PLOS ONE

RESEARCH ARTICLE

Analytical cryptanalysis upon $N = p^2q$ utilizing Jochemsz-May strategy

Nurul Nur Hanisah Adenan[1☯], **Muhammad Rezal Kamel Ariffin**[1,2☯*], **Faridah Yunos**[2‡], **Siti Hasana Sapar**[1,2‡], **Muhammad Asyraf Asbullah**[1,2‡]

1 Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor, Malaysia, **2** Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Serdang, Selangor, Malaysia

☯ These authors contributed equally to this work.
‡ These authors also contributed equally to this work.
* rezal@upm.edu.my

Citation: Adenan NNH, Kamel Ariffin MR, Yunos F, Sapar SH, Asbullah MA (2021) Analytical cryptanalysis upon $N = p^2q$ utilizing Jochemsz-May strategy. PLoS ONE 16(3): e0248888. https://doi.org/10.1371/journal.pone.0248888

Editor: Pandi Vijayakumar, University College of Engineering Tindivanam, INDIA

Received: September 27, 2020

Accepted: March 6, 2021

Published: March 24, 2021

Data Availability Statement: All relevant data are within the manuscript and Supporting information files. Datasets can be generated or analyzed by the reader from the characteristics of the data set as mentioned in the article. The characteristics can be found from the hypothesis and assumptions stated in the results within the article.

Funding: The research was supported by Ministry of Higher Education Malaysia with Fundamental Research Grant Scheme (FRGS/2/2013/SG04/UPM/02/2).

Abstract

This paper presents a cryptanalytic approach on the variants of the RSA which utilizes the modulus $N = p^2q$ where p and q are balanced large primes. Suppose $e \in \mathbb{Z}^+$ satisfying gcd $(e, \phi(N)) = 1$ where $\phi(N) = p(p-1)(q-1)$ and $d < N^{\delta}$ be its multiplicative inverse. From $ed - k\phi(N) = 1$, by utilizing the extended strategy of Jochemsz and May, our attack works when the primes share a known amount of Least Significant Bits(LSBs). This is achievable since we obtain the small roots of our specially constructed integer polynomial which leads to the factorization of N. More specifically we show that N can be factored when the bound $\delta < \frac{11}{9} - \frac{2}{9}\sqrt{4 + 18\gamma}$. Our attack enhances the bound of some former attacks upon $N = p^2q$.

1 Introduction

Secure communication up till the 70's was executed through symmetrical ways. In other word, both of the encryption and decryption processes used the same key. Later in 1978, the first assymetric cryptosystem went public and solved the problematic issue of distributing keys. This cryptosystem used different keys to encrypt and decrypt the data. It is known as the RSA cryptosystem [1]. The construction of the RSA algorithms comprise of key generation, encryption and decryption. During the key generation process, two large balanced primes p and q are generated and the modulus $N = pq$ is computed. Next, let e be a random integer such that gcd $(e, \phi(N)) = 1$ where $\phi(N) = (p-1)(q-1)$ is the Euler totient function. Let d be its multiplicative inverse of e such that $ed \equiv 1 \bmod \phi(N)$. Let (N, e) be publicised for encryption purpose while $p, q, \phi(N), d$ are kept private. For decryption process, private parameter d is needed. The mathematical difficulty of the RSA cryptosystem relies on the hardness of solving the integer factorization problem on $N = pq$, solving the key equation $ed - k\phi(N) = 1$ and solving the RSA diophantine key equation that is, $C \equiv M^e \bmod N$. Up until today, the RSA cryptosystem has remained secure.

In 1990, [2] found out a potential weakness on this cryptosystem. He proved that if $d < \frac{1}{3}N^{\frac{1}{4}}$, then one can factor N by using the continued fractions expansion method. In the following years, more resarchers worked on the same objective as [2] and managed to enhance

Competing interests: The authors have declared that no competing interest exist.

the bound d. Later in 1996, [3] came out with an astounding method that is very useful to find the roots of either univariate or multivariate polynomial. Since then, this method has been used extensively in both cryptography and cryptanalysis. [4] utilized this method in their attack and they improved the bound of [2] up to $d < N^{0.292}$.

