Relationship between Divisors' Distribution and Square Root of a RSA Modulus

Xingbo Wang and Yanjie Miao

Abstract—The article investigates relationship between divisor's distribution and the square root of a RSA modulus. With the help of T₃ tree, it proves several conclusions that can determine the scope of the small divisor of a semiprime whose divisor-ratio is smaller than 2. The proved conclusions are helpful to judge if a small divisor of a semiprime is on certain level of T₃. Numerical experiments in Mathematica are made and the experiments strongly support the proved conclusions.

Index Terms—Cryptography, RSA modulus, square root, divisor distribution.

I. INTRODUCTION

One of the issues that attract the eyeballs of researchers in cryptography is the problem of factoring an integer. It is known that the safety of the RSA public cryptosystem is built upon the great difficulty of factoring an RSA modulus. Accordingly, factorization of the RSA modulus has become a practical criterion to challenge human being's intelligence and thousands of people have still kept doing the factorization, as overviewed in [1]-[7].

In August 2016, Wang introduced a new approach, called T₃ tree, to study integers in article [8]. Through the approach, many new properties of integers were disclosed, as introduced in papers [9]-[11], and even new approaches to factorize integers were found, as claimed in papers [12]-[14]. It is sure that, the T₃ tree ideology is revealing its characteristics in studying odd integers.

As a new number structure, there are many new properties to disclose. For example, paper [15] investigated the influence of divisor-ratio to distribution of semiprime's divisor on T₃, papers [16], [17] investigated square root of a node on the tree, paper [18] proved some inequalities on the tree and paper [19] explored the traits of a RSA modulus on the tree. The paper [19] proved that, the two divisors of a RSA modulus N would lie on the same level or on two adjacent levels, at least one divisor would lie on the same level as where $\lfloor \sqrt{N} \rfloor$ is clamped, and there were three possible cases by means of which the two divisors of N distribute. The paper had already mentioned the importance of $\lfloor \sqrt{N} \rfloor$ in analyzing the distribution of the divisors but it did not explore $\lfloor \sqrt{N} \rfloor$ as much as expected.

Accordingly, this paper follows the study of paper [19], investigating the relationship between $\lfloor \sqrt{N} \rfloor$ and the distribution of the two divisors.

II. PRELIMINARIES

A. Definitions and Notations

Let S be a set of finite positive integers with s_0 and s_n being the smallest and the biggest nodes respectively; an integer x is said to be *clamped* in S if $s_0 \leq x \leq s_n$. Symbol $x \triangle S$ indicates that x is clamped in S . Symbol $\lfloor x \rfloor$ is the floor function, an integer function of real number x that satisfies inequality $x-1 < \lfloor x \rfloor \leq x$, or equivalently $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Let $N = pq$ be an odd integer with $1 < p < q$; then $k = \frac{q}{p}$ is called the *divisor-ratio* of N .

In this whole paper, symbol T_3 is the T₃ tree that was introduced in [8] and [9] and symbol $N_{(k,j)}$ is by default the node at position j on level k of T_3 , where $k \geq 0$ and $0 \leq j \leq 2^k - 1$. By using the asterisk wildcard *, symbol $N_{(k,*)}$ means a node lying on level k . An integer X is said to be clamped on level k of T_3 if $2^{k+1} \leq X \leq 2^{k+2} - 1$ and symbol $X \triangle k$ indicates X is clamped on level k . If a positive integer X is clamped on level k and there is a node Y of T_3 satisfying $x = \lfloor \sqrt{Y} \rfloor$, then X is said to be a *floor square root* of the node Y and Y is called a *square source* of X . An odd integer O satisfying $2^{k+1} + 1 \leq O \leq 2^{k+2} - 1$ is said to be on level k of T_3 , and use symbol $O \triangle k$ to express it.

Symbol $A \otimes B$ means A holds and simultaneously B holds, symbol $A \oplus B$ means A or B holds. Symbol $(a = b) > c$ means a takes the value of b and $a > c$. Symbol $A \Rightarrow B$ means conclusion B can be derived from condition A . The union symbol $\cup$ of set operation is also used in this paper.

