Strategic Way of Factoring Modulus $N = p^r q$

Sadiq Shehu$^{1}$, Abdullahi Hussaini$^{1}$ and Zahriya Lawal$^{2}$

$^{1}$Department of Mathematics, Faculty of Science, Sokoto State University, Sokoto, Nigeria.
$^{2}$Department of Computer Science, Faculty of Science, Sokoto State University, Sokoto, Nigeria.

Authors’ contributions

This work was carried out in collaboration among all authors. SS proposed the research idea and drafted the manuscript. AH participated in all the algebra of this research while ZL used maple software to generate all the examples in this research. All authors read and approved the final manuscript.

Abstract

Cryptography is fundamental to the provision of a wider notion of information security. Electronic information can easily be transmitted and stored in relatively insecure environments. This research was present to factor the prime power modulus $N = p^r q$ for $r \geq 2$ using the RSA key equation, if $\frac{e}{N}$ is a convergents of the continued fractions expansions of $N$ and $\frac{e}{N}$. We furthered our analysis on $n$ prime power moduli $N_i = p_i^r q_i$ by transforming the generalized key equations into Simultaneous Diophantine approximations and using the LLL algorithm on $n$ prime power public keys $(N_i, e_i)$ we were able to factorize the $n$ prime power moduli $N_i = p_i^r q_i$, for $i = 1, ..., n$ simultaneously in polynomial time.

Keywords: Prime power, Factorization, LLL algorithm, simultaneous diophantine approximations, continued fraction.
1 Introduction

The most popular public key crytosystem in use today is the RSA cryptosystem, introduced by Rivest, Shamir, and Adleman [1]. Its security is based on the intractability of the integer factorization problem. The cryptosystem is most commonly used for providing privacy and ensuring authenticity of digital data. These days RSA is deployed in many commercial systems. It is used by web servers and browsers to secure web traffic, it is used to ensure privacy and authenticity of Email, it is used to secure remote login sessions, and it is at the heart of electronic credit-card payment systems. In short, RSA is frequently used in applications where security of digital data is a concern.

In 1990, Wiener described a well known attack on RSA using continued fractions with short secret exponent \( x < \frac{1}{4}N^\frac{1}{2} \). Using the fact that \( N \) is approximate to \( \phi(N) \). Wiener proved that \( \left| \frac{N}{N^\frac{1}{2}} \right| < \frac{1}{4}N^\frac{1}{2} \) and \( \frac{N}{N^\frac{1}{2}} \) is among the convergent of the continued fraction expansion of \( \frac{N}{N^\frac{1}{2}} \). Which showed that given the public key \((N,e)\) satisfying the key equation \( cx - y\phi(N) = 1 \), then one can efficiently recover the private exponent \( x \). This leads to the following result [2].

In order to ensure computational efficiency while maintaining the acceptable level of security several variants has been proposed one of such important variant is the prime power modulus. In the prime power the modulus is in the form \( N = p^r q \) for \( r \geq 2 \). As in the standard RSA cryptosystem, the security of prime power modulus depend on the difficulty of factoring integers of the form \( N = p^r q \) \( r \geq 2 \).

Let \( N = p^r q \), be a prime power modulus for \( r \geq 2 \) where \( p \) and \( q \) are two large prime integers such that \( q < p < 2q \). If \( r \approx \sqrt{\log p} \), then \( N \) can be factored in polynomial time. Let \( N = pq \) be an RSA modulus with \( q < p < 2q \). \( N > 8x \) and \( |p - q| < N^\frac{1}{2} \). Let \( e < \phi(N) \), \( \phi(N) > \frac{1}{2}N \) and \( x < N^\frac{1}{2} \)
be a public and private exponent, respectively. If \( \delta < \frac{2}{4} - \beta \), then \( \left| \frac{N}{N^\frac{1}{2}} - \frac{N}{N^\frac{1}{2}} \right| < \frac{1}{4}N^\frac{1}{2} \) and \( \frac{N}{N^\frac{1}{2}} \) is among the convergent of the continued fractions expansion of \( \frac{N}{N^\frac{1}{2}} \) [3].

An efficient algorithm for factoring \( N = p^r q \) when \( r \) is large \( (r \approx \sqrt{\log p}) \) is known, it is expected that the factoring of \( N \) will be intractable when \( r \) is small. Variant designs of the RSA utilizing \( N = p^r q \) for \( r \geq 2 \) exist because of various reasons. For example the HIME(R) design became a standard in Japan because it was able to "carry" more data securely than the existing RSA. [4].

(1998) Takagi showed that the decryption process is about three times faster than RSA cryptosystem using CRT if they choose the 768-bit modulus \( p^r q \) for 256-bit primes \( p \) and \( q \) [5].

AA3 Cryptosystem overcome Rabin’s cryptosystem decryption failure which was due to a 4-to-1 mapping by incorporating the hardness of factoring integer \( N = p^r q \) for \( r = 2 \) coupled with the square root problem as its cryptographic primitive. The design for encryption does not involve "expensive" mathematical operation.

