Journal of Advances in Mathematics and Computer Science

Volume 38, Issue 8, Page 53-65, 2023; Article no.JAMCS.86626

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

Vulnerabilities of $ex^2 - y^2\phi(N) = z$ Using Modulus of the Form $N = p^r q^s$

Sadiq Shehu [a*], Buhari Auwalu Ibrahim [b], Aminu A. Ibrahim [b] and Ahmad Rufai [a]

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

[b] *Department of Mathematics, College of Science, Ummaru Ali Shinkafi Polytechnic Sokoto, Nigeria.*

Author's contribution

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JAMCS/2023/v38i81790

Open Peer Review History:

This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/86626

Received: 27/02/2022
Accepted: 29/04/2022
Published: 17/06/2023

Original Research Article

Abstract

The technical details of RSA works on the idea that it is easy to generate the modulus by multiplying two sufficiently large prime numbers together, but factorizing that number back into the original prime numbers is extremely difficult. Suppose that $N = p^r q^s$ are RSA modulus, where p and q are product of two large unknown of unbalance primes for $2 \leq s < r$. The paper proves that using an approximation of $\phi(N) \approx N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}$, private keys $\frac{x^2}{y^2}$ can be found from the convergents of the continued fractions expansion of

$$\left|\frac{e}{N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}} - \frac{y^2}{x^2}\right| < \frac{1}{2x^4}$$

*Corresponding author: E-mail: sadiqshehuzezi@gmail.com;

which leads to the factorization of the moduli $N = p^r q^s$ into unbalance prime factors p and q in polynomial time. The second part of this reseach report further, how to generalized two system of equations of the form $e_u x^2 - y_u^2 \phi(N_u) = z_u$ and $e_u x_u^2 - y^2 \phi(N_u) = z_u$ using simultaneous Diophantine approximation method and LLL algorithm to find the values of the unknown integers $x, y_u, \phi(N_u)$ and $x_u, y, \phi(N_u)$ respectively, which yeild to successful factorization of k moduli $N_u = p_u^r q_u^s$ for $u = 1, 2, \cdots k$ in polynomial time.

Keywords: Factorization; LLL algorithm; diophantine approximations; unbalance prime; continued fraction.

1 Introduction

The use of public-key cryptography differs dramatically from previous methods. All cryptographic systems have relied on the fundamental tools of substitution and permutation up to the present day [1],[2]. However, in contrast to typical single-key encryption, public-key algorithms are based on mathematical functions and are asymmetric in nature, requiring the usage of two keys. Several myths concerning public keys exist:

1. That public key encryption is more resistant to cryptanalysis than other types of encryption. In truth, the security of any system is determined by the length of the key and the computational labor required to crack the encryption [3],[4].
2. Single key encryption has been replaced with public key encryption. Due to the additional processing power required, this is improbable.
3. This is incorrect: key management is straightforward with public key cryptography[5].

A one-way function is a function that maps a domain into a range and has a unique inverse for each function value, with the constraint that the function is easy to calculate but the inverse is impossible:

$$Y = f(x) \quad easy$$
$$X = f^{-1}Y \quad infeasible$$

A problem is described as "easy" if it can be solved in polynomial time as a function of input length (n). For instance, the computation time is proportional to n^a, where a is a constant. However, the term "infeasible" is not properly defined. In general, if the effort to solve the problem is larger than polynomial time, the problem is infeasible, for example, if the time to compute is proportional to 2^n.
Trapdoor one-way functions are a family of invertible functions f_k such that $Y = f_k(X)$ is easy if k and X known, $X = f_k(Y)$ is easy if k and Y are known, and $X = f_k^{-1}(Y)$ is infeasible if Y is known but k is not known.

The discovery of an appropriate trapdoor one-way function is required for the construction of a workable public-key scheme.

The integer factorization problem was used to secure the RSA modulus $N = pq$ where p and q are positive big prime numbers of equal bit length. The key equation is $ed - k\phi(N) = 1$ where (e, N) and $(d, k, \phi(N), p, q)$ represent public and private keys, respectively. The key generation, encryption, and decryption methods in the RSA cryptosystem are detailed in [6]. Many factoring modulus $N = pq$ attacks can be found in [7], [8], [9], [10], [11], [12] among others. [13] was the first to report an RSA version for $r \geq 2$ that used the multi prime power modulus $N = p^r q$. Takagi claims to have proved that his method encrypted data faster than the traditional RSA modulus $N = pq$. Since then, numerous attacks on the moduli $N = p^r q$ for $rgeq2$ have been documented, using a variety of tactics detailed in [14], [15], [16] and [17]. Prime moduli $N = p^r q^s$ is one of the RSA cryptosystem variants that has been found to have higher decryption efficiency than regular RSA modulus $N = pq$, according to [18], [19]. Using complicated mathematics and logic, the cryptosystem enables secrecy and authenticity in digital communication channels. The integer factorization problem contains the cryptosystem's security. The prime power moduli go through the same key generation, encryption, and decryption operations as the normal

RSA cryptosystem, with the exception that the decryption phase is faster.

Lim (2000) described a cryptanalysis attack on prime power moduli $N = p^r q^s$, using Takagi's approach to discover prime factors (p, q) when $gcd(r, s) = 1$. They demonstrated that their technique decrypted data 15-times faster than the usual RSA cryptosystem, according to [19]. Lu (2015) published another partial key exposure attack on the moduli $N = p^r q^s$ where $gcd(r, s) = 1$, demonstrating that min $\left(\frac{l}{r+l}, \frac{2(r-l)}{r+l}\right)$ fraction of least significant bit(s) $(LSBs)$ or most significant bit(s)$(MSBs)$ of p is necessary to factor N in polynomial time [20].

