Malaysian Journal of Mathematical Sciences 15(S) December: 63–75 (2021)

Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

An Attack on $N = p^2q$ with Partially Known Bits on the Multiple of the Prime Factors

Ruzai, W. N. A.[1], Adenan, N. N. H.[1], Ariffin, M. R. K. *[1], Ghaffar, A. H. A.[2], and Johari, M. A. M.[2]

[1]*Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[2]*Department of Mathematics & Statistics, Faculty of Sciences, Universiti Putra Malaysia, Malaysia*

*E-mail: *rezal@upm.edu.my*
**Corresponding author*

Received: 17 June 2021
Accepted: 7 October 2021

Abstract

This paper presents a cryptanalytic study upon the modulus $N = p^2q$ consisting of two large primes that are in the same-bit size. In this work, we show that the modulus N is factorable if e satisfies the Diophantine equation of the form $ed - k(N - (ap)^2 - apbq + ap) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. Our attack is feasible when some amount of Least Significant Bits (LSBs) of ap and bq is known. By utilising the Jochemsz-May strategy as our main method, we manage to prove that the modulus N can be factored in polynomial time under certain specified conditions.

Keywords: partial-key exposure attack; integer factorization problem; Jochemsz-May strategy; least significant bits.

1 Introduction

In 1978, the world of cryptography was astounded by the invention of the first practical public-key cryptosystem known as RSA [16]. Ever since its existence, RSA is embedded in millions of digital applications with the objectives to provide confidentiality, integrity, authenticity and disallow repudiation. Among essential features of the RSA are the public-key pair (N, e) and private-key tuple $(p, q, d, \phi(N))$. The RSA modulus N is the product of two large balanced primes p and q, while $e \geq 3$ satisfies gcd $(e, \phi(N)) = 1$; $\phi(N)$ is the Euler's totient function and $d \equiv e^{-1} \bmod \phi(N)$. The public parameter e is needed for the encryption process given by $C \equiv M^e \pmod N$ whilst the private parameter d is utilized in the decryption process given by $M \equiv C^d \pmod N$. The security of the RSA relies on the difficulty to solve these hard problems, which are the integer factorization problem, modular e-th root problem and key equation problem. Practically, these problems are considered hard since it should take the best computers available today billions of years to solve. Thus, the RSA is maintained secure until the invention of the so-called practical quantum computer.

The cost incurred for the computational process depends on the size of the parameters e and d as both are utilized in the modular exponentiation process. As an effort to decrease the decryption cost, one might want to choose a small exponent d. Nevertheless, [20] proved that by utilizing a small d, where $d < \frac{1}{3}N^{\frac{1}{4}}$ would result in d being recovered. This was made possible through the continued fractions expansion method. The success achieved by [20] prompted other researchers to investigate this weakness further and increase the unsafe bound of d. For instance, [4] enhanced the bound proposed in [20] up to $d < N^{0.292}$ by utilizing the lattice basis reduction method.

Another potential weakness of the RSA cryptosystem is the partial key exposure, which occurs when one can obtain some relevant bits of the private-key d or its prime factors. [5] presented this type of attack and proved that by having only a quarter of the information is sufficient to reveal the private parameter d. They utilized the method from [7] to achieve their goal. Later, [18] also analyzed this type of weakness and showed that RSA is susceptible if the prime factors share a large number of LSBs such that $|p - q| = 2^m u$ with $2^m = N^\alpha$. They proved that RSA is insecure when $d < N^\delta$ for $\delta < \frac{7}{6} - \frac{2}{3}\alpha - \frac{1}{3}\sqrt{(1 - 4\alpha)(1 - 4\alpha + 6\gamma)}$. In the subsequent years, [15] contributed to this angle of analysis by proposing an attack on partial key exposure. Considering the case from the relation $ed - k(N + 1 - ap - bq) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$, Nitaj's attack worked when certain amount of the LSBs of ap and bq is known.

The researchers made various kinds of attempts to increase the efficiency of key generation and decryption algorithms. The usage of multi-power RSA whereby the modulus $N = pq$ was modified into the form $N = p^r q$ has been proven useful to achieve the goal provided via the Chinese Remainder Theorem [10]. The cryptosystem designed by [19] is the instance that utilised this fact, and the author managed to show that it is indeed less expensive compared to standard RSA.