Another potential weakness upon the RSA cryptosystem is when there is leaked information regarding either the MSB(s) or LSB(s) of the private keys which is known as partial key exposure attack. In 1998, [5] proved that the whole value of d could be retrieved if a quater of d is known [6], and [7] also showed that if the primes share either MSB(s) or LSB(s), then the modulus can be factored in polynomial time. Later in 2014, [8] published an attack on RSA cryptosystem when the primes share the LSB(s) and there exists two public exponents such that their private exponents share their MSB(s).

Multi-Power RSA is one of the variants of the RSA whereby the modulus $N = p^r q$ 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 [9]. Among cryptosystems that utilize this fact are designs by [10–12]. 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 $N = p^r q$ becomes important. [13] proved that $N = p^r q$ is factorable for large r, when $r \cong \log p$. Since then, many attackers made an attempt to cryptanalyse the multi-power RSA modulus. For instance, [14] showed that the modulus $N = p^r q$ is more vulnerable compared to $N = pq$. For $r = 2$, the author proved that N can be factored if $d < N^{0.292}$. In 2014, [15] presented his proof that $N = p^2q$ can be factored by using lattice reduction techniques provided $d < N^{0.395}$.

1.1 Our contribution

We are working on the same purpose as the previous researchers which is to find other weakness of the RSA in order to enhance its security. Therefore in this paper, we present an attack on the modulus $N = p^2q$ where the primes share a known amount of LSB(s). Note that this is an extended result from [8]. We apply the strategy of Jochemsz and May to find small roots of our integer polynomial and show that the modulus N can be factored when $d < N^{\delta}$ where

$$\delta < \frac{11}{9} - \frac{2}{9}\sqrt{4 + 18\gamma}.$$

The construction of this paper is as follows. In Section 1, we intoduce the mechanisms and some results that will be used throughout this paper. In Section 2, we present the result on our attack theoretically. We also make a comparison with the previous attacks. Finally we conclude in Section 4.

2 Materials and methods

This section will discuss briefly on lattice basis reduction, Howgrave-Graham theorem, and useful lemmas that will be needed in this study.

2.1 Lattice

Suppose $\omega, n \in \mathbb{Z}^+$ with $\omega \leq n$. Let $v_1, \cdots, v_\omega$ be linearly independent vectors in real numbers field. A lattice $\mathcal{L}$ is spanned by a set of linear combination $\{v_1, \cdots, v_\omega\}$ in the form

$$\mathcal{L} = \left\{ \sum_{k=1}^{\omega} x_k u_k \mid x_k \in \mathbb{Z} \right\}$$

with the dimension of ω. The lattice is called full rank if the dimension $\omega = n$. Thus, the determinant is calculated by taking the absolute value of the determinant of the matrix whose rows consist of $\{v_1, \cdots, v_\omega\}$ [16]. [17] formulated *LLL* algorithm to find a short basis vector in time polynomial.

Theorem 1 [17] *Let $\mathcal{L}$ be the lattice generated by a set of basis $\{v_1, \ldots, v_\omega\}$ and has the dimension ω. The reduced basis $\{b_1, \ldots, b_\omega\}$ produced by the LLL algorithm satisfies*

$$||b_1|| \leq ||b_2|| \leq \cdots \leq ||b_i|| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}$$

for all $1 \leq i \leq \omega$.

Since its invention, *LLL* algorithm has been extensively applied in order to find reduced basis vectors in a lattice. For instance, [3] introduced a method to find a small roots of modular polynomial. Applying the *LLL* algorithm to find a reduced basis of the lattice generated by the modular polynomial, [3] managed to obtain the roots of the polynomial. Later, [18] described an alternative to Coppersmith's method and he came out with the following theorem.

Theorem 2 [18] *Let $h(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with at ω monomials. Suppose that $h(x_1^{(0)}, \ldots, x_n^{(0)}) \equiv 0 \pmod{R}$ where $|x_i^{(0)}| < X_i$ for $i = 1, \ldots, n$, 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 a notable assumption that also had been used in some earlier proposed attacks such as [4, 15, 19].

