New Jochemsz–May Cryptanalytic Bound for RSA System Utilizing Common Modulus $N = p^2q$

Nurul Nur Hanisah Adenan†‡, Muhammad Rezal Kamel Ariffin *†‡, Siti Hasana Sapar †‡, Amir Hamzah Abd Ghafar †‡ and Muhammad Asyraf Asbullah †‡

Institute for Mathematical Research, Universiti Putra Malaysia, Serdang 43400, Selangor, Malaysian; hanisahadenan@gmail.com (N.N.H.A.); silithas@upm.edu.my (S.H.S.); amir_hamzah@upm.edu.my (A.H.A.G.); ma_asyraf@upm.edu.my (M.A.A.)

* Correspondence: rezal@upm.edu.my
† These authors contributed equally to this work.
‡ These authors contributed equally to this work.

Abstract: This paper describes an attack on the Rivest, Shamir and Adleman (RSA) cryptosystem utilizing the modulus $N = p^2q$ where $p$ and $q$ are two large balanced primes. Let $e_1, e_2 < N$ be the integers such that $d_1, d_2 < N^2$ be their multiplicative inverses. Based on the two key equations $e_1d_1 - k_1\phi(N) = 1$ and $e_2d_2 - k_2\phi(N) = 1$ where $\phi(N) = p(p)(q-1)$, our attack works when the primes share a known amount of least significant bits (LSBs) and the private exponents share an amount of most significant bits (MSBs). We apply the extended strategy of Jochemsz–May to find the small roots of an integer polynomial and show that $N$ can be factored if $\delta < \frac{11}{16} + \frac{9}{8} \delta - \frac{1}{2}\gamma - \frac{1}{3} \sqrt{180\gamma + 990\alpha - 180\beta} + 64$. Our attack improves the bounds of some previously proposed attacks that makes the RSA variant vulnerable.

Keywords: factoring; least significant bits (LSBs); most significant bits (MSBs); multiplicative inverse; Jochemsz–May extended strategy

1. Introduction

In 1978, security in transmitting data between two parties is imperative to avert the information from being expose to an unauthorised person. Rivest, Shamir and Adleman came out with a brilliant public key cryptosystem design. It is also known as an asymmetric cryptosystem as it uses different keys for encrypting and decrypting the data. The cryptosystem is called RSA [1]. For encryption, the public parameters $N$ and $e$ are needed where $N = pq$ and $e$ is an integer that is relatively prime with $\phi(N)$ where $\phi(N) = p(p)(q-1)$ is the Euler totient function. The private key $d$ is an integer satisfying $ed \equiv 1 \pmod {\phi(N)}$ is used for the decryption process. The security of the RSA cryptosystem relies on three hard problems which are the integer factorization problem of $N = pq$, solving the $e^{th}$ root problem of $C \equiv M^e \pmod N$ and solving the diophantine key equation given by $ed - k\phi(N) = 1$.

The efficiency of the RSA algorithm depends on the cost and execution time for encryption and decryption processes. In order to reduce the cost and to accelerate the decryption process, one thus tends to use small decryption exponents. However in 1990, Wiener [2] found out that the RSA cryptosystem is vulnerable when the decryption exponent $d$ is too small. Wiener proved that by using continued fractions, one can factor out $N$ if the $d < \frac{1}{4}N^{\frac{1}{4}}$. Since then, researchers worked on the same purpose in order to improve the bound of $d$. There are different approaches in their analysis. For instance, Boneh and Durfee [3] obtained a better bound of $d < N^{0.292}$ by using Coppersmith’s method [4] to find small solutions of modular polynomial equations.

Multi-Power RSA is one of the variants of RSA whereby the modulus $N = p^2q$ for $r \geq 2$ is utilized. This type of modulus provides advantage for both key generation and the decryption algorithms provided the Chinese Remainder Theorem is utilized [5].
Among cryptosystems that utilize this fact are designs by Takagi [6], Ariffin et al. [7] and Asbullah et al. [8]. Through their papers, the designers managed to show that their cryptosystems had low computing costs compared to the standard RSA. As such, the study of the Integer Factorization Problem of \( N = p'q \) becomes important. Boneh et al. [9] proved that \( N = p'q \) is factorable for large \( r \), when \( r \geq \log p \). Since then, many attackers made an attempt to cryptanalyse the multi-power RSA modulus. We only stated the results from these three former attacks which are May [10], Sarkar [11], and Lu et al. [12] because we aim to improve their unsafe bound of their decryption exponent. The following table presents the bounds from these former attacks and the method that they have been used. Note that these former attacks focused on the modulus \( N = p'q \) but we only consider the bound for \( r = 2 \) for comparison purpose.

Another flaw of the RSA cryptosystem is when the information of MSB(s) or LSB(s) of the private key \( d \) or secret primes are leaked to a third party which could lead to recovery of the entire private key and thus break the cryptosystem. This type of attack is called partial key exposure attacks. Boneh, Durfee and Frankel [13] in 1998 showed that only by knowing a quarter of the private key \( d \), it is adequate for them to recover the whole value of \( d \) by using Coppersmith’s technique. Sun et al. [14] and Zhao et al. [15] also showed that using primes that share either most or least significant bits are insecure and the modulus can be factored in polynomial time. Following through in 2014, Nitaj et al. [16] came out with an idea to attack the modulus \( N = pq \) where the primes share their LSBs and there exists two public parameters \( e_1 \) and \( e_2 \) such that the corresponding decryption parameters \( d_1 \) and \( d_2 \) share their MSBs. They showed that if the RSA cryptosystem satisfies those conditions, then it is possible to factor \( N \) provided \( d_1, d_2 < N^\delta \) where \( \delta < \frac{3}{8} - 2\alpha - \beta - \frac{1}{2} \sqrt{6(1-4\alpha)(5+4\gamma-4\alpha-4\beta)} \). Thus, implementors need to ensure that their private key does not fall below than the bound that can be factorised by the third party.