B. Lemmas

Lemma 1 (See in [8] & [9]). T₃ Tree has the following fundamental properties.

(P1). Every node is an odd integer and every odd integer bigger than 1 must be on the T₃ tree. Odd integer N with $N > 1$ lies on level $\lfloor \log_2 N \rfloor - 1$.

(P2). $N_{(k,j)}$ is calculated by

$$N_{(k,j)} = 2^{k+1} + 1 + 2j, j = 0, 1, \dots, 2^k - 1 \quad (1)$$

Manuscript received December 2, 2018; revised March 14, 2019.

The authors are with Department of Mechatronic Engineering, Foshan University, Foshan, PRC and Guangdong Engineering Center of Information Security for Intelligent Manufacturing System, Foshan, China (e-mail: dr.xbang@qq.com; xbwang@fosu.edu.cn).

and thus

$$2^{k+1} + 1 \leq N_{(k,j)} \leq 2^{k+2} - 1 \quad (2)$$

(P3) Multiplication of arbitrary two nodes of T_3 , say $N_{(m,\alpha)}$ and $N_{(n,\beta)}$, is a third node of T_3 . Let $J = 2^m(1+2\beta) + 2^n(1+2\alpha) + 2\alpha\beta + \alpha + \beta$; the multiplication $N_{(m,\alpha)} \times N_{(n,\beta)}$ is given by

$$N_{(m,\alpha)} \times N_{(n,\beta)} = 2^{m+n+2} + 1 + 2J \quad (3)$$

If $J < 2^{m+n+1}$, then $N_{(m,\alpha)} \times N_{(n,\beta)} = N_{(m+n+1,J)}$ lies on level $m+n+1$ of T_3 ; whereas, if $J \geq 2^{m+n+1}$, $N_{(m,\alpha)} \times N_{(n,\beta)} = N_{(m+n+2,\chi)}$ with $\chi = J - 2^{m+n+1}$ lies on level $m+n+2$ of T_3 .

(P4) The biggest node on left branch of the level k is $2^{k+1} + 2^k - 1$ whose position is $j = 2^{k-1} - 1$, and the smallest node on the right branch of the level k is $2^{k+1} + 2^k + 1$ whose position is $j = 2^{k-1}$.

Lemma 2 (See in [17]). Let $N > 3$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$; then $\lfloor \sqrt{N} \rfloor \triangleq \lfloor \frac{k-1}{2} \rfloor$. Particularly,

$$\left(\lfloor \sqrt{N} \rfloor \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor \right) \triangleq \left\lfloor \frac{k-1}{2} \right\rfloor \quad \text{when } k \text{ is odd whereas}$$

$$\left(\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor \leq \lfloor \sqrt{N} \rfloor \right) \triangleq \left\lfloor \frac{k-1}{2} \right\rfloor \quad \text{when } k \text{ is even.}$$

Lemma 3 (See in [19]). Let $(N = pq) > 128$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$, where divisors p and q satisfy $1 < p < q$ and $1 < \frac{q}{p} = \alpha < 2$; then p and q lie on the same level or on two adjacent levels.

(2) At least one of p and q lies on the same level as where $\lfloor \sqrt{N} \rfloor$ is clamped.

(3) If $k > 2$ then

$$\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \left\lfloor \frac{k+1}{2} \right\rfloor - 2$$

In general, for arbitrary positive integer M and $k > 0$ it holds

$$M \triangleq k \Rightarrow \begin{cases} \left\lfloor \frac{M}{2} \right\rfloor \triangleq k-1 \\ 2M \triangleq k+1 \end{cases}$$

(4) There are 3 possible cases in term of the levels on which p and q lie, which are given by

$$\begin{cases} (p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \\ (p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \\ (p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor) \end{cases}$$