Assumption 1. *The construction of LLL algorithm produces a number of coprime polynomials. The roots of these polynomials can be computed efficiently using the resultant technique.*

2.2 Approximation of primes in RSA

The following results by [20] show an approximation of the size of the primes and approximation of $N - \phi(N)$. These results will be used to approximate the bound for one of the variables in our polynomial.

Lemma 1 *Let $N = p^2q$ with $q < p < 2q$. Then*

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

Lemma 2 *Let $N = p^2q$ with $q < p < 2q$. Then*

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

2.3 Prime sharing bits

The following lemma is reformulated from result [8]. It considers the case when the modulus $N = p^2q$ consists of two primes that share a known amount of their LSBs.

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

$$v = (2^b p_1 + 2^{2b} p_1 q_1 - 2^b p_1 u_0 - 2u_0^2 + u_0).$$

Proof. Suppose that $p - q = 2^b u$. Then $q = p - 2^b u$ and

$$N = p^2q = p^2(p - 2^b u) = p^3 - 2^b up^2. \tag{1}$$

Hence, from (1), we obtain $p^3 \equiv N \pmod{2^b}$. Let u_0 be a solution of the modular form $p^3 \equiv N$

$(\text{mod } 2^b)$. Then, $p \equiv u_0 \ (\text{mod } 2^b)$ is a solution which implies that $p = 2^b p_1 + u_0$ where p_1 is a positive integer. Now we have,

$$q = p - 2^b u = 2^b p_1 + u_0 - 2^b u = 2^b(p_1 - u) + u_0 = 2^b q_1 + u_0$$

where $q_1 = p_1 - u$. Using $N = p^2q$, we get

$$\begin{aligned} N &= (2^b p_1 + u_0)^2 (2^b q_1 + u_0) \\ &= (2^{2b} p_1^2 + 2^{b+1} p_1 u_0 + u_0^2)(2^b q_1 + u_0) \\ &= 2^{3b} p_1^2 q_1 + 2^{2b} p_1^2 u_0 + 2^{2b+1} p_1 u_0 q_1 + 2^{b+1} p_1 u_0^2 + 2^b q_1 u_0^2 + u_0^3. \end{aligned} \tag{2}$$

From (2) we deduce

$$\begin{aligned} 2^{2b} u_0(p_1^2 + 2p_1q_1) + 2^b u_0^2(2p_1 + q_1) + u_0^3 &\equiv N \ (\text{mod } 2^{3b}) \\ 2^{2b} u_0(p_1^2 + 2p_1q_1) + 2^b u_0^2(2p_1 + q_1) &\equiv N - u_0^3 \ (\text{mod } 2^{3b}). \end{aligned} \tag{3}$$

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

$$2^{2b}(p_1^2 + 2p_1q_1) + 2^b u_0(2p_1 + q_1) \equiv u_0^{-1}(N - u_0^3) \ (\text{mod } 2^{3b})$$

which can be rewritten as

$$2^{2b}(p_1^2 + 2p_1q_1) + 2^b u_0(2p_1 + q_1) = 2^{3b} s + s_0$$

where $s_0 \equiv u_0^{-1}(N - u_0^3) \ (\text{mod } 2^{3b})$. Finally we have,

$$\begin{aligned} p^2 + pq - p &= (2^b p_1 + u_0)^2 + (2^b p_1 + u_0)(2^b q_1 + u_0) - (2^b p_1 + u_0) \\ &= 2^{2b} p_1^2 + 2^{b+1} p_1 u_0 + u_0^2 + 2^{2b} p_1 q_1 + 2^b p_1 u_0 + 2^b q_1 u_0 + u_0^2 - 2^b p_1 - u_0 \\ &= 2^{2b}(p_1^2 + 2p_1q_1) + 2^b u_0(2p_1 + q_1) - (2^b p_1 + 2^{2b} p_1 q_1 2^b p_1 u_0 - 2u_0^2 + u_0) \\ &= 2^{3b} s + s_0 - v \end{aligned} \tag{4}$$

where $v = (2^b p_1 + 2^{2b} p_1 q_1 - 2^b p_1 u_0 - 2u_0^2 + u_0)$.