**Our contribution:**

Extending the result from [16], this paper presents an attack on the modulus \( N = p^2q \) when the primes share a known amount of the LSBs while \( d_1 \) and \( d_2 \) share an amount of their MSBs. We formulate a lemma by utilizing the information on the sharing LSBs between the primes. Then, we use the result from the lemma to build an integer multivariate polynomial. We apply the strategy of Jochemsz and May to find the small roots of our integer multivariate polynomial which leads to the factorization of the modulus \( N \). We are able to increase the unsafe bound for the decryption exponent given by \( d_1, d_2 < N^{\delta} \) where

\[
\delta < \frac{11}{10} + \frac{9}{4} - \alpha - \frac{1}{2} + \frac{1}{2} \beta - \gamma - \frac{1}{30} \sqrt{180\gamma + 990\alpha - 180\beta} + 64.
\]

That is, we prove that if \( d_1, d_2 < N^\delta \), then \( N \) can be factored. As such, we improved the bounds made by the previous attacks as shown in Table 1.

**Table 1.** Bounds for \( d \) from the former attacks.

| Former Attack | Bound | Method              |
|---------------|-------|---------------------|
| [12]          | \( d < N^{\frac{\log(\delta^{-1})}{r+1}^2} \) | New proposed algorithm |
| [10]          | \( d < N^\max \frac{r}{(r+1)^2} \) | Coppersmith’s Method   |
| [11]          | \( d < N^{0.39} \) | Lattice reduction    |

The outline of this paper is structured as follows. In Section 2, we describe some fundamental concepts and a few mechanisms that are needed in proving our theorem. Next, in Section 3, we give details on our approach. We finally conclude in Section 4.
2. Materials and Methods

We start this section by introducing in brief on lattice, a theorem on lattice reduced basis, and two useful lemmas on approximation of size of primes in modulus. Then we provide our main lemma of primes sharing bits that has been reformulated from [16]. All of these definitions, theorem and lemmas will be used throughout this paper.

2.1. Lattices

Let \( b_1, ..., b_\omega \in \mathbb{R}^n \) be a set vectors that are linearly independent with \( \omega \leq n \). The lattice \( \mathcal{L} \) constructed by \( b_1, ..., b_\omega \) is the set of linear combinations of \( b_1, ..., b_n \) with dimension \( n \) provided the coefficients are positive integers such that

\[
\mathcal{L} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n; \quad a_1, a_2, \ldots, a_\omega \in \mathbb{Z}
\]

The dimension of this lattice is \( \dim(\mathcal{L}) = \omega \). The lattice is called full ranked lattice if \( \omega = n \). To find the determinant of this type of lattice, one may compute the absolute value of the determinant of the matrix whose rows consist of \( \{v_1, ..., v_\omega\} \). Lenstra, Lenstra, and Lovasz in 1982 [17] invented the LLL algorithm to find a short basis vector in time polynomial. Their theorem is stated as follows.

**Theorem 1.** Let the lattice \( \mathcal{L} \) with \( \dim(\mathcal{L}) = \omega \) be constructed by a basis \( v_1, ..., v_\omega \). The LLL algorithm outputs a reduced basis \( b_1, ..., b_\omega \),

\[
||b_1|| \leq ||b_2|| \leq \cdots \leq ||b_i|| \leq 2^{\frac{\omega(\omega-1)}{2}} \det(\mathcal{L})^{-\frac{1}{\omega-1}}
\]

for all \( 1 \leq i \leq \omega \).

In practice, the LLL algorithm has been broadly known to often produces the vectors that have much smaller norms than theoretically predicted. Hence, by utilizing this algorithm, Coppersmith in 1997 introduced a technique to find small roots for polynomial that is modular form. By applying the LLL algorithm, a number of linear equations with sufficiently small norms will be produced. Later, Howgrave-Graham [18] reformulated Coppersmith’s idea of finding the roots of modular polynomial and thus came out with the theorem as follows.

**Theorem 2.** Let \( f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n] \) be a polynomial with \( \omega \) monomials. Suppose that \( f(x_1^{(0)}, \ldots, x_n^{(0)}) \equiv 0 \pmod{R} \) where \( |x_i^{(0)}| < X_i \) for \( i = 1, ..., n \), and \( h(x_1X_1, \ldots, x_nX_n) < \frac{R}{\sqrt{\omega}} \). Then \( h(x_1^{(0)}, \ldots, x_n^{(0)}) = 0 \) holds over integers.

Remark that our attack relies on Assumption 1 which was also being used in the previous proposed attacks such as [11–13].

**Assumption 1.** The construction of LLL algorithm produces a few polynomials that are algebraically independent. The resultant technique can be used in order to compute the common roots of these polynomials.