Hence, the cryptanalytic study upon the multi-power RSA becomes crucial. [6] proved that $N = p^r q$ could be factored when the size of r is approximate to the size of $\log p$. This became a catalyst for the researchers to conduct more attacks upon this type of cryptosystem. For example, [14] proved that $N = p^r q$ is more insecure than $N = pq$. [17] described his proof that by applying lattice reduction techniques, one can factor $N = p^r q$ provided $d < N^{0.395}$. A year later, [13] also proposed an attack on $N = p^r q$, but they only managed to improve bound from [14]. Nonetheless, there are also other attacks such as [2] and [1] that conducted their attacks, particularly on the modulus $N = p^2 q$, and they showed that N could be factored provided certain conditions must be fulfilled.

Our contributrion. In this article we report Nitaj's attack on the modulus $N = p^2 q$ when the amount of sharing bits of LSBs between the value of ap and bq is known. We consider the value of e satisfying the equation $ed - k(N - (ap)^2 - apbq + ap) = 1$. By utilising the method from [11], we show that N is factorable if

$$\delta < \frac{91}{135} + \frac{29}{45}\beta - \frac{44}{45}\alpha - \frac{2}{3}\gamma - \frac{2}{135}\sqrt{2(3\alpha - 3\beta + 1)(-84\alpha + 45\gamma + 39\beta - 28)}.$$

The paper is organized as follows. Section 2 contains the tools and some essential lemmas that are needed to prove our theorem. Section 3 and 4 present the result of our attack and comparison table of our bound with the previous attacks, respectively. Finally, we conclude our work in Section 5.

2 Preliminaries

This section provides several results that will be used in the rest of the paper which also aided us to construct the new attack later.

2.1 Lattice

Let n and k be the element of $\mathbb{Z}^+$ with n is less than or equal to k. Let $y_1, \ldots, y_n$ be a set of vectors that are linearly independent in $\mathbb{R}$. A lattice $\mathcal{C}$ is built by a set of linear combination $y_1, \ldots, y_n$. The general form of the lattice and its determinant is written as follows;

$$\mathcal{C} = \left\{ \sum_{j=1}^{n} x_j y_j | x_j \in \mathbb{Z} \right\}, \qquad \det(\mathcal{C}) = \sqrt{\det(Y^T Y)},$$

where n is the dimension and Y is the matrix of basis vector y_j. If the value of n is equal to k, then the lattice is said to be full ranked lattice. A lattice is a powerful tool in the development of either cryptography and cryptanalysis field. One of the significant applications of the lattice is the LLL algorithm. It was invented in 1982 by [12] purposely to produce a short basis vector in polynomial time. The following theorem shows the bounds for the reduced vectors.

Theorem 2.1. *Let $\mathcal{C}$ be lattice with the dimension of n with a basis vectors $v_1, \ldots, v_n$. The LLL algorithm yields a reduced basis $b_1, \ldots, b_n$ that satisfies this inequalities*

$$b_1 \leq b_2 \leq b_3 \leq \cdots \leq b_n \leq 2^{\frac{n(n-1)}{4(n+1-k)}} \det(\mathcal{C})^{\frac{1}{n+1-k}},$$

for all $1 \leq n \leq k$.

It was noticed by Coppersmith that the algorithm is a fundamental tool to solve lattice problems. Specifically, [7] provided a solution on how to find small roots of a modular polynomial. The author of [7] used the LLL algorithm to find a reduced basis of a polynomial. Later, [9] reformulated Coppersmith's idea and hence described the following theorem.

Theorem 2.2. [9] *Let $h(y_1, \ldots, y_k) \in \mathbb{Z}[y_1, \ldots, y_k]$ be a polynomial with n terms. Let $h(y_1^{(0)}, \ldots, y_j^{(0)}) \equiv 0 \pmod R$ where $\left|y_j^{(0)}\right| < Y_j$ for $j = 1, \ldots, k$ and $h(y_1Y_1, \ldots, y_kY_k) < \frac{R}{\sqrt{\omega}}$. Then $h(y_1^{(0)}, \ldots, y_k^{(0)}) = 0 \in \mathbb{Z}$ is holds.*

Note that our new attack depends on a well-known assumption which was also being applied by some previous attacks such as [4], [13], and [17].

Assumption 1.*The LLL algorithm yields a number of polynomials that are coprime to each other.The roots of these polynomials can be extracted via resultant technique* [8].

2.2 Approximation of the Primes

The following lemma by [3] shows an approximation of the size of primes p and q when the modulus $N = p^2q$.