(5) There always exists a subdivision of the interval $[2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]$ into 6 subintervals I_1, I_2, I_3, I_4, I_5 and I_6 that satisfy

$$[2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1] = I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5 \cup I_6$$

by means of which holds one of the three cases,

$$p \triangleq I_2 \otimes (q \triangleq I_3 \oplus q \triangleq I_4) \quad , \quad (p \leq \sqrt{N} \leq q) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \quad \text{and}$$

$$p \triangleq I_4 \otimes (q \triangleq I_5 \oplus q \triangleq I_6) .$$

If $1 < \frac{q}{p} < \sqrt{2}$, the 6 subintervals can be given by

$$I_1 = [2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor + 1], I_2 = \left[\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 1 \right]$$

$$I_3 = [2^{\lfloor \frac{k+1}{2} \rfloor} + 1, \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1], I_4 = \left[\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1 \right]$$

$$I_5 = [2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1, \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor + 1], I_6 = \left[\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1 \right]$$

If $1 < \frac{q}{p} < \frac{3}{2}$, they are given by

$$I_1 = [2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1]$$

$$I_2 = [2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 1]$$

$$I_3 = [2^{\lfloor \frac{k+1}{2} \rfloor} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1]$$

$$I_4 = [2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1]$$

$$I_5 = [2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1]$$

$$I_6 = [2^{\lfloor \frac{k+1}{2} \rfloor + 3} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]$$

and when $1 < \frac{q}{p} < 2$, they given by

$$I_1 = [2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1]$$

$$I_2 = [2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 1]$$

$$I_3 = [2^{\lfloor \frac{k+1}{2} \rfloor} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1]$$

$$I_4 = [2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1]$$

$$I_5 = [2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1]$$

$$I_6 = [2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]$$

Lemma 4 (See in [19]). Let $N = pq$ be a node of T_3 and

$(k = \lfloor \log_2 N \rfloor - 1) > 2$, where $1 < p < q$ and $1 < \frac{q}{p} < 2$. Then

$$\left(\lfloor \sqrt{N} \rfloor < 2^{\lfloor \frac{k+1}{2} \rfloor} + 1 \right) \oplus \left(\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1 \right) \otimes \left(\lfloor \sqrt{N} \rfloor \nmid N \right)$$

$$\Rightarrow p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \otimes q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$$

$$\left(\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1 \right) \otimes \left(\lfloor \sqrt{N} \rfloor \mid N \right)$$

$$\Rightarrow (p = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \otimes ((q = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \oplus (q = 2^{\lfloor \frac{k+1}{2} \rfloor + 3})) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$$

$$\left(\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1 \right) \otimes \left(\lfloor \sqrt{N} \rfloor \mid N \right)$$

$$\Rightarrow (p = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$$

$$\otimes ((q = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \oplus (q = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1)) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor$$

$$(2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1 < \lfloor \sqrt{N} \rfloor) \oplus ((\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \otimes (\lfloor \sqrt{N} \rfloor \nmid N))$$

$$\Rightarrow q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor \otimes p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$$

Lemma 5 (See in [20]). For real numbers x and y , it holds

$$(P31) \quad k \leq 2 \left\lfloor \frac{k+1}{2} \right\rfloor \leq k+1 \text{ with positive integer } k$$

III. QUESTION TO BE SOLVED

Consider a RSA modulus N . Let $k = \lfloor \log_2 N \rfloor - 1$; then N is a node on level k of T_3 . Without loss of generality, assume $N = pq$ with $p = N_{(m,\alpha)}$ and $q = N_{(n,\beta)}$ satisfying $1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} = \chi < 2$; then the Lemma 1 indicates $0 \leq m \leq n \leq m+1$ no matter what m and n are. By Lemmas 2, it always holds $\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ for $(k = \lfloor \log_2 N \rfloor - 1) > 2$ and by Lemma 3, there are 3 possible combinations of $N_{(m,\alpha)}$ and $N_{(n,\beta)}$ as list below.

