Journal of Mathematical Sciences and Modelling, 6 (1) (2023) 1-6
Research Article

Journal of Mathematical Sciences and Modelling

Journal Homepage: www.dergipark.gov.tr/jmsm
ISSN 2636-8692
DOI: http://dx.doi.org/10.33187/jmsm.1135988

Asymptotic Bound for RSA Variant with Three Decryption Exponents

Saidu Isah Abubakar[1*], Zaid Ibrahim[1] and Aminu Alhaji Ibrahim[2]

[1]*Department of Mathematics, Faculty of Science, Sokoto State University, Sokoto, Nigeria*
[2]*Department of Mathematics, Faculty of Science, Usmanu Danfodiyo University, Sokot, Nigeria*
[*]*Corresponding Author*

Article Info

Keywords: *Asymptotic, Bound, Cryptanalysis, Decryption, Exponents, RSA variants*
2010 AMS: *11T71*
Received: *26 June 2022*
Accepted: *4 October 2022*
Available online: *2 December 2022*

Abstract

This paper presents a cryptanalysis attack on the RSA variant with modulus $N = p^r q$ for $r \geq 2$ with three public and private exponents (e_1, d_1), (e_2, d_2), (e_3, d_3) sharing the same modulus N where p and q are consider to be primes having the same bit size. Our attack shows that we get the private exponent $\sigma_1\sigma_2\sigma_3 < \left(\frac{r-1}{r+1}\right)^4$, which makes the modulus vulnerable to Coppersmith's attacks and can lead to the factorization of N efficiently where $d_1 < N^{\sigma_1}$, $d_2 < N^{\sigma_2}$, and $d_3 < N^{\sigma_3}$. The asymptotic bound of our attack is greater than the bounds for May [1], Zheng and Hu [2], and Lu et al. [3] for $2 \leq r \leq 10$ and greater than Sarkar's [4] and [5] bounds for $5 \leq r \leq 10$.

1. Introduction

The importance of keeping information secret cannot be overemphasized, especially in this digital era where intruders can easily eavesdrop on someone's information and get access to his private belongings. The Construction of strong encryption scheme(s) using complex mathematics provides confidentiality and privacy to our daily transactions and communication as they pass through insecure communication channels.
The most acceptable and widely used public key cryptosystem is the RSA cryptosystem which was invented in 1976 by Rivest, Shamir, and Adleman [6]. The security of RSA modulus $N = pq$ relies on the integer factorization problem and was first exploited using a private exponent attack by Wiener (1990) as reported in [7]. Other cryptanalysis attacks that led to the polynomial time factorization of the RSA modulus $N = pq$ can be found in [8, 9].
In order to improve the security of standard RSA modulus $N = pq$, various researchers proposed many variants. Prime power modulus $N = p^r q$ for $r \geq 2$ was among the RSA variants developed by Takagi using the Chinese remainder theorem showing that the decryption process is faster than the standard RSA [10]. Also, Boneh et al. presented a partial exposure attack where they proved that prime power modulus $N = p^r q$ can be efficiently factored if someone knows $\frac{1}{r+1}$ fraction of the most significant bits (MSBs) of the prime factors p [11].
The decryption exponent bound of [10] was improved from $d < N^{\frac{1}{2(r+1)}}$ to $d < N^{\frac{r}{(r+1)^2}}$ or $d < N^{\left(\frac{r-1}{r+1}\right)^2}$ by May [1] using the lattice-based technique. Sarkar [4] presented a small secret exponent attack on prime power modulus $N = p^r q$ for $r \geq 2$ where he improved the work of [1] for $r \leq 5$. Similarly, Sarkar improved his work [4] when $2 \leq r \leq 8$ as reported in [5] with a decryption exponent bound of $d < N^{\frac{1}{r+1} + \frac{3r-2\sqrt{3r+3}+3}{3(r+1)}}$. Lu et al. [3] proved that prime power modulus $N = p^r q$ when $r \geq 2$ can be factored efficiently when the decryption exponent bound $d < N^{\frac{r(r-1)}{(r+1)^2}}$. Moreover, Zheng and Hu [2] proposed a cryptanalysis lattice-based construction attack on prime power RSA modulus $N = p^r q$ for $r \geq 2$ with two decryption exponents where they have shown that N is insecure when $\delta_1\delta_2 < N^{\left(\frac{r-1}{r+1}\right)^3}$ where $d_1 < N^{\delta_1}$ and $d_2 < N^{\delta_2}$. By assuming $\delta_1 = \delta_2 = \delta$, [2] made comparisons with previous results of [1, 4] when $r \geq 4$.
In this paper, we employ a similar approach to [2] using lattice-based approach except that we utilize three pairs of public and private exponents (e_1, d_1), (e_2, d_2), and (e_3, d_3) of RSA variant $N = p^r q$ for $r \geq 2$ with three decryption exponents sharing common modulus N, and prove that the security of prime power moduli N can be broken and prime factors p and q can be factored in polynomial-time. We assume $d_1 = N^{\sigma_1}$, $d_2 = N^{\sigma_2}$ and $d_3 = N^{\sigma_3}$ to be the decryption exponents where $d_1 = d_2 = d_3 = d = \sigma$ for $0 < \sigma < 1$ and utilize generalized key