3 The new attack

This section presents the attack on modulus $N = p^2q$ which works when there has a known amount of LSBs shared between the primes p and q.

Theorem 3 *Let $N = p^2q$ be modulus such that $p - q = 2^b u$ where $2^b \approx N^\alpha$. Let e be a public exponents satisfying $e \approx N^\gamma$ and $ed - k\phi(N) = 1$. Suppose that $d < N^\delta$. Then N can be factored in time polynomial if*

$$\delta < \frac{11}{9} - \frac{2}{9}\sqrt{4 + 18\gamma}.$$

Proof. Suppose we have public exponent e and key equation

$$\begin{aligned} ed - k\phi(N) &= 1 \\ ed - k(p(p-1)(q-1)) &= 1 \\ ed - k(N - (p^2 + pq - p)) &= 1. \end{aligned} \tag{5}$$

Suppose that $p - q = 2^b u$. Then, from Lemma 3, $p^2 + pq - p$ can be rewritten in the form $p^2 + pq - p = 2^{3b} s + s_0 - v$ where $s_0 \equiv u_0^{-1}(N - u_0^3)(\text{mod } 2^{3b})$ and u_0 is a solution of the modular

equation $p^3 \equiv N \pmod{2^b}$. Thus, substitutes (4) from Lemma 3 into (5), we get

$$ed - k(N - (2^{3b}s + s_0 - v)) = 1.$$

Rearranging the equation,

$$ed - k(N - s_0) + k(2^{3b}s - v) - 1 = 0. \tag{6}$$

We transform (6) into

$$a_1x_1 + a_2x_2 + x_2x_3 + a_3 = 0.$$

and we fix the coefficients and the variables of the polynomial as follows:

$$\begin{cases} a_1 &= e \\ a_2 &= (N - s_0), \\ a_3 &= -1 \end{cases} \quad \text{and} \quad \begin{cases} x_1 &= d, \\ x_2 &= k, \\ x_3 &= 2^{3b}s - v. \end{cases}$$

Now, we consider the polynomial

$$f(x_1, x_2, x_3) = a_1x_1 + a_2x_2 + x_2x_3 + a_3.$$

Then $(d, k, 2^{3b}\, s - v)$ is a root of $f(x_1, x_2, x_3)$ and can be solved by using Coppersmith's technique [3]. However, we choose to use the extended strategy of Jochemsz and May [21] due to its easier implementation. The following bounds will be needed:

- $\max(e_1, e_2) = N^{\gamma}$.
- $\max(d) < X_1 = N^{\delta}$.
- $k = \frac{e_1d_1 - 1}{\phi(N)} < X_2 = N^{\gamma+\delta-1}$.
- $p - q = 2^b\, u$ with $2^b \approx N^{\alpha}$ and $\alpha < \frac{2}{9}$.
- $p^2 + pq - p = 2^{3b}\, s + s_0 - v$ with $2^{3b}\, s - v < X_3 = N^{2/3}$.

The bounds of the variables are fixed as follows:

$$X_1 = N^{\delta}, X_2 = N^{\gamma+\delta-1}, X_3 = N^{2/3}$$

Let $m, t \in \mathbb{Z}^+$. The set S and M be defined as:

$$S = \bigcup_{0 \le j \le t} \{x_1^{i_1}x_2^{i_2}x_3^{i_3+j} | x_1^{i_1}x_2^{i_2}x_3^{i_3} \text{ monomial of } f^{m-1}\}$$

and the set

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

Neglecting the coefficients, we find the expansion of polynomial $f^{m-1}(x_1, x_2, x_3)$ satisfies

$$f^{m-1}(x_1, x_2, x_3) = \sum_{i_1=0}^{m-1} \sum_{i_2=0}^{i_1} \sum_{i_3=0}^{m-1-i_1} x_1^{i_1}x_2^{i_2}x_3^{i_3} \tag{7}$$

The monomials $x_1^{i_1}x_2^{i_2}x_3^{i_3}$ in (7) can be categorised as:

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

Consequently, the monomials for set M are

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

Define

$$\begin{aligned} W &= ||f(x_1X_1, x_2X_2, x_3X_3)||_\infty \\ &= \max(|a_1|X_1, |a_2|X_2, X_2X_3). \end{aligned}$$

Then W satisfies

$$W \geq |a_1|X_1 = ed \approx N^{\gamma+\delta} = N^{\gamma+\delta}. \tag{8}$$

Next, define

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

Suppose that a_4 is coprime with R. We want to work with a polynomial that has constant term 1, thus we define $f'(x_1, x_2, x_3) = a_4^{-1}f(x_1, x_2, x_3) \mod R$. Next, define the polynomials g and h as:

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

The basis of a lattice $\mathcal{L}$ is built by using the coefficients of polynomials g and h with dimension

$$\omega = \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3} \in M} 1 = \sum_{i_1=0}^{m}\sum_{i_2=0}^{m-i_1}\sum_{i_3=0}^{i_2+t} 1 = \frac{1}{6}(m+1)(m+2)(m+3t+3).$$

In order to construct an upper triangular matrix, we perform the following ordering of the monomials: if $\sum i_j < \sum i'_j$ then $x_1^{i_1}x_2^{i_2}x_3^{i_3} < x_1^{i'_1}x_2^{i'_2}x_3^{i'_3}$ and the monomials are lexicographically ordered if $\sum i_j = \sum i'_j$. The diagonal entries of the matrix are of the form

$$\begin{cases} (X_1X_2)^{m-1}X_3^{m-1+t} & \text{for the polynomials } g \\ WX_1^{m-1+i_1}X_2^{m-1+i_2}X_3^{m-1+t+i_3} & \text{for the polynomials } h. \end{cases}$$

Refer S1 Table in S1 Appendix for the coefficient matrix of $m = 3$ and $t = 1$.

Next, define

$$s_j = \sum_{x_1^{i1} x_2^{i2} x_3^{i3} \in M \setminus S} i_j, \text{ for } j = 1, 2, 3. \tag{9}$$

The determinant of $\mathcal{L}$ is then

$$\det(\mathcal{L}) = W^{|M\setminus S|} X_3^{(m-1+t)|S|+(m-1+t)|M\setminus S|+s_3} \prod_{j=1}^{2} X_j^{(m-1)|S|+(m-1)|M\setminus S|+s_j}$$

which can be simplified into

$$\det(\mathcal{L}) = W^{|M\setminus S|} X_3^{(m-1+t)\omega+s_3} \prod_{j=1}^{2} X_j^{(m-1)\omega+s_j}.$$

All the polynomials $g(x_1, x_2, x_3)$ and $h(x_1, x_2, x_3)$ and their combinations share the root (d, k, 2^{3b} $s - v$) modulo R. A new basis with short vectors is produced after applying the LLL algorithm to the lattice $\mathcal{L}$. For $i = 1, 2$, let $f_i(x_1 X_1, x_2 X_2, x_3 X_3)$ be two short vectors of the reduced basis. Each f_i shares the roots (d, k, 2^{3b} $s - v$). Then by Theorem 3, we have

$$||f_i(x_1X_1, x_2X_2, x_3X_3)|| < 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}} \qquad \text{for} \quad i = 1, 2.$$

In order to fulfill the condition of the bound proposed by [18], we force the polynomials f_i for $i = 1, 2$ to fulfill the condition of

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

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

$$W^{|M\setminus S|} X_3^{(m-1+t)\omega+s_3} \prod_{j=1}^{2} X_j^{(m-1)\omega+s_j} < (W X_1^{m-1} X_2^{m-1} X_3^{m-1+t})^{\omega}$$