- (i). $(N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (N_{(n,\beta)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$
- (ii). $(N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (N_{(n,\beta)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$
- (iii). $(N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (N_{(n,\beta)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor)$

It can see that, in the cases (ii) and (iii), $m = \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ while in the case (i) $m = \left\lfloor \frac{k+1}{2} \right\rfloor - 2$. Since the quantity $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$ can be obtained by calculating the level where $\lfloor \sqrt{N} \rfloor$ is clamped, theoretically, one can always find $N_{(m,\alpha)}$ out on the level $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$ in the cases (ii) and (iii). However, it is mandatory to have a criterion in the time the case (i) occurs because, generally speaking, one does not know when the case (i) comes across. Since it always holds $N_{(m,\alpha)} \leq \lfloor \sqrt{N} \rfloor \leq N_{(n,\beta)}$, one can see that, the location where $\lfloor \sqrt{N} \rfloor$ lies might be a reference to judge where $N_{(m,\alpha)}$ lies. Intuitively, in the case (i), $\lfloor \sqrt{N} \rfloor$ might be very close to the leftmost nodes on level $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$ and in the case (iii) it might be very close to the rightmost nodes. Then what is the “very close” means? This leads to the investigation of this paper, as introduced in following sections.

IV. MAIN RESULTS WITH PROOFS

Proposition 1. Let $N = N_{(m,\alpha)} \times N_{(n,\beta)}$ be a node of T_3 with

$$1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < 2 \text{ and } k = \lfloor \log_2 N \rfloor - 1; \text{ then}$$

$$(k > 2) \otimes (N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (N_{(n,\beta)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$$

$$\Rightarrow 2^{\lfloor \frac{k+1}{2} \rfloor} \leq \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$$

Proof. Since N is on level k , it holds $N \geq 2^{k+1} + 1$. By Lemma 2, $\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$. Then referring to the following deductions

$$N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \Rightarrow N_{(m,\alpha)} \leq 2^{\lfloor \frac{k+1}{2} \rfloor} - 1$$

$$\Rightarrow N_{(n,\beta)} = \frac{N}{N_{(m,\alpha)}} \geq \frac{2^{k+1} + 1}{2^{\lfloor \frac{k+1}{2} \rfloor} - 1}$$

$$\geq \frac{2^{\lfloor \frac{k+1}{2} \rfloor} - 1 + 2}{2^{\lfloor \frac{k+1}{2} \rfloor} - 1} = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1 + \frac{2}{2^{\lfloor \frac{k+1}{2} \rfloor} - 1}$$

it knows $N_{(n,\beta)} \geq 2^{\lfloor \frac{k+1}{2} \rfloor} + 1 + \frac{2}{2^{\lfloor \frac{k+1}{2} \rfloor} - 1}$; and thus

$N_{(n,\beta)} \geq 2^{\lfloor \frac{k+1}{2} \rfloor} + 1$ when $k > 2$. By $\lfloor \sqrt{N} \rfloor \leq N_{(n,\beta)}$, it knows $2^{\lfloor \frac{k+1}{2} \rfloor} + 1$ is the maximal value of $\lfloor \sqrt{N} \rfloor$, that is,

$$\lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor} + 1 \quad (4)$$

Accordingly, by $\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ it knows

$$2^{\lfloor \frac{k+1}{2} \rfloor} \leq \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \quad (5)$$

Since $N_{(m,\alpha)} < N_{(n,\beta)}$, by Lemma 4, it knows the proposition holds.