Email addresses and ORCID numbers: **siabubakar82@gmail.com, 0000-0002-0201-0064 (S. I. Abubakar), malamzaid2@gmail.com, 0000-0002-0251-6495 (Z. Ibrahim), aminualhaji40@gmail.com, 0000-0001-5957-3223 (A. A. Ibrahim)**
Cite as "S.I. Abubakar, Z. Ibrahim, A. A. Ibrahim, *Asymptotic Bound for RSA Variant with Three Decryption Exponents*, J. Math. Sci. Model., 6(1) (2023), 1-6"

equation $e_id_i = 1 + k_i\phi(N)$, where $k_i \in \mathbb{Z}$ and $\phi(N) = p^{r-1}(p-1)(q-1)$ for the construction of three equations of the form

$$e_1d_1 = 1 + k_1p^{r-1}(p-1)(q-1), \tag{1.1}$$
$$e_2d_2 = 1 + k_2p^{r-1}(p-1)(q-1), \tag{1.2}$$
$$e_3d_3 = 1 + k_3p^{r-1}(p-1)(q-1), \tag{1.3}$$

for some positive integers k_1, k_2, k_3. Let e'_1, e'_2, e'_3 be the inverses of $e_1, e_2, e_3 \mod N$ respectively. Then we get:

$$e_1e'_1 = z_1N + 1, \tag{1.4}$$
$$e_2e'_2 = z_2N + 1, \tag{1.5}$$
$$e_3e'_3 = z_3N + 1, \tag{1.6}$$

for some positive integers z_1, z_2, z_3. In order to easily get the prime factors of N, we assume that inverses e'_1, e'_2, or e'_3 does not exist, we can then get the result through finding the $\gcd(e_1, N)$, $\gcd(e_2, N)$ and $\gcd(e_3, N)$. Multiplying equations (1.1) by e'_1 and (1.4) by d_1 respectively and equating them give

$$d_1 - e'_1 = [e'_1k_1(p-1)(q-1) - d_1z_1pq]p^{r-1}. \tag{1.7}$$

Similarly, for equations (1.2) and (1.5) we get the following equation

$$d_2 - e'_2 = [e'_2k_2(p-1)(q-1) - d_2z_2pq]p^{r-1} \tag{1.8}$$

Also, for equations (1.3) and (1.6), we get the following equation

$$d_3 - e'_3 = [e'_3k_3(p-1)(q-1) - d_3z_3pq]p^{r-1}. \tag{1.9}$$

Equations (1.7), (1.8) and (1.9) reduce to the following equations respectively

$$d_1 - e'_1 = 0 \mod p^{r-1}, \tag{1.10}$$
$$d_2 - e'_2 = 0 \mod p^{r-1}, \tag{1.11}$$
$$d_3 - e'_3 = 0 \mod p^{r-1}. \tag{1.12}$$

