Improved Polynomial Attacks For Breaking Modulus of the Form $N = p^r q^s$

Abstract

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

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

then

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

, which leads to the factorization of the moduli $N = p^r q^s$ in polynomial time . We present the second attacks on j multi prime power moduli $N_i = p_i^r q_i^s$ for $i = 1, 2, \ldots, j$ and transform the system of equation into simultaneous Diophantine approximation problem from which we apply lattice basis reduction techniques to find the parameters (x, y_i) or (y, x_i), lead to successful factorization of j moduli N_i simultaneously in polynomial time.

Keywords: Unbalance Prime Numbers, Factorization, LLL algorithm, Diophantine approximations, Continued fraction

1 Introduction

The concept of Public key evolved from an attempt to solve two problems, key distribution and the development of digital signatures. In 1976 Whitfield Diffie and Martin Hellman achieved great success in developing the conceptual framework. For conventional encryption the same key is used for encryption and decryption. This is not a necessary condition. Instead it is possible to develop a cryptographic system that relies on one key for encryption and a different but related key for decryption. Furthermore these algorithms have the following important characteristic: It

is computationally infeasible to determine the decryption key given only knowledge of the algorithm and the encryption key. In addition, some algorithms such as RSA, also exhibits the following characteristics: Either of the two related keys can be used for encryption, with the other used for decryption
Illustrates the Public key process. The steps are:

1. Each system generates a pair of keys.
2. Each system publishes its encryption key (public key) keeping its companion key private.
3. If A wishes to send a message to B it encrypts the message using Bs public key.
4. When B receives the message, it decrypts the message using its private key. No one else can decrypt the message because only B knows its private key.

Public key cryptography is being considered and regarded as one of the major breakthrough in the field of information security. Transmission of information electronically is sometimes exposed to the threat of being attacked by eavesdroppers; this can be tackled through construction of strong encryption schemes. Among the public key cryptosystems, RSA cryptosystem invented by Rivest, Shamir and Adleman is regarded as fast growing, reliable and applicable cryptosystem due to its efficiency in providing confidentiality, integrity of the data being transmitted in an insecure communication channels and verification of the entities involved in communication [1].

Multi prime power modulus $N = p^r q$ for $r \geq 2$ is one of the most important RSA variants in the cryptanalytic Attack as reported by Takagi (1998). Base on his conclusion the scheme performed decryption process faster than standard RSA modulus $N = pq$, [9]. Since then, several cryptanalytic attacks on the moduli $N = p^r q$ for $r \geq 2$ and $N = p^r q^s$ $r, s \geq 2$ with $r > s$ have been reported using various techniques which can be found in [19], [20], [10], [11], [12] and [13]. The prime power moduli $N = p^r q^s$ is count among the variants types of RSA cryptosystem reported with high level efficiency in both the encryption and decryption process over standard RSA modulus $N = pq$, [14]. The cryptosystem provides observed all cryptographic goal such as privacy and authentication in the digital communication channels using complex mathematics and logic. The security of the cryptosystem is embedded in the integer factorization problem. The prime power moduli also undergoes similar processes of key generation, encryption and decryption as in standard RSA cryptosystem except that the decryption process is faster than standard RSA and its variants.

Cryptanalytic attack of the prime power moduli $N = p^r q^s$ has been also reported by Lim et al. (2000) where they utilized Takagi's technique to reveal prime factors (p, q) where $\gcd(r, s) = 1$. They proved that their technique performed decryption process 15-times faster than the standard RSA cryptosystem, [14]. Another partial key exposure attack on the moduli $N = p^r q^s$ where $\gcd(r, s) = 1$ was reported by Lu et al. (2015) where the authors prove 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 needed in order to factor N in polynomial time, [15].

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 a convergent of the continued fraction expansion of x.

Theorem 1.2. *(Simultaneous Diophantine Approximations) There is a polynomial time algorithm, for given rational numbers of the form $\alpha_1, ..., \alpha_n$ and $0 < \varepsilon < 1$, to compute integers $p_1, ..., p_n$ and a positive integer q such that*

$$\max_i |q\alpha_i - p_i| < \varepsilon \quad and \quad q \leq 2^{\frac{n(n-3)}{4}} [11].$$

Theorem 1.3. *Let $N = p^r q^s$ be a known integer of unknown factorization with $gcd(r,s) = 1$ and $p = N^\alpha$, $q = N^\beta$. Suppose that ξ $LSBs$ or $MSBs$ of $p^u q^v$ are known, where u, v are two selected non-negative integers satisfying $\frac{u}{r} > \frac{v}{s}$.Then one can recover the prime factors p and q in polynomial time if $\xi = \alpha\beta(su - rv)\log_2 N$ [18].*

Theorem 1.4. *Let $N = p^2 q$ be a Prime Power RSA modulus with unknown factors p, q such that $q < p < 2q$. Let a, b be suitably small integers with $gcd(a,b) = 1$ such that $|ap^2 - bq^2| < N^{\frac{1}{2}}$. Let e be a public exponent satisfying the equation $eX - NY = ap^2 + bq^2 + Z$ with $gcd(X,Y) = 1$. If $X < \frac{N}{3(ap^2+bq^2)}$ and $|Z| < \frac{|(ap^2-bq^2|}{3((ap^2+bq^2)}N^{1/3}$. Using the continued fraction algorithm he showed that every exponent e in these classes yields the factorization of N in polynomial time, and the number of such weak keys is at least $N^{\frac{1}{3}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for large N [19].*