$$X_3^{s_3} \prod_{j=1}^{2} X_j^{s_j} < W^{\omega-|M\setminus S|}.$$

Using $\omega = |M|$ and $|M| - |M\setminus S| = |S|$, we get

$$\prod_{j=1}^{3} X_j^{s_j} < W^{|S|}. \tag{10}$$

Using (9), we get

$$\begin{aligned} s_1 &= \sum_{i_1=0}^{m}\sum_{i_2=0}^{m-i_1}\sum_{i_3=0}^{i_2+t} i_1 - \sum_{i_1=0}^{m-1}\sum_{i_2=0}^{m-1-i_1}\sum_{i_3=0}^{i_2+t} i_1 \\ &= \frac{1}{6}m(m+1)(m+3t+2) \\ s_2 &= \sum_{i_1=0}^{m}\sum_{i_2=0}^{m-i_1}\sum_{i_3=0}^{i_2+t} i_2 - \sum_{i_1=0}^{m-1}\sum_{i_2=0}^{m-1-i_1}\sum_{i_3=0}^{i_2+t} i_2 \\ &= \frac{1}{6}m(m+1)(2m+3t+4) \\ s_3 &= \sum_{i_1=0}^{m}\sum_{i_2=0}^{m-i_1}\sum_{i_3=0}^{i_2+t} i_3 - \sum_{i_1=0}^{m-1}\sum_{i_2=0}^{m-1-i_1}\sum_{i_3=0}^{i_2+t} i_3 \\ &= \frac{1}{6}(m+1)(m^2+3mt+2m+3t^2+3t). \end{aligned}$$

Correspondingly, we get

$$|S| = \sum_{x_1^{i_1}x_2^{i_2}x_3^{i_3}\in S} 1 = \sum_{i_1=0}^{m-1}\sum_{i_2=0}^{m-1-i_1}\sum_{i_3=0}^{i_2+t} = \frac{1}{6}m(m+1)(m+3t+2).$$

Set $t = \tau m$, then,

$$\begin{aligned} s_1 &= \frac{1}{6}(3\tau+1)m^3 + o(m^3) \\ s_2 &= \frac{1}{6}(3\tau+2)m^3 + o(m^3) \\ s_3 &= \frac{1}{6}(3\tau^2+3\tau+1)m^3 + o(m^3) \\ |S| &= \frac{1}{6}(3\tau+1)m^3 + o(m^3) \end{aligned}$$

Using this, and after simplifying by m^3, the inequality (10) transform into

$$X_1^{\frac{1}{6}(3\tau+1)}X_2^{\frac{1}{6}(3\tau+2)}X_3^{\frac{1}{6}(3\tau^2+3\tau+1)} < W^{\frac{1}{6}(3\tau+1)}$$

Substituting the values of X_1, X_2, X_3 and W from (8) we get

$$(\delta)(\frac{1}{6}(3\tau+1))(\gamma+\delta-1)(\frac{1}{6}(3\tau+2))(\frac{2}{3})(\frac{1}{6}(3\tau^2+3\tau+1)) < (\gamma+\delta)(\frac{1}{6}(3\tau+1))$$

or equivalently,

$$\frac{1}{3}\tau^2 + \frac{1}{6}(3\delta-1)\tau + \frac{1}{36}(6\gamma+12\delta-8) < 0.$$

Differentiate the equation above with respect to τ, we get the optimal value $\tau = \frac{-3\delta+1}{4}$, this

reduces to

$$-27\delta^2 + 66\delta + 24\gamma - 35 < 0$$

which is valid if

$$\delta < \frac{11}{9} - \frac{2}{9}\sqrt{4 + 18\gamma}.$$

Under this condition of δ, we find our reduced polynomials f, f_1, f_2 with the root of $(d, k, 2^{3b}s - v)$. By Assumption 1 in Section 2, the solution of the roots can be extracted using resultant technique. By using the third root $2^{3b}s - v$, we compute $p^2 + pq - p = 2^{3b}s + s_0 - v$. This value is then used to find $\phi(N)$ and since $\phi(N) = p(p-1)(q-1)$ we can factor out p by taking the gcd $(N, \phi(N))$. By knowing the value of p, we can factor the modulus N.

3.1 Comparison with the former attack

We compare our bounds with these three former attacks, [14, 15 and 19] that also work on modulus $N = p^r q$ but we specifically consider the case when $r = 2$. Their attacks 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, their primes do not share any amount of LSBs. Their bounds depend only on the value of r. We compare the results with various values of $\gamma = \log_N(e)$. Our corollary is as follow.