Lemma 2.1. [3] *Suppose $N = p^2q$ with $q < p < 2q$. Then*

$$2^{-1/3}N^{1/3} < q < N^{1/3} < p < 2^{1/3}N^{1/3}.$$

3 Our New Attack

In this section, the case of the generalized RSA equation $ed - k(N - (ap)^2 - apbq + ap) = 1$ where $\frac{a}{b}$ is the unknown approximation of $\frac{q}{p}$ is considered. Briefly, we utilise the known information of LSBs of the prime factors, insert them into our equation and build an integer multivariate polynomial. Then we use the Jochemsz-May strategy to find the roots of the polynomial and thus factor the modulus N. Our proposed method is formally described as follows.

Theorem 3.1. *Let $N = p^2q$ be the modulus of the RSA. Suppose $ap + bq = N^{1/3+\alpha}$. Let $ap = 2^sp_1 + u_0$ and $bq = 2^sq_1 + v_0$ where s, u_0, v_0 are knowns with $2^s = N^\beta$ and $\frac{a}{b}$ where $a, b < N^\alpha$ is an unknown approximation of $\frac{q}{p}$. Let $e < N^\gamma, d < N^\delta$ and k is an element of $\mathbb{Z}^+$ that satisfy an equation*

$$ed - k(N - (ap)^2 - apbq + ap) = 1.$$

Then, N is factorable if

$$\delta < \frac{91}{135} + \frac{29}{45}\beta - \frac{44}{45}\alpha - \frac{2}{3}\gamma - \frac{2}{135}\sqrt{2(3\alpha - 3\beta + 1)(-84\alpha + 45\gamma + 39\beta - 28)}.$$

Proof. We have variant of RSA key equation where $ed - k(N - (ap)^2 - (ap)(bq) + (ap)) = 1$. First, substitute the value of $ap = 2^s p_1 + u_0$ and $bq = 2^s q_1 + v_0$. Then, by expanding the equation, we obtain

$$ed - k(N - (2^s p_1 + u_0)^2 - (2^s p_1 + u_0)(2^s q_1 + v_0) + (2^s p_1 + u_0)) = 1,$$
$$ed - k(N - 2^{2s} p_1^2 - 2^{s+1} u_0 p_1 - u_0^2 - 2^{2s} p_1 q_1 - 2^s v_0 p_1 - 2^s u_0 q_1 - u_0 v_0 + 2^s p_1 + u_0) = 1.$$

Rearrange the equation, we would have

$$ed - (N - u_0^2 - u_0 v_0 + u_0)k + 2^s(2^s p_1^2 - p_1 + 2^s p_1 q_1)k + 2^s(2u_0 + v_0)kp_1 + 2^s u_0 q_1 k - 1 = 0.$$

We finally transform the above equation into polynomial $f(x_1, x_2, x_3, x_4, x_5)$

$$a_1 x_1 + a_2 x_2 + a_3 x_2 x_3 + a_4 x_2 x_4 + a_5 x_2 x_5 + a_6 = 0,$$

where

$$\begin{cases} a_1 &= e, \\ a_2 &= -(N - u_0^2 - u_0 v_0 + u_0), \\ a_3 &= 2^s, \\ a_4 &= 2^s(2u_0 + v_0), \\ a_5 &= 2^s u_0, \\ a_6 &= -1, \end{cases} \quad \text{and} \quad \begin{cases} x_1 &= d, \\ x_2 &= k, \\ x_3 &= 2^s p_1^2 - p_1 + 2^s p_1 q_1, \\ x_4 &= p_1, \\ x_5 &= q_1. \end{cases}$$

We set the bounds for the unknowns

i) $d < X_1 = N^{\delta}$,

ii) $k = \frac{ed-1}{N} < X_2 = N^{\gamma+\delta-1}$,

iii) $2^s p_1^2 - p_1 + 2^s p_1 q_1 < 2^s p_1^2 + 2^s p_1 q_1$

$$= 2^s p_1(p_1 + q_1)$$

$$= \frac{2^s(ap)}{2^s}\left(\frac{ap+bq}{2^s}\right)$$

$$< X_3 = N^{\frac{2}{3}+2\alpha-\beta},$$

iv) $p_1 = \frac{ap}{2^s} < X_4 = N^{\frac{1}{3}+\alpha-\beta}$,

v) $q_1 = \frac{bq}{2^s} < X_5 = N^{\frac{1}{3}+\alpha-\beta}$.