Applying method of [12] for solving multivariate linear equations modulo unknown divisor, we can estimate the unknown divisor of our attacks. Since the modulus is $N = p^rq$ for $r \geq 2$ and $q < p < 2q$. Multiplying by p^r gives $N < p^{r+1} < 2N$. Since $q \approx p \approx N^{\frac{1}{r+1}}$, we have $p^{r-1} \approx N^{\frac{r-1}{r+1}}$.
Moreover, the Coppersmith technique will be deployed in finding small roots of the constructed modular equations which can later be transformed into finding them over integers. This can be achieved through constructing a set of polynomials sharing common root modulo R to produce some integer linear combinations of the constructed polynomials' coefficient vectors whose norm is expected to be sufficiently small using the LLL algorithm. This enables us to get an asymptotic bound $\sigma < \left(\frac{r-1}{r+1}\right)^{\frac{4}{3}}$, where $d_1 < N^{\sigma_1}$, $d_2 < N^{\sigma_2}$, $d_3 < N^{\sigma_3}$. Also, we assume $\sigma_1 = \sigma_2 = \sigma_3 = \sigma$ in order to compare our results with the theoretical results of [1], [2], [3], [4] and [5], our work show that for $5 \leq r \leq 10$ we obtain better bounds.
The rest of the paper is organised as follows. In section 2, we give definitions of lattice and determinant, some important theorems and a lemma to be used in this research. Section 3 presents the major contributions of this paper where results are thoroughly discussed and comparisons of theoretical bounds with earlier reported bounds are presented. Finally, in Section 4 we conclude the paper.

2. Preliminaries

In this section, we define some basic terms that are found to be useful in this research work.

Definition 2.1 (Lattice)**.** *A lattice $\mathscr{L}$ is a discrete additive subgroup of $\mathbb{R}^m$. Let $b_1, \cdots, b_n \in \mathbb{R}^m$ be $n \leq m$ linearly independent vectors. The lattice generated by $\{b_1, \cdots, b_n\}$ is the set*

$$\mathscr{L} = \sum_{i=1}^{n} \mathbb{Z}b_i = \left\{ \sum_{i=1}^{n} x_ib_i | x_i \in \mathbb{Z} \right\}.$$

The set $B = \langle b_1, \cdots, b_n \rangle$ is called a lattice basis for $\mathscr{L}$. The lattice dimension is $dim(\mathscr{L}) = n$. If $n = m$ then $\mathscr{L}$ is said to be a full rank lattice.
A lattice $\mathscr{L}$ can be represented by a basis matrix. Given a basis B, a basis matrix M for the lattice generated by B is the $n \times m$ matrix defined by the rows of the set $b_1 ..., b_n$

$$M = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

It is often useful to represent the matrix M by B. A very important notion for the lattice $\mathscr{L}$ is the determinant [13].

Definition 2.2 (Determinant [13])**.** *Let $\mathscr{L}$ be a lattice generated by the basis $B = \langle b_1, ..., b_n \rangle$. The determinant of $\mathscr{L}$ is defined as*

$$det(\mathscr{L}) = \sqrt{det(BB^T)}.$$

If $n = m$, we have

$$det(\mathscr{L}) = \sqrt{det(BB^T)} = |det(B)|.$$

Theorem 2.3 ([2], [14]). *Let L be a lattice spanned by a basis $(b_1, b_2, \cdots, b_m)$. The Lenstra-Lenstra-Lovasz (LLL) algorithm outputs a reduced basis $(v_1, v_2, \cdots, v_m)$ of L in polynomial time that satisfies*

$$||V_1||, ||V_2||, \cdots, ||V_m|| \leq 2^{\frac{m(m-1)}{4(m+1-i)}} det(L)^{\frac{1}{(m+1-i)}}$$

for $1 \leq i \leq m$.