Theorem 1.1. *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 count among the convergent of the continued fraction expansion of x.

Theorem 1.2. *(Simultaneous Diophantine Approximations) For given rational numbers of the type $\omega_1, ..., \omega_n$ and $0 < \varepsilon < 1$, there is a polynomial-time procedure to compute integers $p_1, ..., p_n$ and a positive integer q such that*

$$\max_i |q\omega_i - p_i| < \varepsilon \quad \text{and} \quad q \leq 2^{\frac{n(n-3)}{4}} [15].$$

2 Factoring $N = p^r q^s$ By Applying The Continued Fraction Method

In this section, we present results using continued fractions to factor multi prime power modulus $N = p^r q^s$ with $2 \leq s < r$ for some unknown parameters $(\phi(N), x, y, p, q)$ using one of the appropriate approximation of $\phi(N)$ given as $\phi(N) \approx N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}$ where (N, e) are public keys satisfying key equation $ex^2 - y^2\phi(N) = z$.

Let $N = p^r q^s$ be multi prime power moduli where p and q are unbalance prime numbers for $2 \leq s < r$. If $q < p < \lambda q$ and $q^s < p^r < \lambda q^s$, then

$$\lambda^{-\frac{1}{2r}} N^{\frac{1}{2r}} < q < N^{\frac{1}{2r}} < p < \lambda^{\frac{1}{2r}} N^{\frac{1}{2r}}$$

and approximation of

$$\phi(N) \approx N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}$$

Proof. Assume that $N = p^r q^s$, $q < p < \lambda q$ and $q^s < p^r < \lambda q^s$ for $2 \leq s < r$ with $\lambda > 2$, after that, multiplied by p^r yield $p^r q^s < p^{2r} < \lambda p^r q^s$ which implies $N < p^{2r} < \lambda N$, hence $N^{\frac{1}{2r}} < p < \lambda^{\frac{1}{2r}} N^{\frac{1}{2r}}$. Therefore, since $N = p^r q^s$, then $q^s = \frac{N}{p^r}$ as a result of which $\lambda^{-\frac{1}{2s}} N^{\frac{1}{2s}} < q < N^{\frac{1}{2s}}$. Since p and q are unbalance prime numbers, for $\lambda > 2$, we have

$$\lambda^{-\frac{1}{2r}} N^{\frac{1}{2r}} < q < N^{\frac{1}{2r}} < p < \lambda^{\frac{1}{2r}} N^{\frac{1}{2r}}.$$

Also, using the modulus $N = p^r q^s$ then th eulers totian function $\phi(N) = p^{r-1}q^{s-1}(p-1)(q-1)$, allawed us to yield an approximation of $\phi(N)$ using the primes $p \approx N^{\frac{1}{2r}}$ and $q \approx \lambda^{-\frac{-1}{2r}} N^{\frac{1}{2r}}$ as follows:

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

$$\begin{aligned}
\phi(N) &\approx N - \left(N^{\frac{r}{2r}}\lambda^{\frac{-s+1}{2r}}N^{\frac{s-1}{2r}} + N^{\frac{r-1}{2r}}\lambda^{\frac{-s}{2r}}N^{\frac{s}{2r}}\right) + N^{\frac{r-1}{2r}}\lambda^{\frac{-s+1}{2r}}N^{\frac{s-1}{2r}}\\
&\approx N - \left(N^{\frac{r}{2r}+\frac{s-1}{2r}}\lambda^{\frac{1-s}{2r}} + N^{\frac{r-1}{2r}+\frac{s}{2r}}\lambda^{\frac{-s}{2r}}\right) + N^{\frac{r-1}{2r}+\frac{s-1}{2r}}\lambda^{\frac{1-s}{2r}}\\
&\approx N - \left(N^{\frac{r+s-1}{2r}}\lambda^{\frac{1-s}{2r}} + N^{\frac{r-1+s}{2r}}\lambda^{\frac{-s}{2r}}\right) + N^{\frac{r-1+s-1}{2r}}\lambda^{\frac{1-s}{2r}}\\
\phi(N) &\approx N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}
\end{aligned}$$

This completes the proof. □

Theorem 2.1. *Let $N = p^r q^s$ be a multi prime power modulus, where p and q are unbalance prime numbers with $q < p < \lambda q$ and $q^s < p^r < \lambda q^s$ and $2 \leq s < r$ with $\lambda > 2$. Also, suppose that (e, N) and $(x, p, q, \phi(N))$ are tuples of public and private keys, respectively, such that $ex^2 - y^2\phi(N) = z$ where $1 < e < \phi(N) < N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}$ with $\gcd(x, y) = 1$ and $z < N^{\frac{1}{r}+\alpha}$. Let $\mu = p^{r-2}q^{s-2}(p-1)(q-1)$ become well-known. If $p \approx N^{\frac{1}{2r}}$ and $q \approx \lambda^{-\frac{1}{2r}}N^{\frac{1}{2r}}$ and $z < N^{\frac{1}{r}+\alpha}$ then*

$$x < \frac{N^{\frac{1}{2}} - N^{\frac{r+s-1}{4r}}\left(\lambda^{\frac{1-s}{4r}} + \lambda^{\frac{-s}{4r}}\right) + N^{\frac{r+s-2}{4r}}\lambda^{\frac{1-s}{4r}}}{\sqrt{2N^{\frac{1+2\alpha r}{2r}}}}$$

and $\left|\frac{e}{N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}} - \frac{y^2}{x^2}\right| < \frac{1}{2x^4}$, as a result of which N is factorized into unbalance prime factors p and q in polynomial time.