We apply the Jochemsz-May strategy to solve for the roots of the polynomial. Firstly, let $m, t \in \mathbb{Z}^+$. Define the set

$$S = \bigcup_{0 \leq j \leq t} \{x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} | x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \text{ monomial of } f^{m-1}\},$$

and the set

$$M = \{\text{monomials of } x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} f \mid x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in S\}.$$

Now we want to find the expansion of $f^{m-1}(x_1, x_2, x_3, x_4, x_5)$. By using binomial expansion, we obtain the following summation. Note that, we neglect the coefficients in order to avoid redundancy. Thus, we have

$$\sum_{i_1=0}^{m-1} \sum_{i_2=0}^{m-1-i_1} \sum_{i_3=0}^{i_2} \sum_{i_4=0}^{i_2-i_3} \sum_{i_5=0}^{i_2-i_3-i_4} x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5}. \tag{1}$$

For simplicity, the monomials of expression in (1) can be categorised as follows:

$$x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in S \text{ if } \begin{cases} i_1 = 0, \ldots, m-1, \\ i_2 = 0, \ldots, m-1-i_1, \\ i_3 = 0, \ldots, i_2, \\ i_4 = 0, \ldots, i_2 - i_3, \\ i_5 = 0, \ldots, i_2 - i_3 - i_4 + t. \end{cases}$$

$$x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in M \text{ if } \begin{cases} i_1 = 0, \ldots, m, \\ i_2 = 0, \ldots, m - i_1, \\ i_3 = 0, \ldots, i_2, \\ i_4 = 0, \ldots, i_2 - i_3, \\ i_5 = 0, \ldots, i_2 - i_3 - i_4 + t. \end{cases}$$

Define $W = ||f(x_1X_1, x_2X_2, x_3X_3, x_4X_4x_5X_5||_\infty$. Thus, we choose

$$W \geq |a_1|X_1 = ed \approx N^{\gamma+\delta}, \tag{2}$$

since the term $|a_1|X_1$ is the maximum value of our polynomial f. Next, define

$$R = WX_1^{m-1}X_2^{m-1}X_3^{m-1}X_4^{m-1}X_5^{m-1+t}.$$

Suppose that a_6 and R do not share any common factors. Thus, we define

$$f'(x_1, x_2, x_3, x_4, x_5) = a_6^{-1} f(x_1, x_2, x_3, x_4, x_5) \pmod{R}.$$

This is important as we want to work with a polynomial that has a constant term one. Next, define the polynomials

$$\begin{aligned} g &= x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} f' X_1^{m-1-i_1} X_2^{m-1-i_2} X_3^{m-1-i_3} X_4^{m-1-i_4} X_5^{m-1+t-i_5}, \\ &\quad \text{with } x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in S, \\ h &= x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} R, \\ &\quad \text{with } x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in M \backslash S. \end{aligned}$$

The coefficients of g and h is used to construct a basis of a lattice $\mathcal{C}$ with dimension

$$\begin{aligned} \sigma = \sum_{x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in M} 1 &= \sum_{i_1=0}^{m} \sum_{i_2=0}^{m-i_1} \sum_{i_3=0}^{i_2} \sum_{i_4=0}^{i_2-i_3} \sum_{i_5=0}^{i_2-i_3-i_4} 1, \\ &= \frac{1}{120}(m+1)(m+2)(m+3)(m+4)(m+5t+5). \end{aligned}$$

In order to build a right triangular matrix M (see Table 1), we construct the following monomials ordering: if $\sum i_j < \sum i'_j$ then $x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} < x_1^{i'_1} x_2^{i'_2} x_3^{i'_3} x_4^{i'_4} x_5^{i'_5}$ and the monomials are alphabetically ordered if $\sum i_j = \sum i'_j$.

The following form described the diagonal entries of the lattice.

$$\begin{cases} (X_1X_2X_3X_4)^{m-1} X_5^{m-1+t} & \text{for the polynomials } g, \\ W X_1^{m-1+i_1} X_2^{m-1+i_2} X_3^{m-1+i_3} X_4^{m-1+i_4} X_5^{m-1+t+i_5} & \text{for the polynomials } h. \end{cases}$$

Table 1: The coefficient lattice for $m = 2$ and $t = 0$.