For $i = 3$, the above LLL equation becomes

$$||V_1||||V_2||||V_m|| \leq 2^{\frac{m(m-1)}{4(m-2)}} det(L)^{\frac{1}{(m-2)}}.$$

Lemma 2.4 ([15]). *Let $g(x_1, x_2, \cdots, x_n) \in \mathbb{Z}[x_1, x_2, \cdots, x_n]$ be an integer polynomial that is a sum of at most m monomials. Suppose that*

1. $g(x_1^{(0)}, x_2^{(0)}, \cdots, x_n^{(0)}) \equiv 0(\mod R)$, *where* $|x_1^{(0)}|X_1, \cdots, |x_n^{(0)}| < X_n$,
2. $||g(x_1X_1, x_2X_2, \cdots, x_nX_n)|| < \frac{R}{\sqrt{m}}$.

   This can also be true over the integers $(x_1^{(0)}, x_2^{(0)}, \cdots, x_n^{(0)}) = 0$.

Thus we can solve the polynomials derived from the LLL algorithm. Consider the three basis vectors by the LLL algorithm, the condition for finding common root over the integers is as follows

$$2^{\frac{m(m-1)}{4(m-2)}} det(L)^{\frac{1}{(m-2)}} < \frac{R}{\sqrt{m}},$$
$$2^{\frac{m(m-1)}{4(m-2)}} det(L) < R^{m-2}M^{-\frac{m-2}{2}},$$
$$det(L) < R^{m-2}M^{-\frac{m-2}{2}}2^{-\frac{m(m-1)}{4(m-2)}}.$$

Since we usually have $m < R$, an error term ε is used on behalf of the small terms except R^m, then the above equation reduces to $det(L) < R^{m-\varepsilon}$.
We obtain a lower triangular basis matrix in our method all the time. The determinant can be calculated as $det(L) = N^{sN}X_1^{s_1}X_2^{s_2}X_3^{s_3}$ where s_i denotes the sum of the total exponents of X_i or N that appears on the diagonal. Hence we give the following condition

$$N^{sN}X_1^{s_1}X_2^{s_2}X_3^{s_3} < R^m. \tag{2.1}$$

3. Results

This section presents the major findings of this paper. The discussion is as follows:
To solve equations (1.10-1.12), we apply shift polynomials technique for a positive integer u as define below:

$$pj_1, pj_2, pj_3(x_1, x_2, x_3) = (x_1 - e_1')^{j_1}(x_2 - e_2')^{j_2}(x_3 - e_3')^{j_3}N^{\max(u-j_1-j_2-j_3,0)}$$

where $|x_1| < X_1,\ |x_2| < X_2,\ |x_3| < X_3$.
So all the polynomials $pj_1, pj_2, pj_3(x_1, x_2, x_3)$ share common root $(d_1, d_2, d_3) \mod p^{u(r-1)}$. The optimal condition for choosing the shift polynomials is given in [12], thus applying it in our case with three unknown private keys we have

$$0 \leq \sigma_1 j_1 + \sigma_2 j_2 + \sigma_3 j_3 \leq \frac{r-1}{r+1}u.$$

When we consider a general case where $\sigma_1 = \sigma_2 = \sigma_3 = \sigma$, we get a more concise condition as

$$0 \leq j_1 + j_2 + j_3 \leq \left(\frac{r-1}{r+1}\right)\frac{u}{\sigma}.$$

Taking $u = r = 3$, we can search for integer linear combinations of all

$$pj_1, pj_2, pj_3(x_1X_1, x_2X_2, x_3X_3)$$

by the LLL algorithm and ensure that its norm is sufficiently small to satisfy the conditions of Lemma 2.4. Thus, we have

$$pj_1, pj_2, pj_3(x_1, x_2, x_3) = (x_1 - e_1')^{j_1}(x_2 - e_2')^{j_2}(x_3 - e_3')^{j_3}N^{\max(u-j_1-j_2-j_3,0)}.$$

Using the above equation, we derive the following monomials:

$p(i_1,i_2,i_3)$	1	x_1	x_2	x_3	x_1x_2	x_2x_3	x_1x_3	x_1^2	x_2^2	x_3^2	x_1^3	$x_1x_2x_3$	$x_1^2x_2$	$x_2^2x_3$	$x_2x_3^2$	x_2^3	x_3^3	x_1^4	$x_2^3x_3$	$x_2x_3^3$	$x_2^2x_3^2$
$p(0,0,0)$	N^3																				
$p(1,0,0)$	*	X_1N^2																			
$p(0,1,0)$	*	*	X_2N^2																		
$p(0,0,1)$	*	*	*	X_3N^2																	
$p(1,1,0)$	*	*	*	*	X_1X_2N																
$p(0,1,1)$	*	*	*	*	*	X_2X_3N															
$p(1,0,1)$	*	*	*	*	*	*	X_1X_3N														
$p(2,0,0)$	*	*	*	*	*	*	*	X_1^2N													
$p(0,2,0)$	*	*	*	*	*	*	*	*	X_2^2N												
$p(0,0,2)$	*	*	*	*	*	*	*	*	*	X_3^2N											
$p(3,0,0)$	*	*	*	*	*	*	*	*	*	*	X_1^3										
$p(1,1,1)$	*	*	*	*	*	*	*	*	*	*	*	$X_1X_2X_3$									
$p(0,2,1)$	*	*	*	*	*	*	*	*	*	*	*	*	$X_1^2X_2$								
$p(0,2,1)$	*	*	*	*	*	*	*	*	*	*	*	*	*	$X_2^2X_3$							
$p(0,1,2)$	*	*	*	*	*	*	*	*	*	*	*	*	*	*	$X_2X_3^2$						
$p(0,3,0)$	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	X_2^3					
$p(0,0,3)$	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	X_3^3				
$p(4,0,0)$	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	X_1^4			
$p(0,3,1)$	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	$X_2^3X_3$		
$p(0,1,3)$	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	$X_2X_3^3$	
$p(0,2,3)$	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	$X_2^2X_3^3$

Table 3.1: Monomials

Taking u as a given parameter, the dimension m of the full-rank lattice can be calculated which can further allow us to compute $\det(L)$. This can be computed by enumerating the exponential numbers of X_1, X_2, X_3 and N respectively from the lower triangular square matrix s depicted above. Thus we get

$$m = \sum_{\sigma_1 j_1+\cdots+\sigma_n j_n}^{1} 1 = \frac{u^n}{n!}\frac{\beta^n}{\sigma_1\cdots\sigma_n} + o(u^n), \quad \beta = \frac{r-1}{r+1}.$$

So, in our case $m = n = 3$, we have

$$m = \sum_{\sigma_1 j_1+\sigma_2 j_2+\sigma_3 j_3}^{\frac{r-1}{r+1}u} 1 = \frac{1^3}{6}\frac{\left(\frac{r-1}{r+1}u\right)^3}{\sigma_1\sigma_2\sigma_3} = \frac{1}{6\sigma_1\sigma_2\sigma_3}\left(\frac{r-1}{r+1}u\right)^3 + o(u^3).$$

Also, to compute u_N we can use similar method as outlined in [2] and [12]. Thus, we have

$$\begin{aligned}
u_N &= \sum_{i_1+i_2+\cdots+j_n=0}^{s} (\sum_{i=j}^{n} j_i + n - 1)(u - \sum_{i=1}^{n} j_i) = \frac{u^{n+1}}{(n+1)!} + o(u^{n+1}),\\
u_N &= \frac{1}{4!}u^4 + o(u^4) = \frac{1}{24}u^4 + o(u^4),\\
u_n &= \sum_{\sigma_1+\sigma_2+\cdots\sigma_j n=0} jn = \frac{u^{n+1}}{(n+1)!}\frac{\beta^{n+1}}{\sigma_1\cdots\sigma_{i-1}\sigma_j^2\sigma_i+\sigma_n} + o(u^{n+1}),\\
u_1 &= \sum_{\sigma_1 j_1+\sigma_2 j_2+\sigma_3 j_3=0}^{\frac{r-1}{r+1}u} j_1 = \frac{1^4}{24}\frac{\left(\frac{r-1}{r+1}u\right)^4}{\sigma_1^2\sigma_2\sigma_3} = \frac{1}{24\sigma_1^2\sigma_2\sigma_3}\left(\frac{r-1}{r+1}u\right)^4 + o(u^4),\\
s_2 &= \sum_{\sigma_1 j_1+\sigma_2 j_2+\sigma_3 j_3=0}^{\frac{r-1}{r+1}u} j_2 = \frac{1^4}{24}\frac{\left(\frac{r-1}{r+1}u\right)^4}{\sigma_1\sigma_2^2\sigma_3} = \frac{1}{24\sigma_1\sigma_2^2\sigma_3}\left(\frac{r-1}{r+1}u\right)^4 + o(u^4),\\
s_3 &= \sum_{\sigma_1 u_1+\sigma_2 u_2+\sigma_3 u_3=0}^{\frac{r-1}{r+1}u} j_3 = \frac{1^4}{24}\frac{\left(\frac{r-1}{r+1}u\right)^4}{\sigma_1\sigma_2\sigma_3^2} = \frac{1}{24\sigma_1\sigma_2\sigma_3^2}\left(\frac{r-1}{r+1}u\right)^4 + o(u^4).
\end{aligned}$$