**Our contribution.** Our research show that for a given bound \( r \geq 2 \), the modulus \( N = p^r q \) can be factor in polynomial time which counters the statement "When \( r \) is small in general \( p^r q \) is intractable (see [4])." This paper, present two new attacks on the prime power modulus \( N = p^r q \). For the first attack, we consider the prime power modulus \( N = p^r q \) and public of exponent \( e \) satisfying the equation \( cx - y\phi(N) = 1 \) for some unknown integers \( \phi(N), x,y \) to show that \( \frac{N}{N^\frac{1}{2}} \) is a convergents of the continued fractions expansions of \( \frac{\left( \frac{\left( \frac{N}{N^\frac{1}{2}} \right)}{N^\frac{1}{2}} \right) - \frac{N}{N^\frac{1}{2}}}{N^\frac{1}{2}} \) which yield the factorization of \( N = p^r q \) in polynomial time.

For second attack we transform the generalized key equations into a simultaneous diophantine problem and apply lattice basis reduction techniques to find the parameters \((x,y_i)\) or \((y,x_i)\) which leads to factorization of \( \omega \) moduli \( N_i \) in polynomial time.
The rest of the paper is structured as follows. In section 2, we give review of continued fraction, lattice basis reduction and simultaneous diophantine approximations with some useful results needed for the attack. In section 3, 4 we report our finding for the first and second attacks. We conclude this paper in section 5.

2 Preliminaries

We state the definition and important results concerning the continued fraction, lattice basis reduction techniques and simultaneous diophantine equations as will as some useful lemmas needed for the attacks.

Definition 2.1(Continued Fraction). A continued fraction is an expression of the form

\[ a_0 + \frac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_n + \ddots} }} = [a_0, a_1, \ldots, a_n, \ldots] \]

which, for simplicity, can be rewritten as

\[ x = [a_0, a_1, \ldots, a_n, \ldots] \].

If \( x \) is a rational number, then the process of calculating the continued fraction expansion will finish in some finite index \( n \) and

\[ x = [a_0, a_1, \ldots, a_n] \].

The convergents \( \frac{p_n}{q_n} \) of \( x \) are the fractions denoted by \( \frac{p_i}{q_i} = [a_0, a_1, \ldots, a_i] \) for \( i \geq 0 \).

Theorem 2.2 (Legendre). Let \( x = [a_0, a_1, a_2, \ldots] \) be a continued fraction expansion of \( x \). If \( X \) and \( Y \) are coprime integers such that

\[ x - \frac{Y}{X} < \frac{1}{2X^2} \]

Then \( Y = p_n \) and \( X = q_n \) for some convergent \( \frac{p_n}{q_n} \) of \( x \) with \( n \geq 0 \).

Lattice 2.3 Let \( u_1, \ldots, u_d \) be \( d \) linearly independent vectors of \( \mathbb{R}^n \) with \( d \leq n \). The set of all integer linear combinations of the vectors \( u_1, \ldots, u_d \) is called a lattice and is in the form

\[ \mathcal{L} = \left\{ \sum_{i=1}^{d} x_i u_i \mid x_i \in \mathbb{Z} \right\} \]

The set \((u_1, \ldots, u_d)\) is called a basis of \( \mathcal{L} \) and \( d \) is its dimension. The determinant of \( \mathcal{L} \) is defined as

\[ \det(\mathcal{L}) = \sqrt{\det(U^T U)} \]

where \( U \) is the matrix of the \( u_i \)'s in the canonical basis of \( \mathbb{R}^n \).

Define \( \|v\| \) to be the Euclidean norm of a vector \( v \in \mathcal{L} \). A central problem in lattice reduction is to find a short non-zero vector in \( \mathcal{L} \).

The LLL algorithm produces a reduced basis and the following result fixes the sizes of the reduced basis vector (see [6]).

Theorem 2.4 Let \( L \) be a lattice of dimension \( \tau \) with a basis \( \{w_1, \ldots, w_\tau\} \). The LLL algorithm produces a reduced basis \( \{b_1, \ldots, b_\tau\} \) satisfying

\[ \|b_1\| \leq \|b_2\| \leq \ldots \leq \|b_\tau\| \leq 2^{\frac{\tau(\tau-1)}{4n}} \det(L)^{\frac{1}{\tau+1}} \]

for all \( 1 \leq i \leq \tau \).
Theorem 2.5 (Simultaneous Diophantine Approximations). There is a polynomial time algorithm, for given rational numbers $\alpha_1, \ldots, \alpha_n$ and $0 < \varepsilon < 1$, to compute integers $p_1, \ldots, p_n$ and a positive integer $q$ such that

$$\max_i |q\alpha_i - p_i| < \varepsilon \quad \text{and} \quad q \leq 2^{\frac{p(n-1)}{1}}$$

Proof. See [7] Appendix A.