Theorem 1.5. *Suppose that $N = p^r q$ is a prime power modulus with $q < p < 2q$, and $e < \phi(N) < N - \left(2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N^{\frac{r-1}{r+1}}\right)$ satisfying an equation*
$ed - k\phi(N) = 1$ for some unknown integers $\phi(N)$, d,k. If $\phi(N) > \frac{3}{4}N$ with $N > 8d$ and from lemma 3.2, $\left|\left(2^{\frac{2r+1}{r+1}} p^{\frac{r^2-r-1}{r+1}} q^{\frac{r}{r+1}}\right)\right| \left(p + 2^{-\frac{2r+1}{r+1}} p^{\frac{r}{r+1}} q^{-\frac{r}{r+1}}\right) < \frac{1}{8}N^\omega$ where $\omega < 1$, and $d < N^\delta$. If $\delta < \frac{1-\omega}{2}$, then

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

[13].

Theorem 1.6. *Suppose that $N_i = p_i^r q_i$, $1 \leq i \leq n$ for $n \geq 2$, be n moduli. Let $N = min\ N_i$ and e_i, $i = 1, ..., n$, be n public exponents. Define $\delta = \frac{n\kappa - \omega n + n}{(n+1)}$ where $0 < \omega \leq 1$. Let $1 < e_i < \phi(N_i) < N_i - \psi$ where $\psi = N_i - 2^{\frac{2r+1}{r+1}} N_i^{\frac{r}{r+1}} - 2^{\frac{r-1}{r+1}} N_i^{\frac{r-1}{r+1}}$. If there exist an integer $d < N^\delta$ and n integers $k_i < N^\delta$ such that*

$$e_i d - k_i \phi(N_i) = 1$$

for $i = 1, ..., n$, then one can factor the n moduli $N_1, ..., N_n$ in polynomial time [13].

Theorem 1.7. *Let $N = p^2q^2$ be a multi prime power modulus with $q^2 < p^2 < 2q^2$ and the relation $1 < e < \phi(N) < N + 2^{\frac{1}{4}}N^{\frac{1}{2}} - \left(2^{\frac{1}{2}}N^{\frac{3}{4}} + 2^{\frac{1}{4}}N^{\frac{3}{4}}\right)$ hold satisfies equation $ed - k\phi(N) = 1$ for some unknown integers $\phi(N)$, d, and k. If $d < \frac{1}{2}(N + 2^{\frac{1}{2}}N^{\frac{3}{4}} - \xi)N^{-\delta}$, then*

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

[20].

Theorem 1.8. *Let $N_i = p_i^2q_i^2$, $1 \leq i \leq n$ be n prime power moduli and $N = \min\{N_i\}$, e_i, $h_{2i} = (p_i - 1)(q_i - 1)$ be n public exponents. Define $\delta = \frac{n-\gamma n}{(n+1)}$ where $0 < \gamma \leq \frac{4}{5}$. Let $1 < e_i < \phi(N_i) < N_i - \xi$ where $\xi = 2N^{\frac{3}{4}} + N^{\frac{1}{2}}$. If there exist an integer $d < N^{\delta}$ and n integers $k_i < N^{\delta}$ such that*

$$e_id - k_i\phi(N_i) = 1$$

for $i = 1, ..., n$, then one can factor n moduli $N_1, ..., N_n$ in polynomial time [20].

2 Attack Using Continued Fraction Method to Factoring $N = p^rq^s$

In this section, we present results using continued fractions to factor multi prime power modulus $N = p^rq^s$ 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 $\phi(N) \approx \lambda^{\frac{r-s}{2r}}\left(N^{\frac{r+s}{2r}+N^{\frac{r+s-2}{2r}}}\right) - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{r-s+1}{2r}} + \lambda^{\frac{r-s-1}{2r}}\right)$ where (N, e) are public keys satisfying key equation $ex^2 - y^2\phi(N) = z$.

Lemma 2.1. *Let $N = p^rq^s$ be 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

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

Proof. Suppose $N = p^rq^s$, $q < p < \lambda q$ and $q^s < p^r < \lambda q^s$ for $2 \leq s < r$ with $\lambda > 2$, then multiplying by p^r gives $p^rq^s < p^{2r} < \lambda p^rq^s$ which implies $N < p^{2r} < \lambda N$, that is $N^{\frac{1}{2r}} < p < \lambda^{\frac{1}{2r}}N^{\frac{1}{2r}}$. Also, since $N = p^rq^s$, then $q^s = \frac{N}{p^r}$ which in turn implies $\lambda^{-\frac{1}{2s}}N^{\frac{1}{2s}} < q < N^{\frac{1}{2s}}$. 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, from the given modulus $N = p^r q^s$ the eulers totian function can be defining as $\phi(N) = p^{r-1}q^{s-1}(p-1)(q-1)$, which allawed us to compute a better approximation of $\phi(N)$ using the primes $p \approx \lambda^{\frac{1}{2r}} N^{\frac{1}{2r}}$ and $q \approx \lambda^{-\frac{1}{2r}} N^{\frac{1}{2r}}$ as follows:

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

But $p + q = \lambda^{-\frac{1}{2r}} N^{\frac{1}{2r}} + \lambda^{\frac{1}{2r}} N^{\frac{1}{2r}}$ and

$$\begin{aligned} pq &= \lambda^{\frac{1}{2r}} N^{\frac{1}{2r}} \left(\lambda^{-\frac{1}{2r}} N^{\frac{1}{2r}}\right) \\ &= \lambda^{\frac{1}{2r} - \frac{1}{2r}} N^{\frac{1}{2r} + \frac{1}{2r}} \\ &= \lambda^0 N^{\frac{2}{2r}} \\ &= N^{\frac{1}{r}} \end{aligned}$$