Since, we have $det(L) = N^{un}X_1^{u_1}X_2^{u_2}X_3^{u_3}$ for $X_1 = N^{\sigma_1}$, $X_2 = N^{\sigma_2}$, $X_3 = N^{\sigma_3}$ as mentioned above.The norms of the first three vectors can be sufficiently small only if the condition for finding the common root is fulfilled as derived from LLL-reduced basis. This can further be transformed using Lemma 2.4 into the corresponding polynomials with same root and lastly solve for the integers (d_1, d_2, d_3) We can now estimate σ_1, σ_2, σ_3. Using equation 2.1, we have

$$N^{\frac{1}{24}s^4+o(u^4)}N^{\sigma_1\frac{1}{24\sigma_1^2\sigma_2\sigma_3}\left(\frac{r-1}{r+1}u\right)^4+o(u^4)}N^{\sigma_2\frac{1}{24\sigma_1\sigma_2^2\sigma_3}\left(\frac{r-1}{r+1}u\right)^4+o(u^4)}N^{\sigma_3\frac{1}{24\sigma_1\sigma_2\sigma_3^2}\left(\frac{r-1}{r+1}u\right)^4+o(u^4)} < N^{\frac{r-1}{r+1}u\frac{1}{6\sigma_1\sigma_2\sigma_3}\left(\frac{r-1}{r+1}u\right)^3+o(u^3)}.$$

Taking $u \to \infty$ and omitting the lower term $o(u^3)$ gives the following result

$$\begin{aligned}
\frac{1}{24} + \frac{1}{24\sigma_1\sigma_2\sigma_3}\left(\frac{r-1}{r+1}\right)^4 + \frac{1}{24\sigma_1\sigma_2^2\sigma_3}\left(\frac{r-1}{r+1}\right)^4 + \frac{1}{24\sigma_1\sigma_2\sigma_3^2}\left(\frac{r-1}{r+1}\right)^4 &< \frac{1}{6\sigma_1\sigma_2\sigma_3}\left(\frac{r-1}{r+1}\right)^4\\
\sigma_1\sigma_2\sigma_3 &< \left(\frac{r-1}{r+1}\right)^4
\end{aligned}$$

In order to make comparison with other bounds, we assume $\sigma_1 = \sigma_2 = \sigma_3 = \sigma$ as shown in Table 3.2. It gives asymptotic bound of $\sigma < \left(\frac{r-1}{r+1}\right)^{\frac{4}{3}}$.

r	$\left(\frac{r-1}{r+1}\right)^{\frac{4}{3}}$	[1]	[2]	[3]	[4]	[5]
2	0.231	0.222	0.192	0.222	0.395	0.395
3	0.396	0.250	0.353	0.375	0.461	0.410
4	0.506	0.360	0.464	0.480	0.508	0.437
5	0.582	0.444	0.544	0.550	0.545	0.464
6	0.638	0.510	0.603	0.610	0.574	0.489
7	0.681	0.562	0.649	0.65	0.598	0.512
8	0.715	0.605	0.685	0.690	0.619	0.532
9	0.742	0.640	0.715	0.720	0.637	0.549
10	0.868	0.669	0.740	0.743	0.653	0.565

Table 3.2: Comparison of Bounds

From Table 3.2, one can observe that, our bound is better than [2], [4] and [5] for $r \geq 2$ and also better than all the compared bounds for $5 \leq r \leq 10$.