3 First Attack on RSA Modulus $N = p^r q$

Let $(N, e)$ be a public key satisfying an equation satisfying an equation $ex - y\phi(N) = 1$ for some unknown integers $\phi(N), x, y$. In this section, we present a result based on continued fractions and show how to factor the prime power modulus $N = p^r q$

Lemma 3.1 Let $N = p^r q$ be a prime power modulus with $q < p < 2q$. Then

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

Proof. Let $N = p^r q$ and suppose $q < p < 2q$. Then multiplying by $p^r$ we get $p^r q < p^r p < 2p^r q$ which implies $N < p^{r+1} < 2N$, that is $N^{\frac{1}{r+1}} < p < 2N^{\frac{1}{r+1}}$. Also since $N = p^r q$, then $q = \frac{N}{p^r}$ which in turn implies $2^{-r} N^{\frac{1}{r}} < q < N^{\frac{1}{r}}$. Hence

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

Let $N = p^r q$ therefore using $\phi(N) = p^{r-1}(p - 1)(q - 1)$ we compute the approximation of $\phi(N)$ that is

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

The following result gives an interval for $N - \phi(N) = p^r + p^{r-1}q - p^{r-1}$ in terms of $N$. It shows that if $p \approx 2^\frac{1}{r+1} N^{\frac{1}{r}} \approx q$ then

Which is a good approximation to $\phi(N)$. Also if $p \approx 2q$ then

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

Which is also a good approximation to $\phi(N)$. 

Lemma 3.2 Suppose that $N = p^r q$ is a prime power modulus for $q < p < 2q$ and $\phi(N) = N - (p^r + p^{r-1}q - p^{r-1})$ then we shows that $|N - (2^\frac{1}{r+1} N^{\frac{1}{r+1}} - 2^\frac{1}{r+1} N^{\frac{1}{r+1}}) - \phi(N)| < 2^\frac{1}{r+1} p^{\frac{1}{r+1} + \frac{1}{r+1}} q^{\frac{1}{r+1}}$$

\[ p - 2^\frac{\varepsilon}{\varepsilon+1} p^\frac{\varepsilon+1}{\varepsilon+1} q^{\frac{1}{\varepsilon+1}} \]
Proof. Let \( N = p^r q \) be a prime power modulus and suppose that
\[ \phi(N) = p^{r-1}(p - 1)(q - 1) = p^r q - p^r - p^{r-1}q + p^{r-1} = N - (p^r + p^{r-1}q - p^{r-1}) \]

Then
\[
\begin{align*}
N & - \left[ \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 3 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right] - \phi(N) \\
& = N - \phi(N) - \left[ \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 3 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right] \\
& = p^r + p^{r-1}q - p^{r-1} - \left[ \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 3 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right] \\
& = p^r + p^{r-1}q - p^{r-1} - \left[ \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 3 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} + p^r - p^{r-1} \right] \\
& = \left[ \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - p^{r-1}q - 2 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right] \\
& = \left[ \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 2 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right] \\
& < \left[ \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 2 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right]
\end{align*}
\]

Which terminate the proof.

\[ \blacksquare \]

Theorem 3.3. Suppose that \( N = p^r q \) is a prime power modulus with \( q < p < 2q \), and \( e < \phi(N) < N - \left( \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 2 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right) \) satisfying an equation
\[ ex - y\phi(N) = 1 \]
for some unknown integers \( \phi(N), x, y \). If \( \phi(N) > \frac{3}{4}N \) with \( N > 8x \) and from lemma 3.2. \( \left( \frac{2x^{r-1} + 1}{2x^{r-1} + 1} p^{x^{r-1} q^{r-1}} \right) \left( p + 2^{x^{r-1} q^{r-1}} p^{x^{r-1} q^{r-1}} \right) < \frac{1}{2}N^\omega \) where \( \omega < 1 \), and \( x < N^\delta \). If \( \delta < \frac{1-\omega}{2} \), then
\[
\left| \frac{e}{N - \left( \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 2 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right)} - \frac{y}{x} \right| < \frac{1}{2x^2}
\]

