Journal of Advances in Mathematics and Computer Science

Volume 38, Issue 8, Page 33-46, 2023; Article no.JAMCS.86625

ISSN: 2456-9968

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

Breaking Modulus of the form $N = p^r q^s$ with Improved Polynomial Attacks

Sadiq Shehu [a*], Hamza Abdullahi [b], Aminu A. Ibrahim [b] and Rufai Ahmad [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/v38i81788

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/86625

Original Research Article

Received: 25/02/2022

Accepted: 29/04/2022

Published: 17/06/2023

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

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

,

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

which leads to the factorization of the moduli $N = p^r q^s$ in polynomial time. The second assaults on s multi prime power moduli are described $N_i = p_i^r q_i^s$ for $i = 1, 2, \ldots, \omega$. We use lattice basis reduction techniques to obtain the parameters (x, y_i) or (y, x_i) after transforming the system of equations into a simultaneous Diophantine approximation problem, and it resulted in simultaneous factorization of s moduli N_i in polynomial time.

Keywords: Unbalance prime numbers; factorization; LLL algorithm; diophantine approximations; continued fraction.

1 Introduction

The public key notion arose from an attempt to overcome two issues: key distribution and the development of digital signatures. Whitfield Diffie and Martin Hellman developed the conceptual framework in 1976, and it was a huge success. The same key is used for both encryption and decryption in traditional encryption [1], [2], [3]. This is an optional requirement. Instead, a cryptographic system might be created that uses one key for encryption and another key for decryption. In addition, these algorithms have the following significant feature: Knowing simply the algorithm and the encryption key makes determining the decryption key computationally impossible. Furthermore, some algorithms, such as RSA, have the following properties: For encryption, one of the two associated keys can be utilized, while the other can be used for decryption.

Illustrates the Public key process. The steps are:

1. A pair of keys is generated by each system.
2. Each system makes its encryption key (public key) public while preserving its private key.
3. If A intends to transmit a message to B, the message is encrypted using B's public key.
4. When B receives the message, it uses its private key to decrypt it. Because only B has access to the message's private key, no one else can decrypt it.

Public key cryptography is regarded as one of the most significant breakthroughs in the world of information security. Electronic data transmission is occasionally vulnerable to eavesdroppers; this can be mitigated by implementing robust encryption techniques [4], [5]. RSA cryptosystem, created by Rivest, Shamir, and Adleman, is recognized as a fast-growing, dependable, and usable cryptosystem due to its efficiency in ensuring secrecy, integrity, and verification of the entities participating in communication through insecure communication channels [6].

According to Takagi, one of the most important RSA variants in the cryptanalytic attack is multi prime power modulus $N = p^r q$ for $r \geq 2$. (1998). Based on his findings, the system decrypted data faster than the usual RSA modulus $N = pq$ [7]. Several cryptanalytic assaults 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 since then, utilizing various approaches detailed in [8], [9], [10], [11], [12] and [13].

The prime power moduli $N = p^r q^s$ are among the RSA cryptosystem variants that have been observed to be more efficient in both encryption and decryption than the normal RSA modulus $N = pq$, according to [14]. Using complicated mathematics and logic, the cryptosystem achieves all cryptographic goals such as privacy and authenticity in digital communication channels. The integer factorization problem is integrated in the cryptosystem's security [15], [16], [17],[18], [19]. The prime power moduli go through the same key generation, encryption, and decryption operations as regular RSA and its variants, with the exception that the decryption phase is faster.

Lim et al. presented a cryptoanalytic attack on the prime power moduli $N = p^r q^s$, where they used 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 [14]. Lu et al. (2015) reported another partial key exposure attack on the moduli $N = p^r q^s$ where $gcd(r, s) = 1$, and 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 required 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 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*

$$\max_i |q\alpha_i - p_i| < \varepsilon \quad and \quad q \leq 2^{\frac{n(n-3)}{4}} [12].$$

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 $\xi = \alpha\beta(su - rv)\log_2 N$ [21].*

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 [9].*

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

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

[10].

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 [10].

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*

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

[8].

Theorem 1.8. *Let $N_i = p_i^2q_i^2$, $1 \le i \le n$ 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 $0 < \gamma \le \frac{4}{5}$. 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 [8].

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 $2 \le s < r$ 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 $ex^2 - y^2\phi(N) = z$. Let $N = p^rq^s$ be prime power moduli where p and q are unbalance prime numbers for $2 \le s < r$. 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 $2 \le s < r$ 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 $N = p^rq^s$ 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

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

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 2.1. *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

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

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 2.1 works

1: Initialization: The public key pair (N, e) and Z satisfying Theorem 2.1.
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 App-roximation 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 2.2. *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 2.2 works

1: Initialization: The public key pair (N_i, e_i) and J_{2i} satisfying Theorem 2.2.
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 2.3. *We consider the following three prime power moduli and their three public exponents respectively.*

$N_1 = 3054746277741819273430001182901285013661605701338686593702446244570040751574316991 9$
$N_2 = 1980167137252605584028223588167805130375468866954571133294015793319156213295155205028 3$
$N_3 = 1549483365332671559061268169025481406820669589588526986356004469922342458947497741082 9$
$e_1 = 2678568660902068602641031003825598529211604966375744571218377116696483871616614513 3$
$e_2 = 8447487518936057807108730931124815951433849837849755936229954172922270355243957212802$
$e_3 = 1269666863137164109418429966422772521265406318375180141980856823527761599974362469263 7$