$$M = \left[\begin{array}{cccccccccccccccccccccc}
 & 1 & x_2 & x_2x_5 & x_2x_4 & x_2x_3 & x_2^2 & x_2^2x_5 & x_2^2x_5^2 & x_2^2x_4 & x_2^2x_4x_5 & x_2^2x_4^2 & x_2^2x_3 & x_2^2x_3x_5 & x_2^2x_3x_4 & x_2^2x_3^2 & x_1 & x_1x_2 & x_1x_2x_5 & x_1x_2x_4 & x_1x_2x_3 & x_1^2 \\
g_{0,0,0,0,0} & \text{A} & ** & ** & ** & ** & & & & & & & & & & & ** & & & & & \\
g_{0,1,0,0,0} & & \text{A} & & & & ** & ** & & ** & & & ** & & & & & ** & & & & \\
g_{0,1,0,0,1} & & & \text{A} & & & & ** & ** & & ** & & & ** & & & & & ** & & & \\
g_{0,1,0,1,0} & & & & \text{A} & & & & & ** & ** & ** & & & ** & & & & & ** & & \\
h_{0,1,1,0,0} & & & & & \text{A} & & & & & & & ** & ** & ** & ** & & & & & ** & \\
h_{0,2,0,0,0} & & & & & & \text{B} & & & & & & & & & & & & & & & \\
h_{0,2,0,0,1} & & & & & & & \text{B} & & & & & & & & & & & & & & \\
h_{0,2,0,0,2} & & & & & & & & \text{B} & & & & & & & & & & & & & \\
h_{0,2,0,1,0} & & & & & & & & & \text{B} & & & & & & & & & & & & \\
h_{0,2,0,1,1} & & & & & & & & & & \text{B} & & & & & & & & & & & \\
g_{0,2,0,2,0} & & & & & & & & & & & \text{B} & & & & & & & & & & \\
g_{0,2,1,0,0} & & & & & & & & & & & & \text{B} & & & & & & & & & \\
h_{0,2,1,0,1} & & & & & & & & & & & & & \text{B} & & & & & & & & \\
h_{0,2,1,1,0} & & & & & & & & & & & & & & \text{B} & & & & & & & \\
h_{0,2,2,0,0} & & & & & & & & & & & & & & & \text{B} & & & & & & \\
h_{1,0,0,0,0} & & & & & & & & & & & & & & & & \text{A} & ** & ** & ** & ** & ** \\
h_{1,1,0,0,0} & & & & & & & & & & & & & & & & & \text{B} & & & & \\
h_{1,1,0,0,1} & & & & & & & & & & & & & & & & & & \text{B} & & & \\
h_{1,1,0,1,0} & & & & & & & & & & & & & & & & & & & \text{B} & & \\
h_{1,1,1,0,0} & & & & & & & & & & & & & & & & & & & & \text{B} & \\
h_{2,0,0,0,0} & & & & & & & & & & & & & & & & & & & & & \text{B}
\end{array}\right]$$

As observed from Table 1, note that the symbol $**$ implies that the entry has value and the letters A and B signify the following:

$A = X_1 X_2 X_3 X_4 X_5,$
$B = X_1^{i_1} X_2^{i_2} X_3^{i_3} X_4^{i_4} X_5^{i_5} R.$

Next, we define

$$s_j = \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in M} i_j - \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in S} i_j, \tag{3}$$

for $j = 1, 2, 3, 4, 5$.

Taking the product of the diagonal of the lattice, we obtain the determinant of $\mathcal{C}$,

$$\begin{aligned}\det(\mathcal{C}) &= W^{|M\setminus S|} X_5^{(m-1+t)|S|+(m-1+t)|M\setminus S|+s_5} \prod_{j=1}^{4} X_j^{(m-1)|S|+(m-1)|M\setminus S|+s_j},\\ &= W^{|M\setminus S|} X_5^{(m-1+t)\sigma+s_5} \prod_{j=1}^{4} X_j^{(m-1)\sigma+s_j}.\end{aligned}$$

We obtain four new bases containing short vectors which are $f_i(x_1X_1, x_2X_2, x_3X_3, x_4X_4, x_5X_5)$, for $i = 1, \ldots, 4$ after applying the LLL algorithm to the lattice $\mathcal{C}$. Each f_i is a combination of g and h, and then share the roots $(d, k, 2^s p_1^2 - p_1 + 2^s p_1 q_1, p_1, q_1)$. Then by Theorem 2.1, we have for $i = 1, \ldots, 4$,

$$||f_i(x_1X_1, x_2X_2, x_3X_3, x_4X_4, x_5X_5)|| < 2^{\frac{\sigma(\sigma-1)}{4(\sigma-3)}} \det(\mathcal{C})^{\frac{1}{\sigma-3}}.$$