With

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

Therefore

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

This completes the proof. □

Theorem 2.2. *Let $N = p^r q^s$ be a multi prime power modulus with condition $q < p < \lambda q$ and $q^s < p^r < \lambda q^s$ where p and q are distinct unbalance prime numbers and $2 \leq s < r$ with $\lambda > 2$. Also, suppose that (e, N) and $(x, p, q, \phi(N))$ are public and private key tuples respectively such that $ex^2 - y^2\phi(N) = z$ where $1 < e < \phi(N) < \lambda^{\frac{r-s}{2r}} \left(N^{\frac{r+s}{2r}} + N^{\frac{r+s-2}{2r}}\right) - N^{\frac{r+s-1}{2r}} \left(\lambda^{\frac{r-s+1}{2r}} + \lambda^{\frac{r-s-1}{2r}}\right)$. Let $W = p^{r-2}q^{s-2}(p-1)(q-1)$ be known. If $p \approx \lambda^{\frac{1}{2r}} N^{\frac{1}{2r}}$ and $q \approx \lambda^{-\frac{1}{2r}} N^{\frac{1}{2r}}$ and $z < N^{\frac{1+2\alpha r}{2r}}$ then*

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

and $\left| \frac{e}{\lambda^{\frac{r-s}{2r}} \left(N^{\frac{r+s}{2r}} + N^{\frac{r+s-2}{2r}}\right) - N^{\frac{r+s-1}{2r}} \left(\lambda^{\frac{r-s+1}{2r}} + \lambda^{\frac{r-s-1}{2r}}\right)} - \frac{y^2}{x^2} \right| < \frac{1}{2(x^2)^2}$, *which leads to the factorization of N into unbalance prime factors p and q in polynomial time.*

Proof. Let $N = p^r q^s$ be the multi prime power modulus satisfying the key equation $ex^2 - y^2\phi(N) = z$ where $\phi(N) = p^{r-1}q^{s-1}(p-1)(q-1)$, and suppose that$z = N^{\frac{1+2\alpha r}{2r}}$, then we can have the following

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

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

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

Therefore, from Theorem 1.1 we can write

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

then

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

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

Algorithm 1 : An ouline on how Theorem 2.2 works

1: Initialization: The public key pair (N, e) and Z satisfying Theorem 2.2.
2: Choose r, s, to be suitable small positive integers where $2 \leq s < r$.
3: **for any** (r, s) **do**
4: The convergents $\frac{y^2}{x^2}$ of the continued fractions expansion of $\frac{\frac{e}{e}}{\left(\lambda^{\frac{r-s}{2r}}\left(N^{\frac{r+s}{2r}}+N^{\frac{r+s-2}{2r}}\right)-N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{r-s+1}{2r}}+\lambda^{\frac{r-s-1}{2r}}\right)\right)}$.
5: **end for**
6: Compute $\phi(N) := \frac{ex^2-z}{y^2}$
7: Compute $H := \gcd(\phi(N), N)$
8: Compute $p^{r-2} := \gcd(Z, H)$
9: Compute $q^s := \frac{N}{p^r}$
10: **return** prime factors p and q.

□

2.1 Attacks on Generalized System of Equations Using $\phi(N_i) < \left(\lambda^{\frac{r-s}{2r}}\left(N^{\frac{r+s}{2r}}+N^{\frac{r+s-2}{2r}}\right)-N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{r-s+1}{2r}}+\lambda^{\frac{r-s-1}{2r}}\right)\right)$ as Approximation of $\phi(N)$

In this section, we show that if $e_i < \phi(N_i) < \phi(N_i) < \left(\lambda^{\frac{r-s}{2r}}\left(N^{\frac{r+s}{2r}}+N^{\frac{r+s-2}{2r}}\right)-N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{r-s+1}{2r}}+\lambda^{\frac{r-s-1}{2r}}\right)\right)$, then $N_i = p_i^r q_i^s$, can be factored simultaneously using simultaneous Diophantine Approximation and lattice basis reduction methods for $i = 1, ..., j$ and $2 \leq s < r$.

Theorem 2.3. *Let $N_i = p_i^r q_i^s$ be the multi prime power moduli where $q < p < \lambda q$, $q^s < p^r < \lambda q^s$ $2 \leq s < r$, $\lambda > 2$ and $J_i = p_i^{r-2} q_i^{s-2}(p_i - 1)(q_i - 1)$ be known. Let (e_i, N_i) and $(x, p_i, q_i, \phi(N_i))$ be public and private key tuples satisfying the equestion of the form $e_i x^2 - y_i^2(\phi(N)) = z$ such that $1 < e_i < \phi(N_i) < \left(\lambda^{\frac{r-s}{2r}}\left(N^{\frac{r+s}{2r}}+N^{\frac{r+s-2}{2r}}\right)-N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{r-s+1}{2r}}+\lambda^{\frac{r-s-1}{2r}}\right)\right)$. Let $N = \max\{N_i\}$, define $\Lambda = \frac{r+s(\omega)-r+s(\alpha\omega)-r\xi\omega}{r+s(1+3\omega)}$ for $0 < \alpha, \xi < 1$. If there exists integers $x, y_i < N^{\Lambda}$, then one can simultaneously factor ω moduli $N_1, ..., N_\omega$ in polynomial time for $i = 1, ..., \omega,$.*