Applying Coppersmith’s method, Jochemsz and May [19] introduced a strategy purposely to solve for the small roots of a polynomial. Interestingly, their strategy can be used on either modular or integer of multivariate polynomial. It was also easier to understand and implement. Thus, in our work, we used their strategy in order to find the roots of our polynomial.

2.2. Approximation of Size of Primes in Modulus

Asbullah and Ariffin [20] produced the following lemmas to show an approximation of \( N - \phi(N) \). Lemma 1 describes the size of \( p \) and \( q \) for the modulus \( N = p^2q \) which
then was utilized in Lemma 2 to approximate the size of $N - \phi(N)$. In our work, we use Lemma 2 to approximate the bound for one of the variables in our polynomial.

**Lemma 1.** Suppose $N = p^2q$ where $p$ and $q$ are balanced primes. Then

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

**Lemma 2.** Suppose $N = p^2q$ where $p$ and $q$ are balanced primes. Then

$$2N^{2/3} - N^{1/3} < N - \phi(N) < \left(2^{2/3} + 2^{-1/3}\right)N^{2/3} - 2^{1/3}N^{1/3}$$

2.3. Prime Sharing LSBs on the Modulus $N = pq$

We present the lemma by [16]. The authors study the case where the modulus $N = pq$ consists of the primes that share some known amount of LSBs.

**Lemma 3.** Let $N = pq$ be an RSA modulus where $p, q$ are balanced primes. Let $p - q = 2^b u$ for a known value of $b$. Then $p = 2^b p_1 + u_0$ and $q = 2^b q_1 + u_0$ where $u_0$ is the solution of the equation $x^2 \equiv N \pmod{2^b}$ and $p + q = 2^{2b} v + v_0$ with

$$v_0 \equiv 2u_0 + (N - u_0^2)u_0^{-1} \pmod{2^{2b}}.$$  

**Proof.** See [16].

2.4. Prime Sharing LSBs on the Modulus $N = p^2q$

This section presents the lemma that has been reformulated from the result [16]. It considers the case where the primes of the modulus $N = p^2q$ share some known amount of their LSBs.

**Lemma 4.** Let $N = p^2q$ be modulus and suppose that $p - q = 2^m u$ for a known value of $m$. Let $p = 2^m p_1 + u_0$ and $q = 2^m q_1 + u_0$ where $u_0$ is a solution to $p^3 \equiv N \pmod{2^m}$. If $s_0 \equiv u_0^{-1}(N - u_0^2) \pmod{2^{3m}}$ then $p^2 + pq - p = 2^{3m} s_0 - v$ where

$$v = 2^m p_1 + 2^m p_1 q_1 - 2^m p_1 u_0 - 2u_0^2 + u_0.$$  

**Proof.** See Appendix A.

3. Our New Attack

In this section, we present the theorem of an attack on modulus $N = p^2q$ which applies when the primes share a known amount of LSBs and there exists $d_1$ and $d_2$ that share an amount of MSBs.

**Theorem 3.** Let $N = p^2q$ be modulus such that $p - q = 2^m u$ where $2^m \approx N^\alpha$. Let $e_1, e_2 \approx N^\gamma$ be two public exponents that satisfy $e_1 d_1 - k_1 \phi(N) = 1$, and $e_2 d_2 - k_2 \phi(N) = 1$. Suppose that $d_1, d_2 \leq N^\delta$ and $|d_1 - d_2| < N^\delta$. Then $N$ can be factored if

$$\delta < \frac{11}{10} + \frac{9}{4} \alpha - \frac{1}{2} \beta - \frac{1}{2} \gamma - \frac{1}{30} \sqrt{180 \gamma + 990 \alpha} - 180 \beta + 64.$$  

**Proof.** See Appendix B.

4. Comparison with the Previous Attacks

We make a comparison of bounds with the previous analysis upon the modulus $N = p^r q$ for $r = 2$. Their analysis focused on the RSA key equation $ed - k\phi(N) = 1$ where $\phi(N) = p^{r-1}(p^r - 1)(q - 1)$. Note that in these former attacks, they do not consider
where the private exponent or the primes share an amount of LSBs or MSBs. Thus, in our comparison, we let $\beta = d_1 - d_2 = 1$, $\alpha = 0.2$. We get the following corollary.

**Corollary 1.** Let $N = p^2q$ be modulus with balanced primes. Let $e_1, e_2 \approx N^\gamma$ satisfies $e_1d_1 - k_1\phi(N) = 1$, and $e_2d_2 - k_2\phi(N) = 1$. Let $d_1, d_2 < N^\delta$. Then $N$ can be factored if

$$
\delta < \frac{21}{20} - \frac{1}{2}\gamma - \frac{1}{30}\sqrt{180\gamma + 82}.
$$

Table 2 shows that our bound improves the previous bounds. The value of $\delta$ increases impressively as the value of $\gamma$ decreases. Note that the bounds from the former attacks only consider the value of $r$, thus the values of $\delta$ is fixed for all values of $\gamma$. Refer Table 1 in Section 1 to see the bounds from these former attacks for $r = 2$.