For $i = 1, \ldots, 4$, the polynomials f_i must fulfill the bound from Theorem 2.2 which is

$$||f_i(x_1X_1, x_2X_2, x_3X_3, x_4X_4, x_5X_5)|| < \frac{R}{\sqrt{\sigma}}.$$

An adequate condition is

$$2^{\frac{\sigma(\sigma-1)}{4(\sigma-3)}} \det(\mathcal{C})^{\frac{1}{\sigma-3}} < \frac{R}{\sqrt{\sigma}},$$

which can be transformed into $\det(\mathcal{C}) < R^{\sigma}$, that is

$$\begin{aligned} W^{|M\setminus S|} X_5^{(m-1+t)\sigma+s_5} \prod_{j=1}^{4} X_j^{(m-1)\sigma+s_j} &< (W X_1^{m-1} X_2^{m-1} X_3^{m-1} X_4^{m-1} X_5^{m-1+t})^{\sigma},\\ \frac{X_5^{(m-1+t)\sigma+s_5} \prod_{j=1}^{4} X_j^{(m-1)\sigma+s_j}}{(X_1^{m-1} X_2^{m-1} X_3^{m-1} X_4^{m-1} X_5^{m-1+t})} &< \frac{W^{\sigma}}{W^{|M\setminus S|}},\\ X_5^{s_5} \prod_{j=1}^{4} X_j^{s_j} &< W^{\sigma-|M\setminus S|}.\end{aligned}$$

Using $\sigma = |M|$ and $|M| - |M\backslash S| = |S|$, we have

$$\prod_{j=1}^{5} X_j^{s_j} < W^{|S|}. \tag{4}$$

Using (3), we easily obtain

$$\begin{aligned}
s_1 &= \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in M} i_1 - \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in S} i_1\\
&= \frac{1}{120}m(m+1)(m+2)(m+3)(m+5t+4),\\
s_2 &= \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in M} i_2 - \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in S} i_2\\
&= \frac{1}{120}m(m+1)(m+2)(m+3)(4m+15t+16),\\
s_3 &= \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in M} i_3 - \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in S} i_3\\
&= \frac{1}{120}m(m+1)(m+2)(m+3)(m+5t+4),\\
s_4 &= \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in M} i_4 - \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in S} i_4\\
&= \frac{1}{120}m(m+1)(m+2)(m+3)(m+5t+4),\\
s_5 &= \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in M} i_5 - \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in S} i_5\\
&= \frac{1}{120}(m+1)(m+2)(m+3)(m^2+5mt+10t^2+4m+10t).
\end{aligned}$$

Similarly, we have

$$|S| = \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}\in S} 1 = \frac{1}{120}m(m+1)(m+2)(m+3)(m+5t+4).$$

Set $t = \tau m$, then,

$$\begin{aligned}
s_1 &= \frac{1}{120}(5\tau+1)m^5 + o(m^5),\\
s_2 &= \frac{1}{120}(15\tau+4)m^5 + o(m^5),\\
s_3 &= \frac{1}{120}(5\tau+1)m^5 + o(m^5),\\
s_4 &= \frac{1}{120}(5\tau+1)m^5 + o(m^5),\\
s_5 &= \frac{1}{120}(10\tau^2+5\tau+1)m^5 + o(m^5),\\
|S| &= \frac{1}{120}(5\tau+1)m^5 + o(m^5).
\end{aligned} \tag{5}$$

Using (5), and after simplifying by m^5, we can transform (4) into

$$X_1^{\frac{1}{120}(5\tau+1)}X_2^{\frac{1}{120}(15\tau+4)}X_3^{\frac{1}{120}(5\tau+1)}X_4^{\frac{1}{120}(5\tau+1)}X_5^{\frac{1}{120}(10\tau^2+5\tau+1)} < W^{\frac{1}{120}(5\tau+1)}.$$

Replacing the values of X_1, X_2, X_3, X_4, X_5 and W from (3) and (2) we get

$$\frac{1}{120}(\delta)(5\tau+1) + \frac{1}{120}(\gamma+\delta-1)(15\tau+4) + \frac{1}{120}\left(\frac{1}{3}+\alpha-\beta\right)(10\tau^2+5\tau+1)$$
$$+\frac{1}{120}\left(\frac{1}{3}+\alpha-\beta\right)(5\tau+1) + \frac{1}{120}\left(\frac{2}{3}+2\alpha-2\beta\right)(5\tau+1) < \frac{1}{120}(\gamma+\delta)(5\tau+1),$$

or equivalently,

$$(30\alpha-30\beta+10)\tau^2 + (60\alpha-45\beta+45\delta+30\gamma-25)\tau + 12\alpha-9\beta+12\delta+9\gamma-8 < 0. \tag{6}$$