Proof. Suppose $N_i = p_i^r q_i^s$ be ω multi prime power moduli and $N = \max\{N_i\}$, let $W = \lambda_i^{\frac{r-s+1}{2r}} N_i^{\frac{r+s-1}{2r}} + \lambda_i^{\frac{r-s-1}{2r}} N_i^{\frac{r+s-1}{2r}}$ if $y_i < N^{\Lambda}$, then $e_i x^2 - y_i^2 \phi(N_i) = z$ can be rewritten as

$$\begin{aligned}
e_i x^2 - y_i^2(p_i^{r-1} q_i^{s-1}(p_i - 1)(q_i - 1)) &= z \\
e_i x^2 - y_i^2\left(\lambda_i^{\frac{r-s}{2r}}\left(N_i^{\frac{r+s}{2r}}+N_i^{\frac{r+s-2}{2r}}\right)-N_i^{\frac{r+s-1}{2r}}\left(\lambda_i^{\frac{r-s+1}{2r}}+\lambda_i^{\frac{r-s-1}{2r}}\right)\right) &= z_i \\
e_i x^2 - y_i^2\left(\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}} - \lambda_i^{\frac{r-s+1}{2r}} N_i^{\frac{r+s-1}{2r}} - \lambda_i^{\frac{r-s-1}{2r}} N_i^{\frac{r+s-1}{2r}}\right) &= z_i \\
e_i x^2 - y_i^2\left(\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + W_i - \left(\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - \phi(N_i) + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right) + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right) &= z_i
\end{aligned}$$

$$e_i x^2 - y_i^2 \left(\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}} \right) = z_i + y_i^2 \left(W_i - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \phi(N_i) - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}} \right)$$

$$\left| \frac{e_i}{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}} x^2 - y_i^2 \right| = \frac{\left| z_i + y_i^2 \left(W_i - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \phi(N_i) - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}} \right) \right|}{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}}.$$

Suppose $N = \max\{N_i\}$ and $y_i < N^{\Lambda}$, $\left| \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}} \right| > \frac{r}{r+s} N$, for $r, s > 0$ with $r > s$ and $\left| W_i - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \phi(N_i) - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}} \right| < N^{\Lambda + \frac{r}{r+s}\xi}$ for $0 < \xi, \Lambda < 1$, $z_i < N^{\frac{1}{r}+\alpha}$

$$\begin{aligned}
\left| \frac{z_i + y_i^2 \left(W_i - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \phi(N_i) - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}} \right)}{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}} \right| &\leq \left| \frac{z_i + y_i^2 \left(N^{\Lambda + \frac{r}{r+s}\xi} \right)}{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}} \right| \\
&< \frac{N^{\frac{1}{r}+\alpha} + N^{\Lambda} \left(N^{\Lambda + \frac{r}{r+s}\xi} \right)}{\frac{r}{r+s} N} \\
&< \frac{N^{\frac{1}{r}+\alpha} + N^{2\Lambda + \Lambda + \frac{r}{r+s}\xi}}{\frac{r}{r+s} N} \\
&< \frac{N^{2\Lambda + \Lambda + \frac{r}{r+s}\xi + \alpha - 1}}{\frac{r}{r+s}} \\
&< \frac{r}{r+s} N^{3\Lambda + \frac{r}{r+s}\xi + \alpha - 1}
\end{aligned}$$

This implies

$$\left| \frac{e_i}{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}} x^2 - y_i^2 \right| < \frac{r}{r+s} N^{3\Lambda + \frac{r}{r+s}\xi + \alpha - 1}.$$

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

$$N^{\Lambda} \varepsilon^{\omega} = \left(\frac{r}{r+s} \right)^{\omega} N^{3\Lambda + \frac{r}{r+s}\xi + \alpha - 1} = \left(\frac{r}{r+s} \right)^{\omega}$$

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

$$\left| \frac{e_i}{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}} x^2 - y_i^2 \right| < \varepsilon, \qquad x < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega} \cdot \varepsilon^{-\omega}.$$

Using Theorem 1.2, we can obtain the unknown parameters x and y_i. One can observe that from $e_i x^2 - y_i^2 \phi(N_i) = z_i$ we get

$$\begin{aligned} \phi(N_i) &= \frac{e_i x^2 - z}{y_i^2} \\ \gcd(\phi(N_i), N_i) &= H_i \\ p_i^{r-2} &= \gcd(J_i, H_i) \\ q_j^s &= \frac{N_i}{p_i^r}. \end{aligned}$$

Finally, the prime factors (p_i, q_i) of the prime power moduli N_i can be found simultaneously in polynomial time for N_i for $i = 1, \ldots, \omega$. □

Let

$$\Psi_1 = \frac{e_1}{\lambda_1^{\frac{r-s}{2r}} N_1^{\frac{r+s}{2r}} - W_1 + \lambda_1^{\frac{r-s}{2r}} N_1^{\frac{r+s-2}{2r}}}, \Psi_2 = \frac{e_2}{\lambda_2^{\frac{r-s}{2r}} N_2^{\frac{r+s}{2r}} - W_2 + \lambda_2^{\frac{r-s}{2r}} N_2^{\frac{r+s-2}{2r}}}$$

$$\Psi_3 = \frac{e_3}{\lambda_3^{\frac{r-s}{2r}} N_3^{\frac{r+s}{2r}} - W_3 + \lambda_3^{\frac{r-s}{2r}} N_3^{\frac{r+s-2}{2r}}}$$