Proof. Assume that $N = p^r q^s$ for $2 \leq s < r$ be multi prime power modulus satisfying $q < p < \lambda q$ and $q^s < p^r < \lambda q^s$,with $z = N^{\frac{1}{r}+\alpha}$ then $ex^2 - y^2\phi(N) = z$ where $\phi(N) = p^{r-1}q^{s-1}(p-1)(q-1)$,can be rewritten as

$$\begin{aligned}
ex^2 - y^2(p^{r-1}q^{s-1}(p-1)(q-1)) &= z\\
ex^2 - y^2\left(N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}\right) &= z
\end{aligned}$$

Dividing by $x^2\left(N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}\right)$ gives

$$\begin{aligned}
&\left|\frac{e}{\left(N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}\right)} - \frac{y^2}{x^2}\right|\\
&= \left|\frac{z}{x^2\left(N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}\right)}\right|\\
&= \frac{N^{\frac{1}{r}+\alpha}}{x^2\left(N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}\right)}
\end{aligned}$$

Therefore, from Theorem 1.1 we can write

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

then

$$x < \frac{N^{\frac{1}{2}} - N^{\frac{r+s-1}{4r}}\left(\lambda^{\frac{1-s}{4r}} + \lambda^{\frac{-s}{4r}}\right) + N^{\frac{r+s-2}{4r}}\lambda^{\frac{1-s}{4r}}}{\sqrt{2N^{\frac{1+2\alpha r}{2r}}}}.$$

Algorithm 1 : An ouline on how Theorem 2.1 works

```
Initialization: The public key pair $(N, e)$ and $\mu$ satisfying Theorem 2.1.
Choose $r$, $s$, to be appropriate modest positive integers where $2 \leq s < r$.
**for any** $(r, s)$ **do**
    The convergents $\frac{y^2}{x^2}$ of the continued fractions expansion of
$\frac{e}{\frac{e}{\left(N-N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}}+\lambda^{\frac{-s}{2r}}\right)+N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}\right)}}$.
**end for**
Compute $\phi(N) := \frac{ex^2-z}{y^2}$
Compute $G := \gcd(\phi(N), N)$
Compute $p^{r-2} := \gcd(\mu, G)$
Compute $q^s := \frac{N}{p^r}$
**return** prime factors $p$ and $q$.
```

Hence $\frac{y^2}{x^2}$ can be obtained from the convergents of the continued fractions expansion of $\frac{e}{\left(N-N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}}+\lambda^{\frac{-s}{2r}}\right)+N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}\right)}$.

□

2.1 System of Equations Using $N_u - N_u^{\frac{r+s-1}{2r}}\left(\lambda_u^{\frac{1-s}{2r}} + \lambda_u^{\frac{-s}{2r}}\right) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}$ as Approximation of $\phi(N)$

In this section, we show that if $e_U < \phi(N_U) < N_u - N_u^{\frac{r+s-1}{2r}}\left(\lambda_u^{\frac{1-s}{2r}} + \lambda_u^{\frac{-s}{2r}}\right) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}$, then $N_u = p_u^r q_u^s$, can be factored utilizing Diophantine Approximation and lattice basis reduction approaches at the same time. for $u = 1, ..., k$ and $2 \leq s < r$.

Theorem 2.2. *Let $N_u = p_u^r q_u^s$ for $u = 1, 2, \ldots, k$ be the multi prime power moduli with unbalance prime factors p and q such that $q < p < \xi q$, $q^s < p^r < \lambda q^s$ $2 \leq s < r$, $\lambda > 2$. Suppose that $Y_u = p_u^{r-2} q_u^{s-2}(p_u - 1)(q_u - 1)$ be known. Let (e_u, N_u) and $(x, p_u, q_u, \phi(N_u))$ be public and private key tuples respectively. If $1 < e_u < \phi(N_u) < \left(N_u - N_u^{\frac{r+s-1}{2r}}\left(\lambda_u^{\frac{1-s}{2r}} + \lambda_u^{\frac{-s}{2r}}\right) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)$ and $N = \min\{N_i\}$, with existance of the unknown positive integers $x, y_i < N^\alpha$, define $\alpha = \frac{2(\omega)-(\Lambda\omega)-2\delta\omega}{2(1+3\omega)}$ for $0 < \Lambda, \delta < 1$ satisfying the generalige equation $e_u x^2 - y_u^2(\phi(N_u)) = z_u$, then k prime power moduli N_u can be recovered concurrently in polynomial time for $u = 1, ..., k$.*

Proof. Suppose $N_u = p_u^r q_u^s$ be k multi prime power moduli for $r, s > 0$ and $r > s$ with $N = \min\{N_u\}$, let $G = N_u^{\frac{r+s-1}{2r}}\left(\lambda_u^{\frac{1-s}{2r}} + \lambda_u^{\frac{-s}{2r}}\right)$ if $y_i < N^\alpha$, then $e_i x^2 - y_u^2\phi(N_u) = z_u$ can be rewritten as

$$\begin{aligned} e_u x^2 - y_u^2(p_u^{r-1} q_u^{s-1}(p_u - 1)(q_u - 1)) &= z_u \\ e_u x^2 - y_u^2\left(N_u - N_u^{\frac{r+s-1}{2r}}\left(\lambda_u^{\frac{1-s}{2r}} + \lambda_u^{\frac{-s}{2r}}\right) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right) &= z_u \\ e_u x^2 - y_u^2\left(N_u - G + G - \left(N_u - \phi(N_u) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)\right) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}} &= z_u \end{aligned}$$

$$e_u x^2 - y_u^2\left(N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}\right) = z_u + y_u^2\left(G - N_u + \phi(N_u) - N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)$$

$$\left|\frac{e_u}{N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}}x^2 - y_u^2\right| = \frac{\left|z_u + y_u^2\left(G - N_u + \phi(N_u) - N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)\right|}{N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}}.$$