Differentiate (6) with respect to τ, we obtain the optimal value $\tau = \frac{9\beta-9\delta-12\alpha-6\gamma+5}{4(3\alpha-3\beta+1)}$, this reduces to

$$135\delta^2 + (180\gamma+264\alpha-174\beta-182)\delta + 144\alpha^2 - 168\alpha + 168\alpha\gamma$$
$$-192\alpha\beta + 63\beta^2 - 108\beta\gamma + 110\beta + 60\gamma^2 - 124\gamma + 63 < 0,$$

which is valid if

$$\delta < \frac{91}{135} + \frac{29}{45}\beta - \frac{44}{45}\alpha - \frac{2}{3}\gamma - \frac{2}{135}\sqrt{2(3\alpha-3\beta+1)(-84\alpha+45\gamma+39\beta-28)}. \tag{7}$$

Abiding the condition in (7), we find our reduced polynomial f, f_1, f_2, f_3, f_4 that contain the desired roots of $(d, k, 2^m p_1^2 - p_1 + 2^m p_1 q_1, p_1, q_1)$ which is achievable by applying the LLL algorithm to our lattice. Then, by Assumption 1, we can extract the roots from the polynomials by using the resultant technique. We compute $ap = 2^m p_1 + u_0$ using the third root p_1. Then, by taking the $\gcd(N, ap) = p$ will lead to the factorization of N. □

4 Comparison with the Previous Attack

In this section, we present the comparison of bounds between ours and another three attacks proposed by [14], [17], and [13]. Particularly, all the three attacks analysed the prime-power RSA modulus $N = p^r q$. However, we only examine the case for $r = 2$. All the previous attacks utilised the key equation $ed - k\phi(N) = 1$ where $\phi(N) = p^{r-1}(p^r - 1)(q-1)$.

Note that in these previous attacks, they did not consider the case of sharing bits and their bounds relied only on the degree of p which is r. Thus, we neutralized our bound and produce the following corollary. By using various values of $\gamma = \log_N(e)$, we then compare the results. Our corollary is described as follows.

Corollary 4.1. *Let the modulus of the RSA is $N = p^2 q$ with the condition $p = 2^s p_1 + u_0$ and $q = 2^s q_1 + v_0$ where s, u_0, v_0 are knowns with $2^s = N^\beta$. Let $e \approx N^\gamma, d \approx N^\delta$ and k is an element in $\mathbb{Z}^+$ satisfies $ed - k(N - p^2 - pq + p) = 1$. Then N can be factored if*

$$\delta < \frac{91}{135} + \frac{29}{45}\beta - \frac{2}{3}\gamma - \frac{2}{135}\sqrt{2(1-3\beta)(45\gamma+39\beta-28)}.$$

Table 2: Comparison of the new method with the method of [13], [14], [17] for $\beta = 0.1$.

$\gamma = \log_N(e)$ Bound of δ	$\gamma = 0.66$	$\gamma = 0.60$	$\gamma = 0.55$	$\gamma = 0.54$
Lu et al. [13]	0.22	0.22	0.22	0.22
May [14]	0.22	0.22	0.22	0.22
Sarkar [17]	0.39	0.39	0.39	0.39
Our bound in Corollary 1	0.25	0.30	0.35	0.37

Remark 4.1. *Now, we will look at the bound for γ that is applicable for our attack. We can observe that from Corollary 4.1, if we set the value of $\beta = 0.1$, then we get*

$$\delta < \frac{997}{1350} - \frac{2}{3}\gamma - \frac{2}{135}\sqrt{63\gamma - \frac{1687}{50}}. \tag{8}$$

Suppose that $e = N^{\gamma}$. From the standard RSA key equation, we have

$$ed = 1 + k\phi(N) > \phi(N) \approx N.$$

Thus,

$$d > \frac{N}{e} = N^{1-\gamma}. \tag{9}$$

When considering the exponent of N from (9), thus the condition in (8) becomes

$$1 - \gamma \quad < \tfrac{997}{1350} - \tfrac{2}{3}\gamma - \tfrac{2}{135}\sqrt{63\gamma - \tfrac{1687}{50}}).$$

A direct calculation would give us $\gamma < \frac{33}{50} \approx 0.66$ which indicates that our attack is applicable for smaller value of γ.