**Table 2.** Comparison with methods from [10–12] for $\alpha = 0.2$ and $\beta = 1$.

| Bound of $\delta$ | $\gamma = \log_N(e)$ | $\gamma = 0.7$ | $\gamma = 0.60$ | $\gamma = 0.5$ | $\gamma = 0.4$ | $\gamma = 0.3$ |
|-------------------|------------------------|----------------|----------------|----------------|----------------|----------------|
| [12]              | 0.22                   | 0.22           | 0.22           | 0.22           | 0.22           | 0.22           |
| [10]              | 0.22                   | 0.22           | 0.22           | 0.22           | 0.22           | 0.22           |
| [11]              | 0.39                   | 0.39           | 0.39           | 0.39           | 0.39           | 0.39           |
| Our bound in Corollary 1 | 0.21 | 0.29 | 0.36 | 0.43 | 0.51 |

**Remark 1.** We want to analyze the bound for $\gamma$ that works for our attack. Observe that from the Corollary 1, after setting the value of $\beta = 1$ and $\alpha = 0.2$ we obtain

$$
\delta < \frac{21}{20} - \frac{1}{2}\gamma - \frac{1}{30}\sqrt{180\gamma + 82}.
$$

Assume that $e = N^\gamma$. From key equation, we have

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

then

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

Now, the condition of Corollary 1 becomes

$$1 - \gamma < \frac{21}{20} - \frac{1}{2}\gamma - \frac{1}{30}\sqrt{180\gamma + 82}.$$  

A straightforward calculation gives us the upper bound of the positive value $\gamma$ which is $\gamma < \frac{29}{30} \approx 0.96$. Hence, the method works for smaller value of $\gamma$. This translates into $d \approx N$.

5. Conclusions

We present an attack on partial key exposure for modulus $N = p^2q$. Note that our attack is an extension from [16]. In our paper, we show that despite the advantages of using the modulus $N = p^2q$, the modulus is still vulnerable to the attack if the primes share some amount of LSBs and the private keys $d_1, d_2$ share some amount of MSBs. We reformulate the lemma from [16] and find the substitution for $p^2 + pq - p$. We utilize the result in our lemma to prove our theorem that is based on the two key equations $e_1d_1 - k_1\phi(N) = 1$ and $e_2d_2 - k_2\phi(N) = 1$. From our theorem, we show that one can factor $N$ when $d < N^\delta$ for $\delta < \frac{11}{10} + \frac{3}{5}a - \frac{1}{2}\beta - \frac{1}{2}\gamma - \frac{1}{30}\sqrt{180\gamma + 990a - 180\beta + 64}$ for $0 < \gamma < 0.96$. Thus, one needs to be careful in selecting their primes and decryption exponents as it may leads to the vulnerability of their cryptosystem and their secret data might leak to an unauthorized
party. There are other schemes that one might be interested to apply in order to keep the data secure such as using covert channel [21] and double blockchain [22].

**Author Contributions:** Formal analysis, N.N.H.A., M.R.K.A., S.H.S., A.H.A.G. and M.A.A.; Funding acquisition, M.R.K.A.; Investigation, N.N.H.A.; Project administration, M.R.K.A.; Validation, S.H.S.; Writing—original draft, N.N.H.A.; Writing—review and editing, M.R.K.A., S.H.S., A.H.A.G. and M.A.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** The research was supported by Ministry of Education of Malaysia with Fundamental Research Grant Scheme (FRGS/1/2019/STG06/UPM/02/8).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

**Appendix A**

**Proof of Lemma 4.** Let \( p - q = 2^m u \). Then \( q = p - 2^m u \) and

\[
N = p^2 q = p^2 (p - 2^m u) = p^3 - 2^m u p^2.
\]  

(A1)

Hence, from (A1), we obtain \( p^3 \equiv N \pmod{2^m} \). Let \( u_0 \) be a solution of the modular equation \( p^3 \equiv N \pmod{2^m} \). Then, \( p \equiv u_0 \pmod{2^m} \) is a solution which can be rewritten as \( p = 2^m p_1 + u_0 \) where \( p_1 \) is a positive integer. Now we have,

\[
q = p - 2^m u = 2^m p_1 + u_0 - 2^m u = 2^m (p_1 - u) + u_0 = 2^m q_1 + u_0
\]

where \( q_1 = p_1 - u \). Utilizing \( N = p^2 q \) would yield

\[
N = (2^m p_1 + u_0)^2 (2^m q_1 + u_0)
\]

\[
= (2^m p_1^2 + 2^m+1 p_1 u_0 + u_0^2) (2^m q_1 + u_0)
\]

\[
= 2^{3m} p_1^2 q_1 + 2^{2m} p_1^2 u_0 + 2^{2m+1} p_1 u_0 q_1 + 2^{m+1} p_1 u_0^2 + 2^m q_1 u_0^2 + u_0^3.
\]

(A2)

From (A2), we deduce

\[
2^{2m} u_0 (p_1^2 + 2 p_1 q_1) + 2^m u_0^2 (2 p_1 + q_1) + u_0^3 \equiv N \pmod{2^{3m}}
\]

\[
2^{2m} u_0 (p_1^2 + 2 p_1 q_1) + 2^m u_0^2 (2 p_1 + q_1) \equiv N - u_0^3 \pmod{2^{3m}}.
\]

(A3)