Algorithm 2 : An ouline on how Theorem 2.3 works

1: Initialization: The public key pair (N_i, e_i) and J_{2i} satisfying Theorem 2.3.
2: Choose $r, s, t \geq 2$, $r > s$ and $N = \max\{N_i\}$ for $i = 1, \ldots, \omega$.
3: **for any** (N, ω, Λ) **do**
4: $\quad \varepsilon := \frac{r}{r+s} N^{3\Lambda + \frac{r}{r+s}\xi + \alpha - 1}$ where $\Lambda = \frac{r+s(\omega)-r+s(\alpha\omega)-r\xi\omega}{r+s(1+3\omega)}$
5: $\quad \mu := [3^{\omega+1} \times 2^{\frac{(\omega+1)(\omega-4)}{4}} \times \varepsilon^{-\omega-1}]$ for $\omega \geq 2$.
6: **end for**
7: Consider the lattice $\mathcal{L}$ spanned by the matrix D as stated below.
8: Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix F.
9: **for any** (D, F) **do**
10: $\quad R := D^{-1}$
11: $\quad U = RF$.
12: **end for**
13: Produce x, y_i from U
14: **for each** triplet (x, y_i, e_i) **do**
15: $\quad \phi(N_i) := \frac{e_i x^2 - z_i}{y_i^2}$
16: $\quad H_i := \gcd(\phi(N_i), N_i)$
17: $\quad p_i^{r-2} := \gcd(J_{2i}, H_i)$
18: $\quad q_i^s := \frac{N_i}{p_i^r}$
19: **end for**
20: **return** the prime factors (p_i, q_i).

Example 2.1. We consider the following three prime power moduli and their three public exponents respectively.

$N_1 = 3054746277741819273430001182901285013661605701338686593702446244570040751574316991 9$

$N_2 = 19801671372526055840282235881678051303754688669545711332940157933191562132951552050283$

$N_3 = 15494833653326715590612681690254814068206695895885269863560044699223424589474977410829$

$e_1 = 26785686609020686026410310038255985292116049663757445712183771166964838716166145133$

$e_2 = 84474875189360578071087309311248159514338498378497559362299541729222703552439572128 02$

$e_3 = 12696668631371641094184299664227725212654063183751801419808568235277615999743624692637$

Let the following integers be known

$J_{21} = 123914554205302009269457469924590555883865957732 0576$

$J_{22} = 10348234215924518081359776733894983543728614020107 4792$

$J_{23} = 11429566735770816287725577847156825089965784028542 7936$

Then $N = \min(N_1, N_2, N_3) = 19801671372526055840282235881678051303754688669545711332940157933191562 13$
$\omega = 3$ with $\Lambda = \frac{(r+s)(\omega)-(r+s)(\alpha\omega)-r\xi\omega}{(r+s)(1+3\omega)} = 0.09421400400$ and $\varepsilon := \frac{r}{r+s}N^{3\Lambda+\frac{r}{r+s}\xi+\alpha-1} =$
0.001257293434. Using Theorem 1.8, we obtain

$$\mu = [3^{\omega+1} \cdot 2^{\frac{(\omega+1)(\omega-4)}{4}} \cdot \varepsilon^{-\omega-1}] = 16207216480000$$

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

$$D = \begin{bmatrix} 1 & -[\mu\eta_1] & -[\mu\eta_2] & -[\mu\eta_3] \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{bmatrix}$$

Therefore, applying the LLL algorithm to $\mathcal{L}$, we obtain the reduced basis as indicated below

$$F = \begin{bmatrix} 5147099 & 144040944 & 96509008 & 420341551 \\ -257153302 & 16734521888 & 7395698016 & -7564654398 \\ 15083903031 & 13050364336 & -11316744048 & -2254846181 \\ [21518106489 & -12096919216 & 4561771888 & 2805288661 \end{bmatrix}$$

Next, we compute

$$U = \begin{bmatrix} 5147099 & 4513258 & 2195777 & 4217600 \\ -257153302 & -225486084 & -109702826 & -210714767 \\ 15083903031 & 13226391415 & 6434865027 & 12359946724 \\ 21518106489 & 18868253021 & 9179726932 & 17632216891 \end{bmatrix}$$

Then, from the first row of matrix U we get $x = 5147099$, $y_1 = 4513258$, $y_2 = 2195777$, $y_3 = 4217600$. Hence using x and y_i for $i = 1, 2, 3$, we compute $B_i = \frac{e_i x^2 - z_i}{y_i^2} = \phi(N_i) = p_i^{r-1}q_i^{s-1}(p_i - 1)(q_i - 1)$

$B_1 = 3054746277735590653710700349671951916798579365688296238941699685453691200262427737 6$

$B_2 = 19801671372470093366909090434439202641620354465206002672226396803270115691714512409368$

$B_3 = 15494833653230354349448718374774008965839936447037583776577973671099483600783481340256$

Applying Algorithm 2 gives $H_i = \gcd(\phi(N_i), N_i)$ and $p_i^{r-2} = \gcd(J_i, H_i)$, for $i = 1, 2, 3$

$H_1 = 123914554205554670723358526821024393894494275705196 9$

$H_2 = 10348234215953763732945171619064598435380989361226867 7$

$H_3 = 11429566735841895930222779627266046213460607052837444 9$

$p_1 = 50265440556693931519$

$p_2 = 540792488541210887563$

$p_3 = 843087436056575221669$

Finally, we compute $q_i^s := \frac{N_i}{p_i^r}$ for $i = 1, 2, 3$, that is

$$q_1 = 490437118529, q_2 = 353838388333, q_3 = 160799440409.$$

This leads to the simultaneous factorization of three moduli N_1,N_2 and N_3 in polynomial time.