Proof. We write the equation \( ex - y\phi(N) = 1 \) as
\[
\begin{align*}
& ex - y(p^r(q - 1) - p - 1) = 1 \\
& ex - y(p^r(pq - p - q + 1)) = 1 \\
& ex - y(p^r(pq - p^{r-1}q + p^{r-1})) = 1 \\
& ex - y(N - (p^r + p^{r-1}q - p^{r-1}q)) = 1 \\
& ex - y(N - (N - \phi(N))) = 1
\end{align*}
\]
Since \( N - \phi(N) = p^r + p^{r-1}q - p^{r-1} \) then
\[
\begin{align*}
ex - y \left( N - \left( \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} - 2 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right) \right) & = 1 \\
ex - y \left( N - \left( \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} + 2 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right) \right) & = 1 + y \left( N - \phi(N) - \frac{2x^{r-1} + 1}{2x^{r-1} + 1} N \frac{1}{x^{r-1} q^{r-1}} + 2 \frac{1}{x^{r-1} q^{r-1}} \frac{r}{x^{r-1}} \right)
\end{align*}
\]
For the Theorem 2.2, to satisfy it is suffice to show that if
\[ N \]
from which we can define
\[ N = 2^{r+1} N^{-\frac{r}{r+1}} - 2^{-\frac{r}{r+1}} N^{\frac{r+1}{r}} \]
Since \( e < \phi(N) < N - 2^{r+1} N^{-\frac{r}{r+1}} - 2^{-\frac{r}{r+1}} N^{\frac{r+1}{r}} \) and \( ex - y\phi(N) = 1 \), \( \phi(N) > \frac{1}{4} N \) with \( N > 8x \), then we have \( \phi(N) > \frac{1}{4} N > \frac{1}{4} \times 8x > 6x \) from the theorem \( \left( \frac{2r+1}{r+1} p^2 - \frac{2r^2}{r+1} q^2 \right) \left( p + 2^{r+1} q \right) < \frac{1}{4} N^\omega \) and \( x < N^\delta \) then
\[
\left| \frac{N - 2^{r+1} N^{-\frac{r}{r+1}} - 2^{-\frac{r}{r+1}} N^{\frac{r+1}{r}} - \phi(N)}{\phi(N)} \right| + \frac{1}{\phi(N)x} < \left( \frac{2r+1}{r+1} p^2 - \frac{2r^2}{r+1} q^2 \right) \left( p + 2^{r+1} q \right) + \frac{1}{\phi(N)x} < \frac{1}{4} N^\omega \]
For the Theorem 2.2, to satisfy it is suffice to show that if \( \omega - 1 < -2\delta \) then \( \delta < \frac{1}{2} \omega \), that is if
\[
\frac{1}{6} N^{\omega-1} + \frac{1}{6} N^{-2\delta} < \frac{1}{6} N^{\omega-1} + \frac{1}{6} N^{-2\omega+1} \]
from which we can find \( \frac{1}{6} N^{\omega-1} + \frac{1}{6} N^{-2\delta} \) among the convergent of the continued fraction expansion of
\[
N - \left( \frac{2^{r+1} N^{-\frac{r}{r+1}} - 2^{-\frac{r}{r+1}} N^{\frac{r+1}{r}}}{N} \right)
\]
The following algorithm is designed to recover the prime factors for prime power modulus \( N = p^t q \) in polynomial time.

\begin{algorithm}
\textbf{Input:} \( N = p^t q \), with \( q < p < 2q \) and public key \((e, N)\) and Theorem (3.4).
\textbf{Output:} the prime factors \( p \) and \( q \).
\begin{enumerate}
\item Compute the continued fraction expansion of \( \left( \frac{2^{r+1} N^{-\frac{r}{r+1}} - 2^{-\frac{r}{r+1}} N^{\frac{r+1}{r}}}{N} \right) \).
\item For each convergent \( \frac{a}{b} \) of \( \left( \frac{2^{r+1} N^{-\frac{r}{r+1}} - 2^{-\frac{r}{r+1}} N^{\frac{r+1}{r}}}{N} \right) \), compute \( \frac{a}{b} \).
\item Compute \( p^{t-1} = \gcd(N, \frac{a}{b}) \)
\item If \( 1 < p^{t-1} < N \), then \( q = \frac{N}{p^{t-1}} \)
\end{enumerate}
\end{algorithm}
Example 3.4. To illustrate our attack for \( r = 3 \), \( x = 43609 \), \( y = 19453 \), let us take for \( N \) and \( e \) the numbers
\[
N = 387586282188297761396493510683056643 \\
e = 172893575246095445935389209743994977
\]
Suppose that \( N \) and \( e \) satisfy all the condition stated in Theorem 9, then taking the continued fraction expansion of \( \frac{e}{N - \left( \frac{2r+1}{N^{r+1}} - 1 \right)} \) we get,
\[
[0, 2, 4, 7, 2, 1, 29, 1, 6, 1, 50, 3, 5, 5, 1, 5, 1, 1, 3, 1, 4112, 2, 1, 1, 1, 6, 23, 1, 1, 5, 1, 2, 1, 1] \\
[17, 5, 1, 1, 1, 101, 5, 1, 2, 3, 6, 5, 6, 1, 36, 12, 1, 8, 2, 2, 1, 5, 2, 4, 1, 1, 3, 3, 2]
\]
Applying the factorization algorithm with the convergent \( \frac{2}{r} = \frac{3700}{8033} \), we obtain
\[
\frac{ex - 1}{y} = \frac{(172893575246095445935389209743994977)(43609) - 1}{19453} \\
= 3875862809287501311177524703013719064
\]
Hence we compute
\[
p = \sqrt{gcd \left( N, \frac{ex - 1}{y} \right)} = 947438773.
\]
Finally for \( p = 605174881 \) we compute \( q = \frac{N}{p^2} = 455737679 \), which leads to the factorization of \( N \).