Suppose \( \gcd(u_0, 2^{3m}) = 1 \), we multiply (A3) with \( u_0^{-1} \) and get

\[
2^{2m} (p_1^2 + 2 p_1 q_1) + 2^m u_0 (2 p_1 + q_1) \equiv u_0^{-1} (N - u_0^3) \pmod{2^{3m}}
\]

which can be rewritten as

\[
2^{2m} (p_1^2 + 2 p_1 q_1) + 2^m u_0 (2 p_1 + q_1) = 2^{3m} s + s_0
\]

where \( s_0 \equiv u_0^{-1} (N - u_0^3) \pmod{2^{3m}} \). Finally we have,

\[
p^2 + q = p = (2^m p_1 + u_0)^2 + (2^m p_1 + u_0) (2^m q_1 + u_0) - (2^m p_1 + u_0)
\]

\[
= 2^{2m} p_1^2 + 2^m+1 p_1 u_0 + u_0^2 + 2^{2m} p_1 q_1 + 2^m p_1 u_0 + 2^m q_1 u_0 + u_0^2 - 2^m p_1 - u_0
\]

\[
= 2^{2m} (p_1^2 + 2 p_1 q_1) + 2^m u_0 (2 p_1 + q_1) - (2^m p_1 + 2^m p_1 q_1 - 2^m p_1 u_0 - 2 u_0^2 + u_0)
\]

\[
= 2^{3m} s + s_0 - v
\]

where \( v = (2^m p_1 + 2^m p_1 q_1 - 2^m p_1 u_0 - 2 u_0^2 + u_0) \).
Appendix B

Proof of Theorem 3. Let $e_1$ and $e_2$ satisfy
\[ e_1d_1 - k_1\phi(N) = 1, \quad (A4) \]
\[ e_2d_2 - k_2\phi(N) = 1. \quad (A5) \]

Subtracting the product of (A4) by $e_2$ and (A5) by $e_1$, we get
\[ e_1e_2(d_1 - d_2) - e_2k_1\phi(N) + e_1k_2\phi(N) = e_2 - e_1. \quad (A6) \]

From Lemma 1, we show that $p^2 + pq - p$ can be substituted by $2^{3m}s + s_0 - v$ where $s_0 \equiv u_0^{-1}(N - u_0^3) \pmod{2^{3m}}$ and $u_0$ is a solution of the congruence $p^3 \equiv N \pmod{2^m}$. Therefore
\[ \phi(N) = p(p-1)(q-1) = N - (p^2 + pq - p) = N - (2^{3m}s + s_0 - v). \quad (A7) \]

Plugging (A7) in (A6), we get
\[ e_1e_2(d_1 - d_2) - e_2k_1\left(N - \left(2^{3m}s + s_0 - v\right)\right) + e_1k_2\left(N - \left(2^{3m}s + s_0 - v\right)\right) = e_2 - e_1. \quad (A8) \]

Rearranging (A8),
\[ e_1e_2(d_1 - d_2) - e_2(N - s_0k_1 + 2^{3m}e_2k_1s - e_2k_1v + e_1(N - s_0)k_2 - 2^{3m}e_1k_2s + e_1k_2v + (e_1 - e_2) = 0 \quad (A9) \]

We transform (A9) into
\[ a_1x_1 + a_2x_2 + a_3x_3x_4 + a_4x_2x_5 + a_5x_3 + a_6x_3x_4 + a_7x_3x_5 + a_8 = 0 \]
and we fix the coefficients and variables as follows:
\[
\begin{align*}
  a_1 &= e_1e_2, \\
  a_2 &= -e_2(N - s_0), \\
  a_3 &= 2^{3m}e_2, \\
  a_4 &= -e_2, \\
  a_5 &= e_1(N - s_0), \\
  a_6 &= -2^{3m}e_1, \\
  a_7 &= e_1, \\
  a_8 &= e_1 - e_2,
\end{align*}
\]
and
\[
\begin{align*}
  x_1 &= d_1 - d_2, \\
  x_2 &= k_1, \\
  x_3 &= k_2, \\
  x_4 &= s, \\
  x_5 &= v.
\end{align*}
\]

Now, we would have the polynomial
\[ f(x_1, x_2, x_3, x_4, x_5) = a_1x_1 + a_2x_2 + a_3x_2x_4 + a_4x_2x_5 + a_5x_3 + a_6x_3x_4 + a_7x_3x_5 + a_8. \]

Then $(d_1 - d_2, k_1, k_2, s, v)$ is a root of $f(x_1, x_2, x_3, x_4, x_5)$ and can be found by using Coppersmith’s technique [4]. However, we choose apply the extended strategy of Jochemsz and May [19] due to its easier implementation. The following bound will be needed:

- $\max(e_1, e_2) = N^\gamma$
- $\max(d_1, d_2) < N^\delta$
- $|d_1 - d_2| < X_1 = N^\beta$
\[ k_1 = \frac{d_1}{d_3} - 1 < X_2 = N^{\gamma + \delta - 1} \]
\[ k_2 = \frac{d_2}{d_3} - 1 < X_3 = N^{\gamma + \delta - 1} \]
\[ p - q = 2^m u \text{ with } 2^m \approx N^a \text{ and } a < \frac{2}{9}. \]
\[ p^2 + pq - p = 2^{3m} s + s_0 - v \text{ with} \]
\[ s = \frac{p^2 + pq - p - s - v}{2^{3m}} < X_4 = N^{2/3 - 3a}, \]
\[ v = 2^{3m} s + s_0 - (p^2 + pq - p) < X_5 = N^{2/3}. \]

Let \( m, t \in \mathbb{Z}^+ \). Define two sets,
\[
S = \bigcup_{0 \leq i \leq t} \{ x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \mid \text{monomial of } f^{m-1} \}
\]
and
\[
M = \{ \text{monomials of } x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} f \mid x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in S \}. \]