Suppose $N = \min\{N_i\}$ and $y_i < N^{\alpha}$, $\left|N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}\right| > \frac{r}{r+1}N$, for $r, s > 0$ with $r > s$ and $\left|G - N_u + \phi(N_u) - N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right| < N^{\alpha+\frac{1}{2}\Lambda}$ for $0 < \alpha, \Lambda < 1$, $z_i < N^{\frac{1}{r}+\alpha} < N^{\delta}$

$$\begin{aligned}\left|\frac{z_u + y_u^2\left(G - N_u + \phi(N_u) - N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)}{N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}}\right| &\leq \left|\frac{N^{\delta} + (N^{\alpha})^2\left(N^{\alpha+\frac{1}{2}\Lambda}\right)}{\frac{r}{r+1}N}\right| \\ &\leq \frac{N^{\delta} + (N^{2\alpha})\left(N^{\alpha+\frac{1}{2}\Lambda}\right)}{\frac{r}{r+1}N} \\ &\leq \frac{N^{\delta} + N^{3\alpha+\frac{\Lambda}{2}}}{\frac{r}{r+1}N} \\ &< \frac{(r+1)N^{3\alpha+\frac{\Lambda}{2}+\delta}}{rN} \\ &< \left(\frac{r+1}{r}\right)N^{3\alpha+\frac{\Lambda}{2}+\delta-1}\end{aligned}$$

This implies

$$\left|\frac{e_u}{N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}}x^2 - y_u^2\right| < \left(\frac{r+1}{r}\right)N^{3\alpha+\frac{\Lambda}{2}+\delta-1}.$$

For the unknown integer positive integer x, we assume that $\varepsilon = \left(\frac{r+1}{r}\right)N^{3\alpha+\frac{\Lambda}{2}+\delta-1}$, with $\alpha = \frac{2(k)-(\Lambda k)-2\delta k}{2(1+3k)}$, then

$$N^{\alpha}\varepsilon^k = N^{\alpha}\left(\frac{r+1}{r}\right)^k\left(N^{3\alpha+\frac{\Lambda}{2}+\delta-1}\right)^k = \left(\frac{r+1}{r}\right)^k$$

For $\left(\frac{r+1}{r}\right)^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$ with $k \geq 2$, we get $N^{\alpha}\varepsilon^k < 2^{\frac{k(k-3)}{4}} \cdot 3^k$. It follows that if $x < N^{\alpha}$ then $x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}$. Hence

$$\left|\frac{e_u}{N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}}x^2 - y_u^2\right| < \varepsilon, \qquad x < 2^{\frac{k(k-3)}{4}} \cdot 3^k \cdot \varepsilon^{-k}.$$

Using Theorem 1.2, we can obtained the unknown integers x and y_u. This can be shown by looking at $e_u x^2 - y_u^2\phi(N_u) = z_u$ we get

$$\begin{aligned}\phi(N_u) &= \frac{e_u x^2 - z}{y_u^2} \\ \gcd(\phi(N_u), N_u) &= R_u \\ p_u^{r-2} &= \gcd(Y_u, R_u) \\ q_u^s &= \frac{N_u}{p_u^r}.\end{aligned}$$

Finally, in polynomial time, the prime factors (p_u, q_u) of the prime power moduli N_u may be discovered concurrently. for N_u for $u = 1, \ldots, k$. □

Let

$$\varDelta_1 = \frac{e_1}{N_1 - G_1 + \lambda_1^{\frac{1-s}{2r}} N_1^{\frac{r+s-2}{2r}}}, \ \varDelta_2 = \frac{e_2}{N_2 - G_2 + \lambda_2^{\frac{1-s}{2r}} N_2^{\frac{r+s-2}{2r}}}$$

$$\varDelta_3 = \frac{e_3}{N_3 - G_3 + \lambda_3^{\frac{1-s}{2r}} N_3^{\frac{r+s-2}{2r}}}$$

Algorithm 2 : An ouline on how Theorem 2.2 works

```
Initialization: The public key pair $(N_u, e_u)$ and $Y_{2u}$ satisfying Theorem 2.2.
Choose $r, s, t \geq 2$, $r > s$ and $N = \max\{N_u\}$ for $u = 1, \dots, k$.
for any $(N, \omega, \varLambda)$ do
    $\varepsilon := \left(\frac{r+1}{r}\right) N^{3\alpha + \frac{\varLambda}{2} + \delta - 1}$ where $\alpha = \frac{2(k) - (\varLambda k) - 2\delta k}{2(1+3k)}$
    $\xi := [3^{k+1} \times 2^{\frac{(k+1)(k-4)}{4}} \times \varepsilon^{-k-1}]$ for $k \geq 2$.
end for
Considering the $\mathcal{L}$ lattice spanned by the matrix $T$, as shown below.
The reduced basis matrix $A$ is obtained using the LLL algorithm on $\mathcal{L}$.
for any $(T, A)$ do
    $L := T^{-1}$
    $S = LA$.
end for
Recover $x$, $y_u$ from $S$
for each triplet $(x, y_u, e_u)$ do
    $\phi(N_u) := \frac{e_u x^2 - z_u}{y_u^2}$
    $R_u := \gcd(\phi(N_u), N_u)$
    $p_u^{r-2} := \gcd(Y_{2u}, R_u)$
    $q_u^s := \frac{N_u}{p_u^r}$
end for
return the essential factors $(p_u, q_u)$ back.
```