4 Second Attack on \( n \) RSA Moduli \( N_i = p_i^{r_i} q_i \)

For \( n \geq 2, r \geq 2 \), we let \( N_i = p_i^{r_i} q_i \), with \( i = 1, ..., n \). The research works upon \( n \) instances \( (N_i, e_i) \) to find the unknown integers \( x, y_i \), satisfying \( e_i x - y_i \phi(N_i) = 1 \) and \( e_i x_i - y_i \phi(N_i) = 1 \). We shows that the \( n \) moduli \( N_i \) for \( i = 1, ..., n \), can be factored in polynomial time if \( N = min \ N_i \), and

**Theorem 4.1** Suppose that \( N_i = p_i^{r_i} q_i \), \( 1 \leq i \leq n \) for \( n \geq 2 \), be \( n \) moduli. Let \( N = min \ N_i \) and \( e_i, i = 1, ..., n \), be \( n \) public exponents. Define \( \delta = \frac{n \omega n}{\omega n + 1} \) where \( 0 < \omega \leq 1 \). Let
\[
1 < e_i < \phi(N_i) < N_i - \psi \text{ where } \psi = N_i - 2^{\frac{2^{r+1}}{N^{r+1}}} N_i^{\frac{2^{r+1}}{N^{r+1}}} - 2^{\frac{2^{r+1}}{N^{r+1}}} N_i^{\frac{2^{r+1}}{N^{r+1}}}.
\]
If there exist an integer \( x < N_i^\delta \) and \( n \) integers \( y_i < N_i^\delta \) such that
\[
e_i x - y_i \phi(N_i) = 1
\]
for \( i = 1, ..., n \), then one can factor the \( n \) moduli \( N_1, ..., N_n \) in polynomial time.

**Proof.** Suppose that \( N_i = p_i^{r_i} q_i \), \( 1 \leq i \leq n \) be \( n \) moduli for \( n \geq 2 \), and \( r \geq 2 \). Let \( N = min \ N_i \), and \( y_i < N_i^\delta \). Then we can rewrite the equation \( e_i x - y_i \phi(N_i) = 1 \) as
\[
e_i x - y_i(N_i - (N_i - \phi(N_i))) = 1 \\
e_i x - y_i(N_i - \psi) = 1 - y_i(N_i - \phi(N_i)) - y_i \phi(N_i) = 1
\]
\[
\frac{e_i}{N_i - \psi} x - y_i = \frac{|1 - y_i(N_i - \phi(N_i) - \psi)|}{N_i - \psi} \tag{4.1}
\]
Let \( N = min \ N_i \), and suppose that \( y_i < N_i^\delta \), and \(|(N_i - \phi(N_i) - \psi)| < \left( 2^{\frac{2^{r+1}}{N^{r+1}}} p_i^{\frac{2^{r+1}}{N^{r+1}}} q_i^{\frac{2^{r+1}}{N^{r+1}}} \right) \)

80
\[ \left| p_i + 2 - \frac{2r+1}{p_i} r_i \frac{q_i}{q} \right|. \] Then
\[ \frac{1 - y_i(N_i - \phi(N_i) - \psi)}{N_i - \psi} \leq \frac{1 + y_i(N_i - \phi(N_i) - \psi)}{N - \psi} \]
\[ < \frac{1}{N} \left( N_i - 2 \frac{2r+1}{p_i} r_i \frac{q_i}{q} + 2 - \frac{2r+1}{p_i} r_i \frac{q_i}{q} \right) \]
\[ < \frac{1}{N} \phi(N) \]
\[ < \frac{N(\frac{1}{2}N\omega - \omega)}{4N} \]
\[ < \frac{1}{6} N^{\omega+\omega-n-1} \]

Plugging in to (1), to get
\[ \frac{e_i}{N_i - \psi} x - y_i < \frac{1}{6} N^{\omega+\omega-n-1} \]

Hence to shows the existence of the integer \( x \), we let \( \varepsilon = \frac{1}{6} N^{\omega+\omega-n-1} \), with \( \delta = \frac{2n-\omega+n}{(n+1)} \). Then we have
\[ N^\delta \varepsilon^n = \left( \frac{1}{6} \right)^n N^{\omega+\omega-n} = \left( \frac{1}{6} \right)^n \]

Therefore since \( \left( \frac{1}{6} \right)^n < 2^{\frac{n(n-3)}{2}} \cdot 3^n \) for \( n \geq 2 \), we get \( N^\delta \varepsilon^n < 2^{\frac{n(n-3)}{2}} \cdot 3^n \). It follows that if \( x < N^\delta \) then \( x < 2^{\frac{n(n-3)}{2}} \cdot 3^n \cdot \varepsilon^{-n} \) summarizing for \( i = 1, \ldots, n \), we have
\[ \frac{e_i x - y_i}{N_i - \psi} < \varepsilon, \quad x < 2^{\frac{n(n-3)}{2}} \cdot 3^n \cdot \varepsilon^{-n} \]

Hence Theorem 2.5, is satisfy and the unknown integers \( x \) and \( y_i \) for \( i = 1, \ldots, n \) can be obtain.

Next from the equation \( e_i x - y_i \phi(N_i) = 1 \) we get
\[ \frac{e_i x - 1}{y_i} = \phi(N_i) = p_i^{\epsilon-1}(p - 1)(q - 1) \]

Therefore by computing \( p_i^{\epsilon-1} = \gcd \left( \frac{e_i x - 1}{y_i}, N_i \right) \) leads to factorization of \( n \) moduli \( N_i, \ldots, N_n \). \( \square \)