Using the binomial expansion formula, we find the expansion of polynomial \( f^{m-1}(x_1, x_2, x_3, x_4, x_5) \).
Neglecting the coefficients, we get
\[
f^{m-1}(x_1, x_2, x_3, x_4, x_5) = \sum_{i_1 = 0}^{m-1} \sum_{i_2 = 0}^{m-1-i_1} \sum_{i_3 = 0}^{m-1-i_1-i_2} \sum_{i_4 = 0}^{i_1} \sum_{i_5 = 0}^{i_2} x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5}. \quad (A10)
\]

The monomials \( x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \) in (A10) can be categorised as:
\[
x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in S \quad \text{if} \quad \begin{cases} i_1 = 0, \ldots, m - 1, \\ i_2 = 0, \ldots, m - 1 - i_1, \\ i_3 = 0, \ldots, m - 1 - i_1 - i_2, \\ i_4 = 0, \ldots, i_2 + i_3, \\ i_5 = 0, \ldots, i_2 + i_3 - i_4 + t, \end{cases}
\]
and
\[
x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in M \quad \text{if} \quad \begin{cases} i_1 = 0, \ldots, m, \\ i_2 = 0, \ldots, m - i_1, \\ i_3 = 0, \ldots, m - 1 - i_2, \\ i_4 = 0, \ldots, i_2 + i_3, \\ i_5 = 0, \ldots, i_2 + i_3 - i_4 + t. \end{cases}
\]

Define
\[
W = ||f(x_1 X_1, x_2 X_2, x_3 X_3, x_4 X_4, x_5 X_5)||_\infty.
\]
Then \( W \) satisfies
\[
W \geq |a_2| X_2 = e_2(N - s_0)k_1 = N^{\gamma + \delta - 1} \approx N^{2\gamma + \delta}. \quad (A11)
\]
Next define
\[
R = WX_1^{m-1} X_2^{m-1} X_3^{m-1} X_4^{m-1} X_5^{m-1}. \]
Suppose that \( a_8 = e_1 - e_2 \) is relatively prime with \( R \). We define \( f'(x_1, x_2, x_3, x_4, x_5) = a_8^{-1} f(x_1, x_2, x_3, x_4, x_5) \mod R \) in order to work with a polynomial with constant term 1. Next, define the polynomials

\[
G = x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5} f' X_1^{m-1-i_1} X_2^{m-1-i_2} X_3^{m-1-i_3} X_4^{m-1-i_4} X_5^{m-1+t-i_5},
\]

with \( x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5} \in S \)

\[
H = x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5} R,
\]

with \( x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5} \in M \backslash S \).

The basis of a lattice \( \mathcal{L} \) is built by using the coefficients of polynomial \( G \) and \( H \) with dimension

\[
\omega = \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5} \in M} 1 = \frac{1}{120} (m + 1)(m + 2)(m + 3)(3m^2 + 10mt + 17m + 20t + 20).
\]

In order to construct an upper triangular matrix, we perform the following ordering of the monomials: 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 lexicographically ordered if \( \sum i_j = \sum i'_j \). The diagonal entries of the matrix are of the form

\[
\begin{cases}
(X_1 X_2 X_3 X_4)^{m-1} X_5^{m-1+t} & \text{for polynomials } G \\
W X_1^{m-1+i_1} X_2^{m-1+i_2} X_3^{m-1+i_3} X_4^{m-1+i_4} X_5^{m-1+t+i_5} & \text{for polynomials } H
\end{cases}
\]

Refer the Table A1 in Appendix C for the coefficient matrix of \( m = 2 \) and \( t = 1 \). Next, we define

\[
s_j = \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5} \in M \backslash S} i_j, \text{ for } j = 1, ..., 5 \quad (A12)
\]

The determinant of \( \mathcal{L} \) is then

\[
\det(\mathcal{L}) = W^{\lceil M \backslash S \rceil} X_5^{(m-1+t)\omega + s_5} \prod_{j=1}^{4} X_j^{(m-1)\omega + s_j}.
\]

All the polynomials \( G \) and \( H \) and their combinations share the root \( (d_1 - d_2, k_1, k_2, s, v) \) modulo \( R \). A new basis with short vectors is produced after applying the LLL algorithm to the lattice \( \mathcal{L} \). For \( i = 1, ..., 4 \), let \( f_i(x_1 X_1, x_2 X_2, x_3 X_3, x_4 X_4, x_5 X_5) \) be four short vectors of the reduced basis. Each \( f_i \) is a combination of \( G \) and \( H \), and then share the root \( (d_1 - d_2, k_1, k_2, s, v) \). Applying Theorem 1 from Section 2, we have for \( i = 1, 2, 3, 4; \)

\[
||f_i(x_1 X_1, x_2 X_2, x_3 X_3, x_4 X_4, x_5 X_5)|| < 2^{\frac{\omega(\omega-1)}{4\omega + 1}} \det(\mathcal{L})^{-\frac{1}{2}}.
\]

