frac{r}{r+1}} N_2^{\frac{r}{r+1}} - \lambda_2^{\frac{1}{r+1}} N_2^{\frac{1}{r+1}}}{e_2}$$

$$H_{1,3} = \frac{N_3 - 2\lambda_3^{\frac{r}{r+1}} N_3^{\frac{r}{r+1}} - \lambda_3^{\frac{1}{r+1}} N_3^{\frac{1}{r+1}}}{e_3}$$

With lattice L spanned by the matrix.

$$W_1 = \begin{vmatrix} 1 - [T_1 \ H_{1,1}][T_1 \ H_{1,2}] - [T_1 \ H_{1,3}] \\ 0 \quad T_1 \quad 0 \quad 0 \\ 0 \quad 0 \quad T_1 \quad 0 \\ 0 \quad 0 \quad 0 \quad T_1 \end{vmatrix}$$

Algorithm 3

1. Initialization : the public key (N_s, e_s) satisfying theorem 3.3
2. Choose $r > 2, e = \min(e_s) = N^{\beta}$ and $N = \min\{N_s\}$ for $s = 1, 2, ... j$
3. For any $(N, \omega, \gamma, \beta) do$
4. $\varepsilon = N^{\xi + \gamma - \beta}$ for $\xi = \frac{\beta j - \gamma j}{1 + j} 0 < \gamma, \beta < 1$
5. $T_1 = \left\{ 3^{\omega+1} \times 2 \frac{(\omega+1)(\omega-4)}{4} . \varepsilon^{-\omega-1} \right\}$ for $\omega \geq 2.$
6. End for.
7. Consider the lattice L spanned by the matrix W_1

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

8. Appling the III algorithm to L for the reduce basis matrix K_1
9. For any $(W_1, K_1)do$
10. $R_1 = W_1^{-1}$
11. $C = R_1.k$
12. Compute $\phi(N_s) = \frac{e_s x_s^2 - 1}{y^2}$
13. $p_s^{r-1} = gcd(\phi(N_s)N_s)$
14. $q_s = N_s \big/ p_s^r$
15. Return the j prime factors (p_s, q_s).

IV. Conclusion

For p and q unbalance prime, we show that the prime power modulus N = $p^r q^s$ can be recovered in polynomial time through the proper utilizing equation of the form $ex^2 - \phi(N)y^2 = 1$ where e, N and $x, p, q, \varphi(N)$ are public key and private key tuples respectively. And we further to prove that If $\phi(N_s) = N_s - (2\lambda_s^{\frac{r}{r+1}} N_s^{\frac{r}{r+1}} - \lambda_s^{\frac{1}{r+1}} N_s^{\frac{1}{r+1}})$ was properly computed as an approximation of $\varphi(N)$ them one can simultaneously factored the generalize modulus $N = p_s^r q_s^s$ in polynomial time.

Reference

1. Batina, L.,et al., (2007). Public-key cryptography on the top of a needle. *IEEE International Symposium on Circuits and Systems,* pages 1831-1834.
2. Boneh, D. and Durfee, G. (1999). Cryptanalysis of RSA with private key d less than $N^{0.292}$. *Advances in Cryptology-EUROCRYPT'99*, 3(6), 1-11.
3. Chen, C.-Y., Hsueh, C.-C., and Lin, Y.-F. (2009). A generalization of de Weger's method. In Information Assurance and Security, IAS'09. *Fifth International Conference on, volume* 1, 344-347.
4. Coppersmith, D. (1997). Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10(4):233-260.
5. De Weger, B. (2002). Cryptanalysis of RSA with small prime difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17-28.
6. Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644-654.
7. Blomer J. and May A. (2004). A generalized Wiener attack on RSA, *In Public Key Cryptography - PKC 2004, Lecture Notes in Computer Science*, 1-13.
8. Lenstra, A. K., Lenstra, H. W., and Lovasz, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515-534.
9. Maitra, S. and Sarkar, S. (2008). Revisiting wieners attack new weak keys in RSA. *International Conference on Information Security*, 228-243.
10. May, A. (2003). New RSA vulnerabilities using lattice reduction methods. PhD thesis, University of Paderborn.
11. Asbullah M. A. and Ariffin, M. R. K. (2015). New attacks on RSA with modulus $N = p^2 q$ using continued fractions. *Journal of Physics, Conference Series, Volume 622, No. 1, IOP Publishing.*
12. 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.
13. Nitaj, A. (2013). Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem. *Artificial Intelligence,Evolutionary Computing and Metaheuristics*,139-168.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue I January 2023

14. Nitaj, A., Arin, M. R. K., Nassr, D. I., & Bahig, H. M. (2014). New Attacks on the RSA Cryptosystem. *Progress in Cryptology-AFRICACRYPT*. Springer International Publishing, 178-198.
15. Okamoto, T. and Uchiyama, S. (1998). A new public-key cryptosystem as secure as factoring. *International Conference on the Theory and Applications of Cryptographic Techniques*, 308-318.
16. Wiener, M. J. (1990). Cryptanalysis of short RSA secret exponents. *Information Theory, IEEE Transactions on*, 36(3):553-558.