Corollary 1 *Let $N = p^2q$ be the modulus where $q < p < 2q$. Let e be a public exponent satisfying $ed - k\phi(N) = 1$ for $\phi(N) = p(p-1)(q-1)$. Suppose that $d < N^{\delta}$. Then N can be factored in time polynomial if*

$$\delta < \frac{11}{9} - \frac{2}{9}\sqrt{4 + 18\gamma}.$$

Note that the bounds for δ of [14, 15 and 19] remain fixed because their bounds only depend on the value of $r = 2$. We describe their bound for d as in the Table 1 below.

Table 2 shows that our bound improves the previous bounds. The value of δ increases inversely proportional to the value of γ.

Table 1. Bounds for d from the former attacks.

Former attack	Bound
[14]	$d < N^{\max\left\{\frac{r}{(r+1)^2}, \frac{(r-1)^2}{(r+1)^2}\right\}} = N^{0.22}$
[15]	$d < N^{0.39}$
[19]	$d < N^{\frac{r(r-1)}{(r+1)^2}} = N^{0.22}$

https://doi.org/10.1371/journal.pone.0248888.t001

Table 2. Comparison of the new result with methods from [14, 15, 19].

Bound of δ \ $\gamma = \log_N(e)$	$\gamma = 0.6$	$\gamma = 0.5$	$\gamma = 0.4$	$\gamma = 0.3$
[14]	0.22	0.22	0.22	0.22
[15]	0.39	0.39	0.39	0.3
[19]	0.22	0.22	0.22	0.22
Our bound in Corollary 1	0.36	0.42	0.47	0.54

https://doi.org/10.1371/journal.pone.0248888.t002

Remark 1 In Corollary 1, it states that N can be factored if

$$\delta < \frac{11}{9} - \frac{2}{9}\sqrt{4 + 18\gamma}.$$

Suppose $e = N^{\gamma}$. We have

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

then

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

From the fact that

$$\delta > 1 - \gamma$$

and combining it with results from Corollary 1, $\delta < \frac{2}{3} - \frac{1}{2}\gamma$, we have

$$1 - \gamma \quad < \frac{11}{9} - \frac{2}{9}\sqrt{4 + 18\gamma}.$$

From here, we can find the bound for the positive value of γ. A direct calculation shows that $\gamma < \frac{2}{3}$. For small values of γ, this translates into $d \approx N$.

4 Conclusion

We describe an attack related to partial key exposure. Our attack works upon the modulus $N = p^2q$ where the primes share an amount of LSB(s). Based on the result of Nitaj et al. [8], we reformulate their lemma within our theorem and find the substitution for $p^2 + pq - p$ which is the value of $N - \phi(N)$. We use the result from our lemma in our theorem which then yields a set of integer polynomials. By applying the extended strategy of Jochemsz and May, one is able to determine the small roots of our integer polynomial and thus factoring the modulus N. We show that N can be factored when $d < N^{\delta}$ for $\delta < \frac{2}{3} + \frac{3}{2}\alpha - \frac{1}{2}\gamma$ where $0 < \gamma < \frac{2}{3}$. As such, we manage to improve the bounds of some previous attacks on the modulus $N = p^2q$.

Supporting information

S1 Appendix.
(PDF)

Author Contributions

Conceptualization: Muhammad Rezal Kamel Ariffin.

Formal analysis: Nurul Nur Hanisah Adenan, Muhammad Rezal Kamel Ariffin.

Funding acquisition: Muhammad Rezal Kamel Ariffin.

Investigation: Muhammad Rezal Kamel Ariffin.

Methodology: Nurul Nur Hanisah Adenan.

Project administration: Muhammad Rezal Kamel Ariffin.

Validation: Muhammad Rezal Kamel Ariffin, Faridah Yunos, Siti Hasana Sapar, Muhammad Asyraf Asbullah.

Writing – original draft: Nurul Nur Hanisah Adenan.

Writing – review & editing: Nurul Nur Hanisah Adenan, Muhammad Rezal Kamel Ariffin, Faridah Yunos, Siti Hasana Sapar, Muhammad Asyraf Asbullah.