Let the following integers be known

$$J_{21} = 123914554205302009269457469924590555883865957732057 6$$
$$J_{22} = 103482342159245180813597767338949835437286140201074792$$
$$J_{23} = 114295667357708162877255778471568250899657840285427936$$

Then $N = \min(N_1, N_2, N_3) = 1980167137252605584028223588167805130375468866954571 1$
$3329401579331915621329515520502 83$, $\omega = 3$ *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* $B_i = \frac{e_i x^2 - z_i}{y_i^2} = \phi(N_i) = p_i^{r-1}q_i^{s-1}(p_i - 1)(q_i - 1)$

$B_1 = 3054746277735590653710700349671951916798579365688296238941699685453691200262427737 6$
$B_2 = 1980167137247009336690909043443920264162035446520600267222639680327011569171451240936 8$
$B_3 = 1549483365323035434944871837477400896583993644703758377657797367109948360078348134025 6$

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

$$H_1 = 123914554205554670723358526821024393894494275705196 9$$
$$H_2 = 1034823421595376373294517161906459843538098936122686 77$$
$$H_3 = 1142956673584189593022277962726604621346060705283744 49$$
$$p_1 = 50265440556693931519$$
$$p_2 = 540792488541210887563$$
$$p_3 = 843087436056575221669$$

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 $0 < \xi, \Lambda < 1$, $z_i < N^{\frac{1}{r}+\alpha}$

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

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

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

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

Example 2.5. *We consider the following three prime power and their three public exponents respectively*

$N_1 = 6340703248489573146699776783402864616649014709302387076202125207107831797108419065960218888 99$
$N_2 = 8613125030789749885050157105802987377506575237381307855535286678523990996611644304378762771 9467$
$N_3 = 6911898390048320288274078246448280119428089063507367851555965739128550126712830482606449728 8441$
$e_1 = 1209441121498138606109493796382897582902062246080629267148794006761920299660944790137354646 10$
$e_2 = 1752247180714006304638128779583803860657567689329592158067606156757245684091682862025285289 5269$
$e_3 = 4577767466445609178512799328767544047498148753594636404744630773302103694230401193171160112 2295$

Also, let

$$J_{21} = 158439274620165701437002989633864726277162784938667584257 76$$
$$J_{22} = 286045938486841534570405941599631591835243299469677171676284$$
$$J_{23} = 224020891530204425264055470874593258917156685795650965642192$$

Then, one can observe that

$$N = \min\{N_1, N_2, N_3\} = 6340703248489573146699776783402864616649014709302387076202125207$$

$$107831797108419065960218888 99$$

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*

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

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 $\Lambda = \frac{(r+s)\gamma\omega - r\omega\xi}{(r+s)(1+3\omega)}$
    $X := [3^{\omega+1} \times 2^{\frac{(\omega+1)(\omega-4)}{4}} \times \varepsilon^{-\omega-1}]$ 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).

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* $i = 1, 2, 3$.

$A_1 = 6340703248426846639119370680286888418609243854537232238337678736200360616695518999715769446 56$
$A_2 = 8613125030762576320889943169447041335515828635143618985566126786896045417849437708226973219372 4$
$A_3 = 6911898390032054758286196668861697385963462501167089050108627922879454453115431931058375807697 6$
$W_1 = 1584392746217330894649731694272757793711290551532955150012 9$
$W_2 = 2860459384877439814331275678260120412457594916202223881619 47$
$W_3 = 2240208915307316058334850523685633489248937908323044937798 47$
$p_1 = 39590251678535457318845 9$
$p_2 = 94997203259955243617562 7$
$p_3 = 72607201394164267557784 9$

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.*

3 Conclusion

For $2 \leq s < r$ with $q < p < \lambda q$ and $q^s < p^r < \lambda q^s$, we suggested two polynomial attacks for cracking the modulus of the form $N = p^r q^s$, where p and q are unbalance prime numbers.

The first method used the method of continued fractions expansion to show that $\frac{y^2}{x^2}$ can be recovered among the convergents of the continued fraction expansion $\frac{e}{\left(\lambda^{\frac{r-s}{2r}}\left(N^{\frac{r+s}{2r}}+N^{\frac{r+s-2}{2r}}\right)-N^{\frac{r+s-1}{2r}}\left(\lambda^{\frac{r-s+1}{2r}}+\lambda^{\frac{r-s-1}{2r}}\right)\right)}$, allowing us to factor in polynomial time the prime power modulus $N = p^r q^s$. The second method made use of 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 j relations of the form $e_i x^2 - y_i^2 \phi(N_i) = z_i$ and $e_i x_i^2 - y^2 \phi(N_i) = z_i$ exist, and the unknown parameters x, x_i, y, y_i can be recovered concurrently using the LLL algorithm, which allows us to factor j prime power moduli In polynomial time, N_i for $i = 1, 2, 3$.

Competing Interests

Authors have declared that no competing interests exist.

References

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

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

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

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

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

[6] 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.

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

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

[9] Asbullah MA, Ariffin MRK. New Attacks on RSA with Modulus $N = p^2q$ Using Continued Fractions. Journal of Physics, Conference Series. 2015;622. No. 1. IOP Publishing.

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

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

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

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

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

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

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

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

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

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

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

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

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)
https://www.sdiarticle5.com/review-history/86625