Algorithm 2
1: Initialization: The public key \( (e_1, N_1) \) satisfying Theorem (4.1).
2: Choose \( x, \delta, N = \min(N_i) \).
3: For any \( (e, \omega, N, \delta, n) \) do
4: \( x = \frac{1}{2} N^{\omega+\omega-n-1} \).
5: \( C = \frac{3n+1}{2} \cdot \frac{2}{(n+1)(n-3)} \cdot \varepsilon^{-n-1} \)
6: end for
7: Consider the lattice \( L \) spanned by the matrix \( M \) as stated above.
8: Applying the LLL algorithm to \( L \) yields the reduced basis matrix \( K \), for any \( (M, K) \) do.
9: Compute \( U := M^{-1} \) and \( W = UK \)
10: end for
11: Produce \( x, y_i \) from \( W \)
12: for each triplet \( (x, y_i, e_i) \) do
13: \( G_i = \frac{e_i x - 1}{y_i} \) for \( i = 1, 2, 3 \)
14: Compute \( p_i^{\epsilon-1} = \gcd \left( N_i, \frac{e_i x - 1}{y_i} \right) \)
15: If \( 1 < p_i^{\epsilon-1} < N_i \) then \( q_i \) is a prime factor
16: end for
17: Return the prime factors \( (p_i, q_i) \)
Example 2. Illustration to our attack on n moduli, we consider the following three prime power and three public exponents

\[ N_1 = 4126740651452862084117424302390269071214683492426431138893 \]
\[ N_2 = 1109082416578983160043430528103952699560958091906830259177083 \]
\[ N_3 = 983682775103505316353506219847517029720435874943493873479 \]
\[ e_1 = 247501884692415639823438804037487074374822169001720148995939 \]
\[ e_2 = 68198736813831465919461357295405393173779982314077028345589 \]
\[ e_3 = 4894896422245154459393575470984472785152089243256548978533 \]

Then \( N = \max(N_1, N_2, N_3) = 4126740651452862084117424302390269071214683492426431138893 \).

For \( n = 3 \) and \( r = 3 \), \( \kappa = 0.1 \) with \( \omega = 0.9 \), we get \( \delta = \frac{n^{n-1} + 2}{(n+1)} = 0.150000000 \) and \( \varepsilon = \frac{1}{2}N^{\lambda+\kappa-1} = 0.001742081052 \). Using Theorem 2.5, we obtained.

\[ C = [3^{n+1} : 2^{\frac{(n+1)(n-4)}{4}}, \varepsilon^{-n-1}] = 43972544270000000 \]

Consider the lattice \( L \) spanned by the matrix

\[
M = \begin{bmatrix}
1 & -[Ce_1/(N_1 - \psi)] & -[Ce_2/(N_2 - \psi)] & -[Ce_3/(N_3 - \psi)] \\
0 & C & 0 & 0 \\
0 & 0 & C & 0 \\
0 & 0 & 0 & C
\end{bmatrix}
\]

Therefore applying the LLL algorithm to \( L \), we obtain the reduced basis with following matrix

\[
K = \begin{bmatrix}
-16199697757 & 370720847948 & -974078152524 & 232934958768 \\
255096849348 & 361440655572 & 1453867584336 & 1276999709248 \\
983992250454 & -46333657944 & -1091425830872 & 3253082328096 \\
5982788697340 & -126861359760 & 3588180829271 & 701960158140
\end{bmatrix}
\]

Next we compute

\[
U \cdot K = \begin{bmatrix}
-16199697757 & -9715777687 & -9961378048 & -806119354 \\
255096849348 & 152994503435 & 156861976167 & 126938572745 \\
-983992250454 & -590149896285 & -605068004978 & -489643698576 \\
5982788697340 & -126861359760 & 3588180829271 & 701960158140
\end{bmatrix}
\]

Then from the first row we obtained \( x = 16199697757, y_1 = 9715777687, y_2 = 9961378048, y_3 = 806119354 \). Hence using \( d \) and \( y_i \) for \( i = 1, 2, 3 \), define \( G_i = e_i x_1 y_i = \phi(N_i) = p_i^{r-1}(p-1)(q-1) \)

\[ G_1 = 4126740651452862084117424302390269071214683492426431138893 \]
\[ G_2 = 1109082416578983160043430528103952699560958091906830259177083 \]
\[ G_3 = 983682775103505316353506219847517029720435874943493873479 \]

Therefore for \( i = 1, 2, 3 \) we compute \( p_i = \sqrt{gcd \left( \frac{n^{n-1}}{y_i}, N_i \right)} \), that is

\[ p_1 = 982781973715051, p_2 = 982781973715051, p_3 = 728752160621389 \]

And finally for \( i = 1, 2, 3 \) we find \( q_i = \frac{N_i}{p_i} \), hence

\[ q_1 = 43474613214943, q_2 = 143631635582489, q_3 = 254164856763691 \]
Which leads to the factorization of three moduli $N_1, N_2, \text{and } N_3$.

**Theorem 4.2** Suppose that $N_i = p_i^i q_i$, $1 \leq i \leq n$ be $n$ moduli with the same size $N$. Let $e_i$, $i = 1, \ldots, n$, be $n$ public exponents with $\min e_i = N^\sigma$, $0 < \sigma < 1$. Let $\delta = \frac{n(n+\sigma-\omega)}{(4+n)}$ where $0 < \omega \leq 1$. If there exist an integer $y < N^\delta$ and $n$ integers $x_i < N^\delta$ such that $e_i x_i - y \phi(N_i) = 1$ for $i = 1, \ldots, n$, then one can factor the $n$ moduli $N_1, \ldots, N_n$ in polynomial time.