We force the polynomials \( f_i \) for \( i = 1, 2, 3, 4 \), to comply with Howgrave-Graham’s bound [18] \(||f_i(x_1 X_1, x_2 X_2, x_3 X_3, x_4 X_4, x_5 X_5)|| < \frac{R}{\sqrt{\omega}} \). The condition is suffice when

\[
2^{\frac{\omega(\omega-1)}{4\omega + 1}} \det(\mathcal{L})^{-\frac{1}{2}} < \frac{R}{\sqrt{\omega}}
\]

which can be transformed into \( \det(\mathcal{L}) < R^\omega \), that is

\[
W^{\lceil M \backslash S \rceil} X_5^{(m-1+t)\omega + s_5} \prod_{j=1}^{4} X_j^{(m-1)\omega + s_j} < (W X_1 X_2 X_3 X_4)^{m-1} X_5^{m-1+t} \omega.
\]
Substituting \( \omega \) with \( |M| \) and \( |M| - |M \setminus S| \) with \( |S| \), we get

\[
\prod_{j=1}^{5} X_j^{y_j} < W^{|S|}. \tag{A13}
\]

Using (A12), we get

\[
s_1 = \frac{1}{120} m(m + 1)(m + 2)(3m^2 + 10mt + 11m + 10t + 6),
\]

\[
s_2 = \frac{1}{120} m(m + 1)(m + 2)(6m^2 + 15mt + 27m + 25t + 27),
\]

\[
s_3 = \frac{1}{120} m(m + 1)(m + 2)(6m^2 + 15mt + 27m + 25t + 27),
\]

\[
s_4 = \frac{1}{120} m(m + 1)(m + 2)(4m^2 + 15mt + 18m + 25t + 18),
\]

\[
s_5 = \frac{1}{120} (m + 1)(m + 2)(4m^3 + 15m^2t + 20mt^2 + 18m^2 + 45mt + 30t^2 + 18m + 30t).
\]

Similarly, we get

\[
|S| = \sum_{x_1, x_2, x_3, x_4, x_5 \in S} 1 = \frac{1}{120} m(m + 1)(m + 2)(3m^2 + 10mt + 11m + 10t + 6).
\]

Set \( t = \tau m \), then,

\[
s_1 = \frac{1}{120}(10\tau + 3)m^5 + o(m^5),
\]

\[
s_2 = \frac{1}{40}(5\tau + 2)m^5 + o(m^5),
\]

\[
s_3 = \frac{1}{40}(5\tau + 2)m^5 + o(m^5),
\]

\[
s_4 = \frac{1}{120}(15\tau + 4)m^5 + o(m^5),
\]

\[
s_5 = \frac{1}{120}(20\tau^2 + 15\tau + 4)m^5 + o(m^5),
\]

\[
|S| = \frac{1}{120}(10\tau + 3)m^5 + o(m^5).
\]

Using this, and after simplifying by \( m^5 \), the inequation (A13) transform into

\[
X_1^{\frac{1}{120}(10\tau + 3)} X_2^{\frac{1}{40}(5\tau + 2)} X_3^{\frac{1}{40}(5\tau + 2)} X_4^{\frac{1}{120}(15\tau + 4)} X_5^{\frac{1}{120}(20\tau^2 + 15\tau + 4)} < W^{\frac{1}{120}(10\tau + 3)}.
\]

Substituting and rearranging the values of \( X_1, X_2, X_3, X_4 \) and \( W \) from (A11) we get

\[
\frac{1}{120}(10\tau + 3)\beta + \frac{1}{40}(5\tau + 2)(\gamma + \delta - 1) + \frac{1}{120}(15\tau + 4) \left( \frac{2}{3} - 3\alpha \right)
\]

\[
+ \left( \frac{2}{3} \right) \frac{1}{120}(20\tau^2 + 15\tau + 4) < \frac{1}{120}(10\tau + 3)(2\gamma + \delta)
\]

or equivalently,

\[
40\tau^2 + (30\beta + 60\delta - 135\alpha + 30\gamma - 30)\tau + 9\beta + 27\delta + 18\gamma - 36\alpha - 20 < 0.
\]
Differentiate the equation above with respect to $\tau$, we get the optimal value

$$\tau = \frac{27\alpha - 6\delta - 12\beta - 6\gamma + 6}{16},$$

this reduces to

$$-720\delta^2 + (3240\alpha - 720\beta - 720\gamma + 1584)\delta - 3645\alpha^2 + 1620\alpha\beta + 1620\alpha\gamma - 2772\alpha$$

$$-180\beta^2 + 648\beta - 360\beta\gamma - 180\gamma^2 + 936\gamma - 820 < 0$$

which is valid if

$$\delta < \frac{11}{10} + \frac{9}{4} \alpha - \frac{1}{2} \beta - \frac{1}{2} \gamma - \frac{1}{30} \sqrt{180\gamma + 990\alpha - 180\beta + 64}.$$ 

We find our reduced polynomial $f, f_1, f_2, f_3, f_4$ with the root of $(d_1 - d_2, k_1, k_2, s, v)$ under this condition. By Assumption 1 in Section 2, the solution of the roots can be extracted using resultant technique. Then, using the fourth and fifth root, $s, v$, we compute

$$p^2 + pq - p = 2^{3m}s + s_0 - v.$$  \hspace{1cm} (A14)

After that, we use (A14) to find $\phi(N) = N - p^2 + pq - p$ and since $\phi(N) = p(p - 1)(q - 1)$, we can get $p$ by taking the gcd$(N, \phi(N))$. This leads to factorization of $N$ and hence terminates the proof. \hspace{1cm} \Box

Appendix C

Remark A1. Note that the values of $A$ and $B$ are as follows:

$A = X_1 X_2 X_3 X_4 X_5$

$B = X_1^i X_2^j X_3^k X_4^l X_5^m R$.  