Theorem 2.4. *Let $N_i = p_i^r q_i^s$ be ω multi prime power moduli $2 \leq s < r$, $q < p < \lambda q$ for $\lambda > 2$ and $J_i = p_i^{r-2} q_i^{s-2}(p_i - 1)(q_i - 1)$ be known integer where (e_i, N_i) are ω public exponents and $(x_i, p_i, q_i, \phi(N_i))$ are private keys for $e_i < \phi(N_i) < \left(\lambda^{\frac{r-s}{2r}}\left(N^{\frac{r+s}{2r}} + N^{\frac{r+s-2}{2r}}\right) - N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{r-s+1}{2r}} + \lambda^{\frac{r-s-1}{2r}}\right)\right)$, with $e = \min\{e_i\} = N^{\gamma}$ and $N = \max\{N_i\}$ satisfying $e_i x_i^2 - y^2(\phi(N_i)) = z_i$. If $x_i, y < N^{\Lambda}$ for $\Lambda = \frac{(r+s)\gamma\omega - r\omega\xi}{(r+s)(1+3\omega)}$ such that $e_i x_i^2 - y^2\phi(N_i) = z_i$ holds, then prime factors p_i and q_i of ω prime power moduli N_i can be simultaneously factored in polynomial time for $i = 1, \cdots, \omega$ and $0 < \gamma, \omega, \xi < 1$.*

Proof. Suppose $N_i = p_i^r q_i^s$ be ω multi prime power moduli and $N = \max\{N_i\}$,$e = \min\{e_i\}$, let $W = \lambda_i^{\frac{r-s+1}{2r}} N_i^{\frac{r+s-1}{2r}} + \lambda_i^{\frac{r-s-1}{2r}} N_i^{\frac{r+s-1}{2r}}$ if $y_i < N^{\Lambda}$, then $e_i x_i^2 - y^2\phi(N_i) = z_i$ can be rewritten as

$$\begin{aligned}
e_i x_i^2 - y^2(p_i^{r-1} q_i^{s-1}(p_i - 1)(q_i - 1)) &= z_i \\
e_i x_i^2 - y^2\left(\lambda_i^{\frac{r-s}{2r}}\left(N_i^{\frac{r+s}{2r}} + N_i^{\frac{r+s-2}{2r}}\right) - N_i^{\frac{r+s-1}{2r}}\left(\lambda_i^{\frac{r-s+1}{2r}} + \lambda_i^{\frac{r-s-1}{2r}}\right)\right) &= z_i \\
e_i x_i^2 - y^2\left(\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}} - \lambda_i^{\frac{r-s+1}{2r}} N_i^{\frac{r+s-1}{2r}} - \lambda_i^{\frac{r-s-1}{2r}} N_i^{\frac{r+s-1}{2r}}\right) &= z_i \\
e_i x_i^2 - y^2\left(\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + W_i - \left(\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - \phi(N_i) + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right) + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right) &= z_i
\end{aligned}$$

$$e_i x_i^2 - y^2\left(\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right) = z_i + y^2\left(W_i - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \phi(N_i) - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right)$$

$$\left|\frac{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}}{e_i} x_i^2 - y^2\right| = \frac{\left|z_i + y_i^2\left(W_i - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \phi(N_i) - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right)\right|}{e_i}.$$

Suppose $N = \max\{N_i\}$, $e = \min\{e_i\}$ and $y_i < N^{\Lambda}$, for $r, s > 0$ with $r > s$ and $\left|W_i - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \phi(N_i) - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right| < N^{\Lambda+\frac{r}{r+s}\xi}$ for $0 < \xi, \Lambda < 1$, $z_i < N^{\frac{1}{r}+\alpha}$

$$\left|\frac{z_i + y_i^2\left(W_i - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} + \phi(N_i) - \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}\right)}{e_i}\right| \leq \left|\frac{z_i + y_i^2\left(N^{\Lambda+\frac{r}{r+s}\xi}\right)}{e_i}\right|$$

$$< \frac{N^{\frac{1}{r}+\alpha} + N^{2\Lambda}\left(N^{\Lambda+\frac{r}{r+s}\xi}\right)}{N^{\gamma}}$$

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

$$< \frac{1}{r+\alpha} N^{3\Lambda+\frac{r}{r+s}\xi-\gamma}$$

This implies

$$\left|\frac{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}}{e_i} x_i^2 - y^2\right| < \frac{1}{r+\alpha} N^{3\Lambda+\frac{r}{r+s}\xi-\gamma}.$$

For the unknown integer positive integer x, we assume that $\varepsilon = \frac{1}{r+\alpha} N^{3\Lambda+\frac{r}{r+s}\xi-\gamma}$, with $\Lambda = \Lambda = \frac{(r+s)\gamma\omega - r\omega\xi}{(r+s)(1+3\omega)}$, then

$$N^{\Lambda}\varepsilon^{\omega} = \left(\frac{1}{r+\alpha}\right)^{\omega} N^{3\Lambda+\frac{r}{r+s}\xi-\gamma} = \left(\frac{1}{r+\alpha}\right)^{\omega}$$

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

$$\left|\frac{\lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s}{2r}} - W_i + \lambda_i^{\frac{r-s}{2r}} N_i^{\frac{r+s-2}{2r}}}{e_i} x_i^2 - y^2\right| < \varepsilon, \qquad y < 2^{\frac{\omega(\omega-3)}{4}} \cdot 3^{\omega} \cdot \varepsilon^{-\omega}.$$