Example 2.3. *We look at the three prime power moduli and their three public exponents.*

$$N_1 = 687491161857965680563093016235875019348393973541176124176392423862 1$$

$$N_2 = 1057223455152130639863520469642754020435834421033251045699872997$$

$$N_3 = 571027477435873329018936776465149417766747906589423518381163537911$$

$$e_1 = 219267129246669196531085440608365300865809881557724681352263444427 3$$

$$e_2 = 939495933919169375962742697129622498560733359703983195160914413$$

$$e_3 = 270024722603295990753712468131199332235272856973239055160027243832$$

Let the following integers be known

$$Y_{21} = 4973169933189448234042417963391255327906 4$$

$$Y_{22} = 226786308539887749360745853036376059808$$

$$Y_{23} = 8780072321323534641793573970486243467484$$

Then $N = \min(N_1, N_2, N_3) = 6874911618579656805630930162358750193483939735411761241763924238621$, $k = 3$ *with* $\alpha = \frac{2(k)-(\Lambda k)-2\delta k}{2(1+3k)} = 0.1050630000$ *and* $\varepsilon := \left(\frac{r+1}{r}\right) N^{3\alpha+\frac{\Lambda}{2}+\delta-1} = 0.006084582790$*. Using Theorem 1.1, we obtain*

$$\xi = [3^{k+1} \cdot 2^{\frac{(k+1)(k-4)}{4}} \cdot \varepsilon^{-k-1}] = 29548252700$$

Consider the lattice $\mathcal{L}$ *spanned by the matrix*

$$T = \begin{bmatrix} 1 & -[\xi\Delta_1] & -[\xi\Delta_2] & -[\xi\Delta_3] \\ 0 & \xi & 0 & 0 \\ 0 & 0 & \xi & 0 \\ 0 & 0 & 0 & \xi \end{bmatrix}$$

As a result, using the LLL algorithm to $\mathcal{L}$*, We get the decreased basis as shown below.*

$$A = \begin{bmatrix} 25479047 & 26037627 & 17974538 & 25718111 \\ 52727986 & -28856574 & 6093144, & 20699382 \\ 2923909 & 20860269 & 69662086 & -55628983 \\ 35984242 & 54428522 & -51636432 & -46473154 \end{bmatrix}$$

Next, we compute

$$S = \begin{bmatrix} 25479047 & 8126239 & 22641818 & 12048409 \\ 52727986 & 16816964 & 46856441 & 24933756 \\ 2923909 & 932546 & 2598316 & 1382644 \\ 35984242 & 11476746 & 31977203 & 17016055 \end{bmatrix}$$

Then, from the first row of matrix S *we get* $x = 25479047$, $y_1 = 8126239$, $y_2 = 22641818$, $y_3 = 12048409$*. Hence using* x *and* y_u *for* $u = 1, 2, 3$*, we compute* $V_u = \frac{e_u x^2 - z_u}{y_u^2} = \phi(N_u) = p_u^{r-1} q_u^{s-1}(p_u - 1)(q_u - 1)$

$$V_1 = 6874911618561746771006566386093552126548469304525378061406197697288$$

$$V_2 = 10572234551410761596580005823327621807173945849386164095442826 56$$

$$V_3 = 5710274774346837747063039941622856555078045724249098473215780329 88$$

Algorithm 2 is used to produce $R_u = \gcd(\phi(N_u), N_u)$ *and* $p_u^{r-2} = \gcd(Y_u, R_u)$*, for* $i = 1, 2, 3$

$$R_1 = 4973169933202403985423393760875815706326 3$$

$$R_2 = 22678630854225905955675600451973411232 1$$

$$R_3 = 87800723213418251327205238043305200144 23$$

$$p_1 = 359748903791989$$

$$p_2 = 48648211020653$$

$$p_3 = 135001682080439$$

Finally, we compute $q_u^s := \frac{N_u}{p_u^r}$ *for* $u = 1, 2, 3$*, that is*

$$q_1 = 384268106903, q_2 = 95825938969, q_3 = 481747793063.$$

This results in polynomial time factorization of three moduli N_1*,* N_2*, and* N_3*.*