Table A1. The coefficient matrix for the case $m = 2$ and $t = 0$.

|   |   |   |   |   |
|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 2 | 0 | 0 |
| 0 | 0 | 2 | 0 | 1 |
| 0 | 0 | 2 | 0 | 2 |
| 0 | 0 | 2 | 1 | 0 |
| 0 | 0 | 2 | 1 | 1 |
| 0 | 0 | 2 | 2 | 0 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 2 |
| 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 2 | 0 |
| 0 | 2 | 0 | 0 | 0 |
| 0 | 2 | 0 | 0 | 1 |
| 0 | 2 | 0 | 0 | 2 |
| 0 | 2 | 0 | 1 | 0 |
| 0 | 2 | 0 | 1 | 1 |
| 0 | 2 | 0 | 2 | 0 |
| 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 0 | 2 |
| 2 | 0 | 0 | 1 | 0 |
| 2 | 0 | 0 | 1 | 1 |
| 2 | 0 | 0 | 2 | 0 |

** denotes the non-zero elements.
References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 1978, 21, 120–126. [CrossRef]

2. Wiener, M.J. Cryptanalysis of short RSA secret exponents. J. IEEE T. Inform. Theory 1990, 36, 553–558. [CrossRef]

3. Boneh, D.; Durfee, G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. J. IEEE Trans. Inform. Theory 2000, 46, 1339–1349. [CrossRef]

4. Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. 1997, 10, 233–260. [CrossRef]

5. Hinek, M.J. Multi-Prime RSA. In Cryptanalysis of RSA and Its Variants; CRC: London, UK; New York, NY, USA, 2010; p. 155.

6. Takagi, T. A fast RSA-type public-key primitive modulo $p^rq$ using Hensel lifting. IEICE Trans. 2004, 87, 94–101.

7. Ariffin, M.R.K.; Asbullah, M.A.; Abu, N.A.; Mahad, Z. A new efficient asymmetric cryptosystem based on the integer factorization problem of $N = p^rq$. MJMS 2013, 10, 19–37.

8. Asbullah, M.A.; Ariffin, M.R.K. Design of Rabin-like cryptosystem without decryption failure. MJMS 2016, 10, 1–18.

9. Boneh, D.; Durfee, G.; Howgrave-Graham, N. Factoring $N = p^rq$ for large r. In Cryptographers’ Track at the RSA Conference; Springer: Cham, Switzerland, 1999; pp. 326–337.

10. May, A. A secret exponent attacks on RSA-type schemes with moduli $N = p^rq$. In International Workshop on Public Key Cryptography; Springer: Berlin/Heidelberg, Germany, 2004; pp. 128–230.

11. Sarkar, S. Small secret exponent attack on RSA variant with modulus $N = p^rq$. Des. Codes Cryptogr. 2014, 73, 383–392. [CrossRef]

12. Lu, Y.; Zhang, R.; Peng, L.; Lin, D. Solving linear equations modulo unknown divisors: Revisited. In International Conference on the Theory and Application of Cryptology and Information Security; Springer: Berlin/Heidelberg, Germany, 2015; pp. 189–213.

13. Boneh, D.; Durfee, G.; Frankel, Y. An attack on RSA given a small fraction of the private key bits. In International Conference on the Theory and Application of Cryptology and Information Security; Springer: Berlin/Heidelberg, Germany, 1998; pp. 25–34.

14. Sun, H.M.; Wu, M.E.; Steinfeld, R.; Guo, J.; Wang, H. Cryptanalysis of short exponent RSA with primes sharing least significant bits. In International Conference on Cryptology and Network Security; Springer: Berlin/Heidelberg, Germany, 2008; pp. 49–63.

15. Zhao, Y.D.; Qi, W.F. Small private-exponent attack on RSA with primes sharing bits. In International Conference on Information Security; Springer: Berlin/Heidelberg, Germany, 2007; pp. 221–229.

16. Nitaj, A.; Ariffin, M.R.K.; Nassr, D.I.; Bahig, H.M. New attacks on the RSA cryptosystem. In International Conference on Cryptology in Africa; Springer: Cham, Switzerland, 2014; pp. 178–198.

17. Lenstra, A.K.; Lenstra, H.W.; Lovasz, H.W. Factoring polynomials with rational coefficients. J. Math. Ann. 1982, 261, 515–534. [CrossRef]

18. Howgrave-Graham, N. Finding small roots of univariate modular equations revisited. In MA International Conference on Cryptography and Coding; Springer: Berlin/Heidelberg, Germany, 1997; pp. 131–142.

19. Jochemsz, E.; May, A. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In International Conference on the Theory and Application of Cryptology and Information Security; Springer: Berlin/Heidelberg, Germany, 2006; pp. 267–282.

20. Asbullah, M.A.; Ariffin, M.R.K. New attacks on RSA with modulus $N = p^rq$ using continued fractions. J. Phys. Conf. Ser. 2015, 622, 191–199. [CrossRef]

21. Zhang, L.; Huang, T.; Hu, X.; Zhang, Z.; Wang, W.; Guan, D.; Zhao, C.; Kim, S. A distributed covert channel of the packet ordering enhancement model based on data compression. Comput. Mater. Contin. 2020, 64, 2013–2030.

22. Zhang, L.; Peng, M.; Wang, W.; Cui, S.; Kim, S. Secure and efficient data storage and sharing scheme based on double blockchain. Comput. Mater. Contin. 2021, 66, 499–515.