Using Theorem 1.2, we can obtain the unknown parameters x and y_i. One can observe that from $e_i x_i^2 - y^2\phi(N_i) = z_i$ we get

$$\begin{aligned} \phi(N_i) &= \frac{e_i x_i^2 - z_i}{y^2} \\ \gcd(\phi(N_i), N_i) &= H_i \\ p_i^{r-2} &= \gcd(J_i, H_i) \\ q_j^s &= \frac{N_i}{p_i^r}. \end{aligned}$$

Finally, the prime factors (p_i, q_i) of the prime power moduli N_i can be found simultaneously in polynomial time for N_i for $i = 1, \ldots, \omega$. □

Let

$$\Psi_1 = \frac{\lambda_1^{\frac{r-s}{2r}} N_1^{\frac{r+s}{2r}} - W_1 + \lambda_1^{\frac{r-s}{2r}} N_1^{\frac{r+s-2}{2r}}}{e_1}, \; \Psi_2 = \frac{\lambda_2^{\frac{r-s}{2r}} N_2^{\frac{r+s}{2r}} - W_2 + \lambda_2^{\frac{r-s}{2r}} N_2^{\frac{r+s-2}{2r}}}{e_2}$$

$$\Psi_3 = \frac{\lambda_3^{\frac{r-s}{2r}} N_3^{\frac{r+s}{2r}} - W_3 + \lambda_3^{\frac{r-s}{2r}} N_3^{\frac{r+s-2}{2r}}}{e_3}$$

Algorithm 3 Theorem 2.4

Initialization: The public key tuple (N_i, e_i) and J_i satisfying Theorem 2.4.
Choose $r, s, t \geq 2$, $r > s$ and $N = \max\{N_i\}$ for $i = 1, \ldots, \omega$.
for any (N, ω, Λ) **do**
    $\varepsilon = \frac{1}{r+\alpha} N^{3\Lambda + \frac{r}{r+s}\xi - \gamma}$, where $\Lambda = \frac{(r+s)\gamma\omega - r\omega\xi}{(r+s)(1+3\omega)}$
    $X := \left[3^{\omega+1} \times 2^{\frac{(\omega+1)(\omega-4)}{4}} \times \varepsilon^{-\omega-1}\right]$ for $\omega \geq 2$.
end for
Consider the lattice $\mathcal{L}$ spanned by the matrix B as stated below.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix M.
for any (B, M) **do**
    $Q := B^{-1}$
    $L = QM$.
end for
Produce x_i, y from L
for each triplet (x_i, y, e_i) **do**
    $\phi(N_i) := \frac{e_i x_i^2 - 1}{y^2}$
    $W_i := \gcd(\phi(N_i), N_i)$
    $p_i^{r-2} := \gcd(J_i, W_i)$
    $q_i^s := \frac{N_i}{p_i^r}$
end for
return the prime factors (p_i, q_i).

Example 2.2. We consider the following three prime power and their three public exponents respectively

$N_1 = 6340703248489573146699776783402864616649014709302387076202125207107831797108419065960218888999$
$N_2 = 8613125030789749885050157105802987377506575237381307855535286678523990996611644304378762771941$
$N_3 = 6911898390048320288274078246448280119428089063507367851555965739128550126712830482606449728841$
$e_1 = 1209441121498138606109493796382897582902062246080629267148794006761920299660944790137354646101$
$e_2 = 1752247180714006304638128779583803860657567689329592158067606156757245684091682862025285289526$
$e_3 = 4577767466445609178512799328767544047498148753594636404744630773302103694230401193171160112229$

Also, let

$J_{21} = 158439274620165701437002989633864726277162784938667584257 76$
$J_{22} = 2860459384868415345704059415996315918352432994696771716762 84$
$J_{23} = 2240208915302044252640554708745932589171566857956509656421 92$

Then, one can observe that

$N = \min\{N_1, N_2, N_3\} = 6340703248489573146699776783402864616649014709302387076202125207107831797108$

and $\min\{e_1, e_2, e_3\} = N^\gamma$ with $\gamma = 0.32$ and $\omega = 3$ we get $\varepsilon = \frac{1}{r+\alpha} N^{3\Lambda + \frac{r}{r+s}\xi - \gamma} = 0.06438580265$ and $\Lambda = \frac{(r+s)\gamma\omega - r\omega\xi}{(r+s)(1+3\omega)} = -0.7989842078$. Using Algorithm 3, we compute

$$X = [3^{\omega+1} \cdot 2^{\frac{(\omega+1)(\omega-4)}{4}} \cdot \varepsilon^{-\omega-1}] = 124190.$$

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

$$B = \begin{bmatrix} 1 & -[X\Psi_1] & -[X\Psi_2] & -[X\Psi_3] \\ 0 & X & 0 & 0 \\ 0 & 0 & X & 0 \\ 0 & 0 & 0 & X \end{bmatrix}$$

Therefore, applying the LLL algorithm to $\mathcal{L}$, we obtain reduced basis as follows

$$M = \begin{bmatrix} 1467 & -806 & -461 & -721 \\ -3585 & -570 & -2175 & -6365 \\ 1669 & -3372 & 8703 & -397 \\ -3597 & -11484 & -3949 & 8371 \end{bmatrix}$$

Next, we compute

$$L = \begin{bmatrix} 1467 & 7691 & 7211 & 2215 \\ -3585 & -18795 & -17622 & -5413 \\ 1669 & 8750 & 8204 & 2520 \\ -3597 & -18858 & -17681 & -5431 \end{bmatrix}$$

From the first row of matrix L we obtain $y = 1467$, $x_1 = 7691$, $x_2 = 7211$, $x_3 = 2215$. Hence using x_i, y and Algorithm 3, we compute $A_i = \frac{e_i x_i^2 - z_i}{y} = \phi(N_i) = p_i^{r-1} q_i^{s-1}(p_i - 1)(q_i - 1)$, $W_i = \gcd(\phi(N_i), N_i)$ and $p_i^{r-2} = \gcd(J_i, W_i)$, for $i = 1, 2, 3$.