Remark 4.2. *Note that for this attack, the increment of our bound could only improve the bounds from [13] and [14]. From Table 2, it can be seen that for N is 1024-bit, we need to know $s \approx 103$-bit in order to factor the modulus provided the bound of d must fall under the unsafe bound as stated in Table 2.*

5 Conclusion

This paper proposed an attack on the prime-power RSA modulus $N = p^2q$ by considering the equation $ed - k(N - (ap)^2 - apbq + ap) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. If the LSBs value of ap and bq are known, then N can be factored. Through our attack, we managed to improve the bounds of some former attacks. All in all, one needs to be cautious in choosing the primes and decryption exponent d so that they do not satisfy the conditions that can lead to the vulnerability of the cryptosystem.

Acknowledgement We thank the reviewers for the constructive comments and editor for the guidance.

Conflicts of Interest The authors declare no conflict of interest.

References

[1] N. N. H. Adenan, M. R. K. Ariffin & M. A. Asbullah (2021). New Jochemsz-May cryptanalytic bound for RSA system utilizing common modulus $N = p^2q$. *Mathematics*, *9*(4), 340. https://doi.org/10.3390/math9040340.

[2] M. R. K. Ariffin, M. A. Asbullah, N. A. Abu & Z. Mahad (2013). A new efficient asymmetric cryptosystem based on the integer factorization problem of $N = p^2q$. *Malaysian Journal of Mathematical Sciences*, *7*(S), 19–37.

[3] M. A. Asbullah & M. R. K. Ariffin (2015). New attacks on RSA with modulus $N = p^2q$ using continued fractions. *Journal of Physics*, *622*(1), 191–199.

[4] D. Boneh & G. Durfee (1999). Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology EUROCRYPT99*, pp. 1–11. Springer, Berlin, Heidelberg.

[5] D. Boneh, G. Durfee & Y. Frankel (1998). An attack on RSA given a small fraction of the private key bits. In *Advances in Cryptology ASIACRYPT98*, pp. 25–34. Springer, Berlin, Heidelberg.

[6] D. Boneh, G. Durfee & N. Howgrave-Graham (1999). Factoring $N = p^rq$ for large r. In *Advances in Cryptology CRYPTO99*, pp. 326–337. Springer, Berlin, Heidelberg.

[7] D. Coppersmith (1997). Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, *10*, 233–260.

[8] I. M. Gelfand, M. M. Kapranov & A. V. Zelevinsky (1994). *Discriminants, Resultants, and Multidimensional Determinants*. Springer, New York, NY.

[9] N. H. Graham (1997). Finding small roots of univariate modular equations revisited. In *Crytography and Coding*, pp. 131–142. Springer, Berlin, Heidelberg.

[10] M. J. Hinek (2010). *Cryptanalysis of RSA and Its Variants*. CRC Press, New York.

[11] E. Jochemsz & A. May (2006). A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In *Advances in Cryptology ASIACRYPT 2006*, pp. 267–282. Springer, Berlin, Heidelberg.

[12] A. K. Lenstra, H. W. Lenstra & H. W. Lovasz (1982). Factoring polynomials with rational coeffcients. *Mathematische Annalen*, *261*(4), 515–534.

[13] Y. Lu, R. Zhang, L. Peng & D. Lin (2015). Solving linear equations modulo unknown divisors: revisited. In *Advances in Cryptology ASIACRYPT 2015*, pp. 189–213. Springer, Berlin, Heidelberg.

[14] A. May (2004). A secret exponent attacks on RSA-type schemes with moduli $N = p^r q$. In *Public Key Cryptography PKC 2004*, pp. 218–230. Springer, Berlin, Heidelberg.

[15] A. Nitaj (2013). An attack on RSA using LSBs of multiples of the prime factors. In *Progress in Cryptology AFRICACRYPT 2013*, pp. 297–310. Springer, Berlin, Heidelberg.

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

[17] S. Sarkar (2014). Small secret exponent attack on RSA variant with modulus $N = p^r q$. *Designs, Codes, and Cryptography*, *73*(2), 383–392.

[18] H. M. Sun, M. E. Wu, R. Steinfeld, J. Guo & H. Wang (2008). Cryptanalysis of short exponent RSA with primes sharing least significant bits. In *Cryptology and Network Security*, pp. 49–63. Springer, Berlin, Heidelberg.

[19] T. Takagi (1998). Fast RSA-type cryptosystem modulo $p^k q$. In *Advances in Cryptology CRYPTO98*, pp. 318–326. Springer, Berlin, Heidelberg.

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