**Proof.** Suppose that $N_i = p_i^i q_i$, $1 \leq i \leq n$ be $n$ moduli for $n \geq 2$, and $r \geq 2$. Then we transform $e_i x_i - y \phi(N_i) = 1$ as

$$\frac{|N_i - y - x_i|}{e_i} = \frac{|1 - y(N_i - \phi(N_i)) - \psi|}{e_i}$$  \hspace{1cm} (4.2)

Let $N = \max N_i$, and suppose that $y < N^\delta$, $\min e_i = N^\sigma$ and $|\phi(N_i) - \psi|$

$$< \left(2 + \frac{2 r^2 - r^1}{p_i + 2 + \frac{2 r^2 - r^1}{q_i}}\right) \left(\frac{p_i + 2 + \frac{2 r^2 - r^1}{q_i}}{q_i}\right) - \frac{r^2}{r^1}.$$  \hspace{1cm} (4.2)

Then

$$\frac{|1 - y(N_i - \phi(N_i) - \psi)|}{e_i} \leq \frac{|1 + y(N_i - \phi(N_i) - \psi)|}{N^\sigma} < \frac{1 + N^\delta \left(2 + \frac{2 r^2 - r^1}{p_i + 2 + \frac{2 r^2 - r^1}{q_i}}\right) \left(\frac{p_i + 2 + \frac{2 r^2 - r^1}{q_i}}{q_i}\right) - \frac{r^2}{r^1}}{N^\sigma} < \frac{N^\delta (\frac{1}{2} N^\omega - \kappa)}{N^\sigma} < \frac{1}{8} N^\delta + \omega - \kappa - \sigma$$

Plugging in to (2), to get

$$\frac{|N_i - y - x_i|}{e_i} < \frac{1}{8} N^\delta + \omega - \kappa - \sigma$$

Hence in order to find the unknown integers $y, x_i$, we let $\epsilon = \frac{1}{8} N^\delta + \omega - \kappa - \sigma$, with $\delta = \frac{n(n+\sigma-\omega)}{(4+n)}$.

Then we have

$$N^\delta \epsilon = \left(\frac{1}{8}\right)^n N^\delta + \delta \omega + \omega - \kappa - \sigma = \left(\frac{1}{8}\right)^n$$

Therefore since $\left(\frac{1}{8}\right)^n < 2^{\frac{n(n-3)}{4}} \cdot 3^n$ for $n \geq 2$, we get $N^\delta \epsilon < 2^{\frac{n(n-3)}{4}} \cdot 3^n$. It follows that if $y < N^\delta$ then $y < 2^{\frac{n(n-3)}{4}} \cdot 3^n \cdot \epsilon^{-n}$ summarizing for $i = 1, \ldots, n$, we have

$$\frac{|N_i - y - x_i|}{e_i} < \epsilon, \quad y < 2^{\frac{n(n-3)}{4}} \cdot 3^n \cdot \epsilon^{-n}$$

Hence Theorem 2.5, is satisfy and we can obtain the unknown integers $y$ and $x_i$ for $i = 1, \ldots, n$.

Next from the equation $e_i x_i - y \phi(N_i) = 1$ we get

$$e_i x_i - \frac{1}{y} = \phi(N_i) = p_i^{r-1} (q_i - 1)$$

Therefore by computing $p_i^{r-1} = \left(\frac{\epsilon^{-r}}{p_i}, N_i\right)$ leads to factorization of $n$ prime power moduli $N_i, \ldots, N_n$. \hfill $\Box$
Algorithm 3

1: Initialization: The public key \((e_i, N_i)\) satisfying Theorem (4.2).
2: Choose \(n, \delta, N = \min(N_i)\).
3: For any \((e, \omega, \sigma, \delta, n)\) do
   4: \(\epsilon = \frac{1}{2} \cdot \frac{1}{n+1} - \frac{(n+1)(n-4)}{4} \cdot e^{-n-1}\)
   5: \(C = [3^{n+1} \cdot 2^{(n+1)(n-4)}, e^{-n-1}]\)
4: end for
7: Consider the lattice \(L\) spanned by the matrix \(M\) as stated above.
8: Applying the LLL algorithm to \(L\) yields the reduced basis matrix \(K\), for any \((M, K)\) do.
9: Compute \(U = M^{-1}\) and \(W = UK\)
10: for each triplet \((x_i, y, e_i)\) do
   11: \(G_i = e^{-1} x_i^e - \frac{\psi}{N_i} - \frac{\omega}{\epsilon}\)
   12: Compute \(p_{i}^{-1} = \gcd(N_i, e_{i}^{-1} x_i^e - \frac{\psi}{N_i} - \frac{\omega}{\epsilon})\)
   13: If \(1 < p_{i}^{-1} < N_i\), then \(q_i = \frac{N_i p_i}{p_{i}^{-1}}\)
   14: end for
15: Return the prime factors \((p_i, q_i)\)