Theorem 2.4. *Let* $N_u = p_u^r q_u^s$ *for* $r, s > 2$*,* $r > s$ *with* $1 \leq u \leq k$ *be* k *multi prime power moduli using unbalance prime* p *and* q *such that* $q < p < \lambda q$ *for* $\lambda > 2$ *and* $M_u = p_u^{r-2} q_u^{s-2}(p_u - 1)(q_u - 1)$ *be an integer that is well-known, and* (e_u, N_u) *are* k *public key exponents and* $(x_u, p_u, q_u, \phi(N_u))$ *be the corresponding private keys tuples with* $e_i < \phi(N_i) < \left(N_u - N_u^{\frac{r+s-1}{2r}}\left(\lambda_u^{\frac{1-s}{2r}} + \lambda_u^{\frac{-s}{2r}}\right) + N_u^{\frac{r+s-2}{2r}} \lambda_u^{\frac{1-s}{2r}}\right)$*. Suppose that* $e = \min\{e_i\} = N^{\beta}$ *and* $N = \min\{N_i\}$ *for* $0 < \beta < 1$*. satisfying* $e_u x_u^2 - y^2(\phi(N_u)) = z_u$ *. If there exist an unknown positive integer* $y < N^{\alpha}$ *and* k *integer* $x_u < N^{\alpha}$ *for all* $\alpha = \frac{2\beta k-\Lambda k-2\delta k}{2(1+3k)}$*, then prime factors* p_u *and* q_u *of* k *prime power moduli* N_u *can be discovered in polynomial time for* $u = 1, \cdots, k$ *and* $0 < \Lambda, \delta < 1$*.*

Proof. Suppose $N_u = p_u^r q_u^s$ be k multi prime power moduli and $N = \max\{N_u\}$,$e = \min\{e_u\} = N^{\beta}$, then $e_u x_u^2 - y^2\phi(N_u) = z_u$ can be rewritten as

$$\begin{aligned}
e_u x_u^2 - y^2(p_u^{r-1}q_u^{s-1}(p_u-1)(q_u-1)) &= z_u \\
e_u x_u^2 - y^2\left(N_u - N_u^{\frac{r+s-1}{2r}}\left(\lambda_u^{\frac{1-s}{2r}} + \lambda_u^{\frac{-s}{2r}}\right) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right) &= z_u \\
e_u x_u^2 - y^2\left(N_u - G + G - \left(N_u - \phi(N_u) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)\right) + N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}} &= z_u
\end{aligned}$$

$$e_u x_u^2 - y^2\left(N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}\right) = z_u + y^2\left(G - N_u + \phi(N_u) - N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)$$

$$\left|\frac{N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}}{e_u}x_u^2 - y^2\right| = \frac{\left|z_u + y^2\left(G - N_u + \phi(N_u) - N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)\right|}{e_u}.$$

Suppose $N = \min\{N_u\}$,and $x_u, y < N^{\alpha}$ are positive numbers for $u = 1, 2, \ldots, k$, $e = \min\{e_u\} = N^{\beta}$ for $r, s > 0$ with $r > s$ and $\left|z_u + y^2\left(G - N_u + \phi(N_u) - N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)\right| < N^{\alpha+\frac{1}{2}\Lambda}$ for $0 < \Lambda < 1$, $z_u < N^{\frac{1}{r}+\alpha} < N^{\delta}$

$$\begin{aligned}
\left|\frac{z_u + y^2\left(G - N_u + \phi(N_u) - N_u^{\frac{r+s-2}{2r}}\lambda_u^{\frac{1-s}{2r}}\right)}{e_i}\right| &\leq \left|\frac{\left(N^{\delta} + N^{2\alpha}N^{\alpha+\frac{1}{2}\Lambda}\right)}{N^{\beta}}\right| \\
&< \frac{N^{3\alpha+\frac{\Lambda}{2}+\delta}}{N^{\beta}} \\
&< \frac{r}{r+1}N^{3\alpha+\frac{\Lambda}{2}+\delta-\beta}
\end{aligned}$$

This implies

$$\left|\frac{N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}}{e_u}x_u^2 - y^2\right| < \frac{r}{r+1}N^{3\alpha+\frac{\Lambda}{2}+\delta-\beta}.$$

For the unknown integer positive integer x, we assume that $\varepsilon = \frac{r}{r+1}N^{3\alpha+\frac{\Lambda}{2}+\delta-\beta}$, with $\alpha = \frac{2\beta k - \Lambda k - 2\delta k}{2(1+3k)}$, then

$$N^{\alpha}\varepsilon^{k} = \left(\frac{r}{r+1}\right)^{k} N^{\alpha+3\alpha k+\frac{\Lambda k}{2}+\delta k-\beta k} = \left(\frac{r}{r+1}\right)^{k}$$

For $\left(\frac{r}{r+1}\right)^{k} < 2^{\frac{k(k-3)}{4}} \cdot 3^{k}$ with $k \geq 2$, we get $N^{\alpha}\varepsilon^{k} < 2^{\frac{k(k-3)}{4}} \cdot 3^{k}$. It follows that if $y < N^{\alpha}$ then $y < 2^{\frac{k(k-3)}{4}} \cdot 3^{k} \cdot \varepsilon^{-k}$. Hence

$$\left|\frac{N_u - G + \lambda_u^{\frac{1-s}{2r}} N_u^{\frac{r+s-2}{2r}}}{e_u}x_u^2 - y^2\right| < \varepsilon, \qquad y < 2^{\frac{k(k-3)}{4}} \cdot 3^{k} \cdot \varepsilon^{-k}.$$

We can get the unknown parameters x and y_u using Theorem 1.2. This can be shown by looking $e_u x_u^2 - y^2\phi(N_u) = z_u$ we get

$$\begin{aligned}
\phi(N_u) &= \frac{e_u x_u^2 - z_u}{y^2} \\
\gcd(\phi(N_u), N_u) &= H_u \\
p_i^{r-2} &= \gcd(M_u, H_u) \\
q_u^{s} &= \frac{N_u}{p_u^{r}}.
\end{aligned}$$

Finally, for N_u, the prime factors (p_u, q_u) of the prime power moduli N_u may be discovered simultaneously in polynomial time for $u = 1, \dots, k$. □