Proposition 2. Let $N = N_{(m,\alpha)} \times N_{(n,\beta)}$ be a node of T_3 with $1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < 2$ and $k = \lfloor \log_2 N \rfloor - 1$; then

$$(k > 2) \otimes (N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (N_{(n,\beta)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$$

$$\Rightarrow 2^{\lfloor \frac{k+1}{2} \rfloor} + 1 \leq \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1$$

Proof. By Lemma 3, $1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < 2 \Rightarrow \lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$. The smallest composite non-square integer N whose two divisors are on level $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$ is given by

$$N = (2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \times (2^{\lfloor \frac{k+1}{2} \rfloor} + 3) = (2^{\lfloor \frac{k+1}{2} \rfloor} + 2)^2 - 1$$

which yields

$$2^{\lfloor \frac{k+1}{2} \rfloor} + 1 < \sqrt{N} < 2^{\lfloor \frac{k+1}{2} \rfloor} + 2$$

and thus

$$\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \quad (6)$$

The biggest composite non-square integer N whose two divisors are on level $\lfloor \frac{k+1}{2} \rfloor - 1$ is given by

$$N = (2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \times (2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3) = (2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 2)^2 - 1$$

which leads to

$$\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1 \quad (7)$$

Accordingly, the proposition holds.

Proposition 3. Let semiprime $N > 128$, $k = \lfloor \log_2 N \rfloor - 1$,

$$eI_4^{\sqrt{2}} = \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1, \quad eI_4^{1.5} = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1 \quad \text{and} \quad eI_4^2 = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1; \text{ then}$$

$$\begin{aligned} & (N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (N_{(n,\beta)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor) \\ \Rightarrow & \begin{cases} eI_4^{\sqrt{2}} \leq \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1, 1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < \sqrt{2} \\ eI_4^{1.5} \leq \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1, 1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < 1.5 \\ eI_4^2 \leq \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1, 1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < 2 \end{cases} \end{aligned}$$

Proof. $N > 128 \Rightarrow k = \lfloor \log_2 N \rfloor - 1 > 6$. Then referring to the proof of Proposition 1, it knows $\lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1 \leq N_{(n,\beta)}$. By $\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$, it knows

$$\lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1$$

Meanwhile, by Lemma 3 it knows, $eI_4^{\sqrt{2}} \leq N_{(m,\alpha)} \leq \lfloor \sqrt{N} \rfloor$ when $1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < \sqrt{2}$, $eI_4^{1.5} \leq N_{(m,\alpha)} \leq \lfloor \sqrt{N} \rfloor$ when $1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < 1.5$ and $eI_4^2 \leq N_{(m,\alpha)} \leq \lfloor \sqrt{N} \rfloor$ when $1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < 2$,

Theorem 2. Let $N = N_{(m,\alpha)} \times N_{(n,\beta)}$ be a node of T3 with

$$1 < \frac{N_{(n,\beta)}}{N_{(m,\alpha)}} < 2 \quad \text{and} \quad k = \lfloor \log_2 N \rfloor - 1; \text{ then}$$

$$\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} \Rightarrow (N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (N_{(n,\beta)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$$

$$(\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1}) \otimes (\lfloor \sqrt{N} \rfloor \nmid N)$$

$$\Rightarrow (N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (N_{(n,\beta)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$$

$$(\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1}) \otimes (\lfloor \sqrt{N} \rfloor \mid N)$$

$$\Rightarrow (N_{(m,\alpha)} = 2^{\lfloor \frac{k+1}{2} \rfloor + 1})$$

$$\otimes ((N_{(n,\beta)} = 2^{\lfloor \frac{k+1}{2} \rfloor + 1}) \oplus (N_{(n,\beta)} = 2^{\lfloor \frac{k+1}{2} \rfloor + 3})) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$$

and

$$2^{\lfloor \frac{k+1}{2} \rfloor + 1} < \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1 \Rightarrow N_{(m,\alpha)} \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$$

Proof. Summarizing the conclusions in Lemma 4, Proposition 1, Proposition 2 and Proposition 3 immediately result in Theorem 2.