Example 3. As an illustration to our attack on \(j\) moduli, we consider the following three prime power and three public exponents

\[
N_1 = 526958416483528951577464338043023736259642678718725418043 \\
N_2 = 9533112375942057553333091631211100569838316635745740203519 \\
N_3 = 310718626963867940790436681707216087278093583076872081556769 \\
e_1 = 189587867285071400829715799314636883375794280812798295130 \\
e_2 = 12601528934607376010170969898987592250407843515108325704858876 \\
e_3 = 8805078568734181465514602669578139909559056780558841963914
\]

Then \(\hat{N} = \max(N_1, N_2, N_3) = 310718626963867940790436681707216087278093583076872081556769\).
Also \(\min(e_1, e_2, e_3) = N^\sigma\) with \(\sigma = 0.2999\), \(n = 3\) and \(r = 3\) with \(\kappa = 0.5432\), we get \(\delta = \frac{\sigma + \omega - \kappa - \sigma}{n+1} = 0.1578000000\) and \(\epsilon = \frac{1}{2} \cdot \frac{1}{n+1} - \frac{(n+1)(n-4)}{4} \cdot e^{-n-1}\). Using Theorem 2.5, we obtained,

\[
C = [3^{n+1} \cdot 2^{(n+1)(n-4)}, e^{-n-1}] = 34110577000000000
\]

Consider the lattice \(L\) spanned by the matrix

\[
M = \begin{bmatrix}
1 & -[C(N_1 - \psi)/e_1] & -[C(N_2 - \psi)/e_2] & -[C(N_3 - \psi)/e_3] \\
0 & C & 0 & 0 \\
0 & 0 & C & 0 \\
0 & 0 & 0 & C
\end{bmatrix}
\]

Therefore applying the LLL algorithm to \(L\), we obtain the reduced basis with following matrix

\[
K = \begin{bmatrix}
-9754353227 & 2454036955 & 10807224176 & -968330316587 \\
220559537355 & 3153932693925 & -126651060240 & 408501423755 \\
2143028210095 & 788021901825 & 259213251460 & 72036739695 \\
1871293353295 & -481263926175 & -3370772406960 & -219598341105
\end{bmatrix}
\]

Next we compute

\[
U \cdot K = \begin{bmatrix}
-9754353227 & -271141163 & -737921136 & -34421717171 \\
220559537355 & 6130886820 & 16685426555 & 778123056129 \\
2143028210095 & 50569690041 & 16212031961 & 7562439991734 \\
1871293353295 & 52016285007 & 141564169855 & 6605526553949
\end{bmatrix}
\]
Then from the first row we obtained \( y = 9754353227, \) \( x_1 = 271141463, \) \( x_2 = 737921136, \) \( x_3 = 34421717171. \) Hence using \( x_i \) and \( y \) for \( i = 1, 2, 3, \) define \( G_i = e_i x_i \) \( 1 \) \( y = \phi(N_i) = p_i^r - 1 (p_i - 1) (q_i - 1) \)

\[
G_1 = 5269854816434953569885140018315624445934914435956070504 \\
G_2 = 953311237594199603535313982589223729428435532070646941728 \\
G_3 = 31071862696386679763427868358684570095348237020566762935120
\]

Therefore for \( i = 1, 2, 3 \) we compute \( p_i = \sqrt{\text{gcd} \left( \frac{e_i x_i - 1}{y}, N_i \right) \} \), that is

\[
p_1 = 632118267940813, \quad p_2 = 790851855676273, \quad p_3 = 932093177449669
\]

And finally for \( i = 1, 2, 3 \) we find \( q_i = \frac{N_i}{p_i} \), hence

\[
q_1 = 208642907616719, \quad q_2 = 1927299898333807, \quad q_3 = 383697793509941
\]

Which leads to the factorization of three prime power moduli \( N_1, N_2, \) and \( N_3. \)

5 Conclusion

The study consider \( N - \left(2^{\frac{e_i - 1}{r}} N^{\frac{r-1}{r}} - 2^{\frac{e_i - 1}{r}} N^{\frac{r-1}{r}} \right) \) as a good approximation of \( \phi(N_i) \) using the modulus \( N = p^r q. \) From the approximation we show that \( \frac{e_i - 1}{r} \) can be recovered among the convergents of the continued fraction expansion of \( \frac{e_i x_i - 1}{y} \) which lead factorization of prime power modulus \( N = p^r q \) in polynomial time. Furthermore, by using the LLL algorithm for \( n \geq 2, \) \( r \geq 2, \) with \( n \) public exponents \( (N_i, e_i) \) satisfying \( n \) relations of the form \( e_i x_i - y_i \phi(N_i) = 1 \) or of the form \( e_i x_i - y_i \phi(N_i) = 1 \) where the unknown parameters \( x, x_i, y, y_i, i = 1, ..., n \) are suitably small in terms of the prime factors of the moduli, enable us to simultaneously factor the \( n \) prime power moduli \( N_i = p_i^r q_i, i = 1, ..., n \) in polynomial time.

Declarations’

Availability of Data and Materials

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Competing Interests

The authors declare that they have no competing interests.

References


© 2020 Shehu et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

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/64279