4. Conclusion

This paper shows that prime power RSA modulus $N = p^r q$ for $r \geq 2$ with three decryption exponents can be attacked using lattice-based attack through combinations of Coppersmith's and [12] lattice-base construction methods. We also showed that the modulus N is insecure if $d_1 < N^{\sigma_1}$, $d_2 < N^{\sigma_2}$ and $d_3 < N^{\sigma_3}$ which yielded asymptotic bound $\sigma < \left(\frac{r-1}{r+1}\right)^{\frac{4}{3}}$. Our results is an improvement on the work of [1], [2], [3], [4] and [5].

Article Information

Acknowledgements: The authors would like to express their sincere appreciation to the Tertiary Education Trust Fund (TETFund) for sponsoring this research work and Sokoto State University for its recommendation and forwarding the proposal to TETFund for approval.

Author's contributions: All authors contributed equally to the writing of this paper. All authors read and approved the final manuscript.

Conflict of Interest Disclosure: No potential conflict of interest was declared by the author.

Supporting/Supporting Organizations: Tertiary Education Trust Fund (TETFund)

Ethical Approval and Participant Consent: It is declared that during the preparation process of this study, scientific and ethical principles were followed and all the studies benefited from are stated in the bibliography.

Plagiarism Statement: This article was scanned by the plagiarism program. No plagiarism detected.

Availability of data and materials: Not applicable.

References

[1] A. May, *Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$*, Proceedings of 7*th* International Workshop on Theory and Practice in Public Key Cryptography, (2004), 218-230.
[2] M. Zheng, H. Hu, *Cryptanalysis of prime power RSA with two private exponents*, Sci. China Inf. Sci., **58** (2015), 8 pages.
[3] Y. Lu, R. Zhang, L. Peng, D. Lin, *Solving linear equations modulo unknown divisors: Revisited*, International Conference in the Theory and Application of Cryptology and Information Security, (2015), 189-213.
[4] S. Sarkar, *Small secret exponent attack on RSA variant with modulus $N = p^r q$*, Des. Codes Cryptogr. **73**(2) (2014), 383-392.
[5] S. Sarkar, *Revisiting Prime Power RSA*, Discrete Applied Mathematics, **203** (2016), 127-133.
[6] R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM, **21** (1978), 120-126.
[7] M. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inf. Theory, **36**(3) (1990), 553-558.
[8] S. I. Abubakar, M. R. K. Ariffin, M. A. Asbullah, *A new simultaneous diophantine attack upon RSA moduli $N = pq$*, In Cryptology and Information Security Conference, (2018), 119-131.
[9] M. K. R. Ariffin, S. I. Abubakar, F. Yunos, M. A. Asbullah, *New cryptanalytic attack on RSA modulus $N = pq$ using small prime difference method*, Cryptography, **3**(1) (2019), 2.
[10] T. Takagi, *Fast RSA-type cryptosystem modulo $p^k q$*, Advances in Cryptology-CRYPTO, **1998** (1998), 318-326.
[11] D. Boneh, G. Durfee, N. Howgrave-Graham, *Factoring $N = p^r q$ for large r*, Proceedings of 19*th* Annual International Cryptology Conference, (1990) (1990), 326-337.
[12] A. Takayasu, N. Kunihiro, *Better lattice construction for solving multivariate linear equations modulo unknown divisors*, Proceedings of the 18*th* Australian Conference (ACISP 2013), (2013), 118-135.
[13] A. Nitaj, *Diophantine and lattice cryptanalysis of the RSA cryptosystem*, Artificial Intelligence, Evolutionary Computing and Metaheuristics, (2013), 139-168.
[14] A. K. Lenstra, H. W. Lenstra, L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann., **261** (1982), 513-534.
[15] N. Howgrave-Graham, *Finding small roots of univariate modular equations revisited*, Darnell M. Cryptography and Coding, (1997), 131-142.