References

1. Rivest RL, Shamir A, and Adleman L, A method for obtaining digital signatures and public-key cryptosystems Comm. of the ACM. 1978; 21:120–126. https://doi.org/10.1145/357980.358017
2. Wiener MJ. Cryptanalysis of short RSA secret exponents. IEEE T. Inform. Theory. 1990; 36:553–558. https://doi.org/10.1007/3-540-46885-4_36
3. Coppersmith D, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J Cryptology,1997; 233–260. https://doi.org/10.1007/s001459900030
4. Boneh D, and Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. Inform. Theory. 2000; 46:1339–1349. https://doi.org/10.1007/3-540-48910-X_1
5. Boneh D, Durfee G, and Frankel Y. An attack on RSA given a small fraction of the private key bits. ASIACRYPT. 1998; 25–34. https://doi.org/10.1007/3-540-49649-1_3
6. Sun HM, Wu ME, Steinfeld R, Guo J, and Wang H. Cryptanalysis of short exponent RSA with primes sharing least significant bits CANS.2008; 49-63. https://doi.org/10.1007/978-3-540-89641-8_4
7. Zhao YD, and Qi WF. Small private-exponent attack on RSA with primes sharing bits Proc. ISC, 2007; 221-229. https://doi.org/10.1007/978-3-540-75496-1_15
8. Nitaj A, Ariffin MRK, Nassr DI, Bahig HM. New attacks on the RSA cryptosystem. Proc AFRICACRYPT. 2014; 178–198. https://doi.org/10.1007/978-3-319-06734-6_12
9. Hinek MJ, Cryptanalysis of RSA and its variants pp. 155. CRC, London, NY, USA (2010).
10. Takagi T. A fast RSA-type public-key primitive modulo $p^k q$ using Hensel lifting. IEICE Transactions. 2004; 87-A:94–101.
11. Ariffin MRK, Asbullah MA, Abu NA, Mahad Z. A new efficient asymmetric cryptosystem based on the integer factorization problem of $N = p^2q$. MJMS. 2013 7:19–37.
12. Asbullah MA, Ariffin MRK. Design of Rabin-like cryptosystem without decryption failure. MJMS. 2016; 10:1–18.
13. Boneh D, and Durfee G, and Howgrave-Graham N. Factoring $N = p^r q$ for large r. CRYPTO. 1999; 326–337. https://doi.org/10.1007/3-540-48405-1_21
14. May A. A secret exponent attacks on RSA-typer schemes with moduli $N = p^r q$. Proc IACR-PKC. 2004; 218–230. https://doi.org/10.1007/978-3-540-24632-9_16
15. Sarkar S. Small secret exponent attack on RSA variant with modulus $N = p^r q$. Des. Codes Cryptogr. 2014; 73:383–392. https://doi.org/10.1007/s10623-014-9928-6
16. Nitaj A. An attack on RSA using LSBs of multiples of the prime factors. Proc AFRICACRYPT. 2013; 297–310. https://doi.org/10.1007/978-3-642-38553-7_17
17. Lenstra AK, Lenstra HW, Lovasz HW, Factoring polynomials with rational coefficients. Math Ann. 1982; 261: 515–534. https://doi.org/10.1007/BF01457454
18. Howgrave-Graham N. Finding small roots of univariate modular equations revisited. IMA Conference on Cryptography and Coding. 1997; 131–142. https://doi.org/10.1007/BFb0024458
19. Lu Y, Zhang R, Peng L, and Lin D. Solving linear equations modulo unknown divisors: revisited. Proc ASIACRYPT. 2015; 189–213. https://doi.org/10.1007/978-3-662-48797-6_9
20. Asbullah MA. New attacks on RSA with modulus $N = p^2q$ using continued fractions. Journal of Physics: Conference Series. 2015 622:191–199. https://doi.org/10.1088/1742-6596/622/1/012019
21. Jochemsz E, May A, A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants Proc ASIACRYPT 2006. 2006; 267-282. https://doi.org/10.1007/11935230_18