$A_1 = 6340703248426846639119370680286888418609243854537232283376787362003606166955189997157694465$

$A_2 = 8613125030762576320889943169447041335515828635143618985566126786896045417849437708226973219375$

$A_3 = 6911898390032054758286196668861697385963462501167089050108627922879454453115431931058375807697$

$W_1 = 158439274621733089464973169427275779371129055153295515001 29$

$W_2 = 28604593848774398143312756782601204124575949162022238816 1947$

$W_3 = 22402089153073160583348505236856334892489379083230449377 9847$

$p_1 = 39590251678535457318 8459$

$p_2 = 94997203259955243617 5627$

$p_3 = 72607201394164267557 7849$

Finally, we compute $q_i^s := \frac{N_i}{p_i^r}$ for $i = 1, 2, 3$ which gives

$$q_1 = 101084908009, q_2 = 316967070643, q_3 = 424941480247.$$

This leads to the simultaneous factorization of three moduli N_1,N_2 and N_3 in polynomial time.

2.2 Conclusion

In this research we proposed two polynomial attack for breaking the modulus of the form $N = p^r q^s$ where p and q are unbalance prime numbers for $2 \leq s < r$ with $q < p < \lambda q$ and $q^s < p^r < \lambda q^s$, First approach applied the method of continued fractions expansion to prove that $\frac{y^2}{x^2}$ can be recovered among the convergents of the continued fraction expansion of $\frac{e}{\left(\lambda^{\frac{r-s}{2r}}\left(N^{\frac{r+s}{2r}}+N^{\frac{r+s-2}{2r}}\right)-N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{r-s+1}{2r}}+\lambda^{\frac{r-s-1}{2r}}\right)\right)}$ which allows us to factor the prime power modulus $N = p^2q^2$ in polynomial time. The second approaches used j public keys (N_i, e_i, J_{2i}) where $J_{2i} = p^{r-2}q^{s-2}(p_i - 1)(q_i - 1)$ when there exist j relations of the form $e_i x^2 - y_i^2 \phi(N_i) = z_i$ and $e_i x_i^2 - y^2 \phi(N_i) = z_i$ such that the unknown parameters x, x_i, y, y_i can be recovered simultaneously using LLL algorithm which enable us to factor j prime power moduli N_i for $i = 1, 2, 3$ in polynomial time.

References

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

[2] Nitaj, Abderrahmane, *The Mathematical Cryptography of the RSA Cryptosystem*, 2012.

[3] M. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Transactions on Information Theory*, **36**, (1990) 553–558.

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

[5] B. de Weger B, Cryptanalysis of RSA with Small Prime Difference, *Applicable Algebra in Engineering Communication and Computing* **13(1)**, (2002).

[6] S. Maitra, and S. Sarkar, Revisiting Wieners attack new weak keys in RSA, *in International Conference on Information Security*, (2008).

[7] A. May, *New RSA Vulnerabilities Using Lattice Reduction Methods*, PhD. thesis, University of Paderborn (2003).

[8] Nitaj, Abderrahmane, Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem, *Artificial Intelligence, Evolutionary Computing and Metaheuristics*, (2013) 139-168.

[9] T. Takagi, Fast RSA-type cryptosystem modulo $p^k q$, *Advances in Cryptology-CRYPTO 1998*, Springer Berlin Heidelberg, (1998), 318–326.

[10] S. Sarkar, Small Secret Exponent Attack on RSA Variant with Modulus $N = p^2 q$, *in Proc. Int. Workshop on Coding and Cryptography -WCC*, (2013), pp. 215–222.

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

[12] Sarkar, S, Revisiting Prime Power RSA, *Discrete Applied Mathematics*, **203** (2016) 127–133.

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

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

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

[16] J. S. Coron, J. C. Faug'ere, G. Renault and R. Zeitoun, Factoring $N = p^r q^s$ for large r and s, *Cryptographers' Track at the RSA Conference*, Springer, Cham, **9610** ,(2016) 448–464.

[17] J. S. Coron and R. Zeitoun, Improved factorization of $N = p^r q^s$, *Cryptographers' Track at the RSA Conference*, Springer, Cham, (2018) 65–79.

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

[19] Asbullah, M. A., and M. R. K. Ariffin, *New Attacks on RSA with Modulus $N = p^2 q$ Using Continued Fractions*, Journal of Physics, Conference Series, Vol. 622. No. 1. IOP Publishing, (2015).

[20] Shehu, Sadiq, Saidu Isah Abubakar, and Zaid Ibrahim. *Polynomial Time Attacks for Modulus $N = p^2 q^2$*. Journal of Applied Mathematics and Computation, 2020, 4(4), 230-240

[21] Lenstra, A.K. , Lenstra, H.W., L. Lovasz, L., *Factoring polynomials with rational coefficients*, Mathematische Annalen, Vol. 261, 513-534, (1982).