Let

$$\Delta_4 = \frac{N_1 - G + \lambda_1^{\frac{1-s}{2r}} N_1^{\frac{r+s-2}{2r}}}{e_1}, \ \Delta_2 = \frac{N_2 - G + \lambda_2^{\frac{1-s}{2r}} N_2^{\frac{r+s-2}{2r}}}{e_2}$$

$$\Delta_3 = \frac{N_3 - G + \lambda_3^{\frac{1-s}{2r}} N_3^{\frac{r+s-2}{2r}}}{e_3}$$

Example 2.5. *We look at the three prime power moduli and their three public exponents.*

$N_1 = 22795749055483621927678226321205433734051338306276296130260787691492306384151304422492765844 9$

$N_2 = 3554411814954353436327829133360230405934550757667338273784791207076143108174479058991431267$

$N_3 = 12563684360130557914543205114177450582145868061677715240442851276342568213990275850644825303$

$e_1 = 8964315903484244209676371804096186424147682321763959913965430256384936632222631188116 60329722$

$e_2 = 262488792749681874783498844039691918361725299202443514287223197874415184706882694351 3443976$

$e_3 = 25458037772397631853474166271558261532396437778643313308829415967084500100595366231398196544$

Also, let

$$M_{21} = 4372516634902392534157696086344369086638329809432661 00720$$
$$M_{22} = 4989396742845338821065245453312862844518312120738379 8000$$
$$M_{23} = 9312975947818087121426896928323219596707133448033725 5520$$

Then, one can observe that

$N = \min\{N_1, N_2, N_3\} = 2624887927496818747834988440396919183617252992024435142872231978744151847068826943513443976$

and $\min\{e_1, e_2, e_3\} = N^\beta$ *with* $\beta = 0.9$ *and* $k = 3$ *we get* $\varepsilon = \frac{r}{r+1} N^{3\alpha + \frac{\Lambda}{2} + \delta - \beta} = 0.01145936875$ *and* $\alpha = \frac{2\beta k - \Lambda k - 2\delta k}{2(1+3k)} = 0.06016185000$*. Using Algorithm 3, we compute*

$$\xi = [3^{k+1} \cdot 2^{\frac{(k+1)(k-4)}{4}} \cdot \varepsilon^{-k-1}] = 2348617238.$$

Consider the lattice $\mathcal{L}$ *spanned by the matrix*

$$C = \begin{bmatrix} 1 & -[\xi\Delta_1] & -[\xi\Delta_2] & -[\xi\Delta_3] \\ 0 & \xi & 0 & 0 \\ 0 & 0 & \xi & 0 \\ 0 & 0 & 0 & \xi \end{bmatrix}$$

As a result, using the LLL algorithm to $\mathcal{L}$*, We get the decreased basis as shown below*

$$T = \begin{bmatrix} 541467 & -492004 & -43415 & -293812 \\ -5530693 & -9947612 & 4564085 & 5191518 \\ -12248412 & -711876 & 15126694 & -22918192 \\ -23106392 & -13752150 & -28045762 & -15716484 \end{bmatrix}$$

Next, we compute

$$L = \begin{bmatrix} 541467 & 137692 & 733211 & 267217 \\ -5530693 & -1406424 & -7489219 & -2729428 \\ -12248412 & -3114702 & -16585813 & -6044660 \\ -23106392 & -5875825 & -31288815 & -11403134 \end{bmatrix}$$

Algorithm 3 Theorem 2.4

```
Initialization: The public key tuple $(N_u, e_u)$ and $M_u$ satisfying Theorem 2.4.
Choose $r, s, t \geq 2$, $r > s$ and $N = \max\{N_u\}$ for $u = 1, \ldots, k$.
for any $(N, k, \Lambda, \beta, \delta)$ do
    $\varepsilon = \frac{r}{r+1} N^{3\alpha + \frac{\Lambda}{2} + \delta - \beta}$, where $\alpha = \frac{2\beta k - \Lambda k - 2\delta k}{2(1+3k)}$
    $\xi := [3^{k+1} \times 2^{\frac{(k+1)(k-4)}{4}} \times \varepsilon^{-k-1}]$ for $k \geq 2$.
end for
Considering the $\mathcal{L}$ lattice spanned by the matrix $C$, as shown below
The reduced basis matrix $T$ is obtained using the LLL algorithm on $\mathcal{L}$.
for any $(C, T)$ do
    $Q := C^{-1}$
    $L = QT$.
end for
Recover $x_u$, $y$ from $L$
for each triplet $(x_u, y, e_u)$ do
    $\phi(N_u) := \frac{e_u x_u^2 - Z_u}{y^2}$
    $W_u := \gcd(\phi(N_u), N_u)$
    $p_u^{r-2} := \gcd(M_u, W_u)$
    $q_u^s := \frac{N_u}{p_u^r}$
end for
return the essential factors $(p_u, q_u)$.
```

The first row of the matrix L yields $y = 541467$, $x_1 = 137692$, $x_2 = 733211$, $x_3 = 267217$. Hence using x_u, y and Algorithm 3, we compute $A_u = \frac{e_u x_u^2 - z_u}{y} = \phi(N_u) = p_u^{r-1} q_u^{s-1}(p_u - 1)(q_u - 1)$, $W_u = \gcd(\phi(N_u), N_u)$ and $p_u^{r-2} = \gcd(M_i, W_u)$, for $u = 1, 2, 3$.

$A_1 = 22795749055483576168423172353063291042921224640621185935130451585454971305065655590352714 7296$

$A_2 = 3554411814954318492020455003484728545856330456953476602527009183139468000711366846142754000$

$A_3 = 1256368436013049362378465592286692258605303539069921205252669146314811219036578771791346 7040$

$W_1 = 4707361273664432054082823665675708876104404704582966 78949$

$W_2 = 49893967428453878730666651905260947623790311831323299329$

$W_3 = 93129759478181347776932335477425532246405296652124251489$

$p_1 = 9720781759292579494 49$

$p_2 = 7003712893587672533 23$

$p_3 = 690335084188136980007$

Finally, we compute $q_u^s := \frac{N_u}{p_u^r}$ for $u = 1, 2, 3$ which gives

$$q_1 = 498167216902549, q_2 = 101716491133001, q_3 = 195419811496561.$$

This results in polynomial time factorization of three moduli N_1, N_2, and N_3.

3 Conclusion

In this research we launch some cryptanalytic attacks on the RSA prime power modulus $N = p^r q^s$. Hence we shows that $\frac{y^2}{x^2}$ is among the convergents of the continued fraction expansion of $\frac{e}{\left(N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}\right)}$ for $N - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{1-s}{2r}} + \lambda^{\frac{-s}{2r}}\right) + N^{\frac{r+s-2}{2r}}\lambda^{\frac{1-s}{2r}}$ as approximation of $\phi(N)$, which allows us to factored the unbalance prime power modulus $N = p^r q^s$ if $x < \frac{N^{\frac{1}{2}} - N^{\frac{r+s-1}{4r}}\left(\lambda^{\frac{1-s}{4r}} + \lambda^{\frac{-s}{4r}}\right) + N^{\frac{r+s-2}{4r}}\lambda^{\frac{1-s}{4r}}}{\sqrt{2N^{\frac{1+2\alpha r}{2r}}}}$, in polynomial time. Furthermore for j public keys $(N_u, e_u, M_u or Y_u)$ where $M_u = Y_u = p_u^{r-2} q_u^{s-2}(p_u - 1)(q_u - 1)$ we were able to recovered the unknown parameters x, x_u, y, y_u through LLL algorithm which enable us to factored k multi prime power moduli $N_u = p_u^r q_u^s$ for $u = 1, 2, 3$ simultaneously in polynomial time.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Coron JS, Zeitoun R. Improved factorization of $N = p^r q^s$. Cryptographers' Track at the RSA Conference. Springer, Cham. 2018;65–79.

[2] Lenstra AK , Lenstra HW, Lovasz L. Factoring polynomials with rational coefficients. Mathematische Annalen. 1982;261:513-534.

[3] Wang S, Qu L, Li C, Wang H. Further Improvement to Factoring $N = p^r q^s$ with Partial Known Bits. Adv. in Math. of Comm. 2019;13(1):21–135.

[4] Asbullah MA, Ariffin MRK. New Attacks on RSA with Modulus $N = p^2 q$ Using Continued Fractions. Journal of Physics, Conference Series. 2015;622(1)IOP Publishing.

[5] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978;21(2):120–126.

[6] Nitaj Abderrahmane. The Mathematical Cryptography of the RSA Cryptosystem; 2012.

[7] Wiener M. Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory. 1990;36:553–558.

[8] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory. 1976;22(6):644–654.

[9] De Weger B. Cryptanalysis of RSA with Small Prime Difference. Applicable Algebra in Engineering Communication and Computing. 2002;13(1).

[10] Maitra S, Sarkar S. Revisiting Wieners attack new weak keys in RSA. In International Conference on Information Security;2008.

[11] May A. New RSA Vulnerabilities Using Lattice Reduction Methods. PhD. thesis, University of Paderborn; 2003.

[12] Nitaj Abderrahmane, Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem. Artificial Intelligence, Evolutionary Computing and Metaheuristics. 2013;139-168.

[13] Takagi T. Fast RSA-type cryptosystem modulo $p^k q$. Advances in Cryptology-CRYPTO 1998. Springer Berlin Heidelberg. 1998:318–326.

[14] Sarkar S. Small Secret Exponent Attack on RSA Variant with Modulus $N = p^2 q$. In Proc. Int. Workshop on Coding and Cryptography –WCC. 2013;215–222.

[15] Nitaj Abderrahmane, Tajjeeddine Rachidi. New Attacks on RSA with Moduli $N = p^r q$, Codes, Cryptology, and Information Security, Springer International Publishing. 2015;352-360.

[16] Sarkar S. Revisiting Prime Power RSA. Discrete Applied Mathematics. 2016;203:127–133.

[17] Sadiq Shehu, Muhammad Rezal Kamel Ariffin, New Attacks on Prime Power $N = p^r q$ Using Good Approximation of $\phi(N)$. Malaysian Journal of Mathematical Science. 2016;11(S):121–136.

[18] Coron JS, Faug‘ere JC, Renault G, Zeitoun R. Factoring $N = p^r q^s$ for large r and s. Cryptographers' Track at the RSA Conference, Springer, Cham. 2016;9610:448–464.

[19] Lim S, Kim S, Yie I, Lee H. A generalized Takagi-cryptosystem with a modulus of the form $p^r q^s$. Progress in Cryptology-INDOCRYPT 2000. Springer Berlin Heidelberg. 2000;1977:283–294.

[20] Lu Y, Peng L, S. Sarkar. Cryptanalysis of an RSA variant with moduli $N = p^r q^l$. The 9th International Workshop on Coding and Cryptography. WCC;2015.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://www.sdiarticle4.com/review-history/86626