V. NUMERICAL EXPERIMENT IN MATHEMATICA

With Mathematica, numerical experiment is easily made by testing distributions of $\lfloor \sqrt{N} \rfloor$, $N_{(m,\alpha)}$ and $N_{(n,\beta)}$. For a given semiprime whose divisor-ratio is smaller than 2, the experiment first calculates the level k where N locates and the level where $\lfloor \sqrt{N} \rfloor$ is clamped, then judge if $2^{\lfloor \frac{k+1}{2} \rfloor} \leq \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ and then if $\lfloor \sqrt{N} \rfloor \mid N$ in the case $\lfloor \sqrt{N} \rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$, in the end it explores where $N_{(m,\alpha)}$ lies. The Mathematica programs are list as follows

```

flsqrt[N_] := Floor[Sqrt[N]];
kl[N_] := Floor[Log[N]] - 1; (*levelofN*)
k2[N_] := Floor[Log[Floor[Sqrt[N]] + 0.1]] - 1;
(*levelofSqrt[N]*)
cmpl[N_] := 2^Floor[Log[N]] / 2;
cmp2[N_] := 2^Floor[Log[N]] / 2 + 1;
inData = {1517, 16637, 66049, 809933, 2129189};
r1 = Table[inData[[i]], {i, 5}]; (*N*)
r2 = Table[flsqrt[inData[[i]]], {i, 5}]; (*Sqrt(N)*)
r3 = Table[kl[inData[[i]]], {i, 5}];
r4 = Table[k2[inData[[i]]], {i, 5}];
r5 = Table[cmpl[inData[[i]]], {i, 5}];
r6 = Table[cmp2[inData[[i]]], {i, 5}];
t = {r1, r2, r3, r4, r5, r6} // MatrixForm
    
```

and the computational results are list in Table I, whose screenshot is as Fig. 1.

TABLE I: NUMERICAL EXPERIMENT IN MATHEMATICA

N	N in T_3	$\lfloor \sqrt{N} \rfloor$ & its level	$2^{\lfloor \frac{k+1}{2} \rfloor} \leq \lfloor \sqrt{N} \rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$	$N_{(m,\alpha)}$
1517	$N_{(9,246)}$	$\lfloor \sqrt{1517} \rfloor = 38 \triangleq 4$	$k = 9, 2^4 + 1 = 33 < \lfloor \sqrt{N} \rfloor$	$37 = N_{(4,2)}$
16637	$N_{(13,4222)}$	$\lfloor \sqrt{16637} \rfloor = 128 \triangleq 6$	$k = 13, 2^6 = 128 = \lfloor \sqrt{N} \rfloor$	$127 = N_{(5,31)}$
66049	$N_{(15,16640)}$	$\lfloor \sqrt{66049} \rfloor = 257 \triangleq 7$	$k = 15, 2^7 + 1 = 257 = \lfloor \sqrt{N} \rfloor$	$257 = N_{(7,0)}$
809933	$N_{(18,142822)}$	$\lfloor \sqrt{809933} \rfloor = 899 \triangleq 8$	$k = 18, 2^8 + 1 = 513 < \lfloor \sqrt{N} \rfloor$	$829 = N_{(8,158)}$
2129189	$N_{(20,10018)}$	$\lfloor \sqrt{2129189} \rfloor = 1459 \triangleq 9$	$k = 20, 2^9 + 1 = 1025 < \lfloor \sqrt{N} \rfloor$	$1063 = N_{(9,19)}$

```

flsqr[N] := Floor[Sqrt[N]];
k1[N] := Floor[Log[N] / Log[2]] - 1; (*level of N*)
k2[N] := Floor[Log[Floor[Sqrt[N]] + 0.1] / Log[2]] - 1;
(*level of Sqrt[N]*)
cmp1[N] := 2^Floor[Floor[Log[N] / Log[2]]];
cmp2[N] := 2^Floor[Floor[Log[N] / Log[2]]] + 1;
inData = {1517, 16 637, 66 049, 809 933, 2 129 189};
r1 = Table[inData[[i]], {i, 5}]; (*N*)
r2 = Table[flsqr[inData[[i]]], {i, 5}]; (*Sqrt(N)*)
r3 = Table[k1[inData[[i]]], {i, 5}];
r4 = Table[k2[inData[[i]]], {i, 5}];
r5 = Table[cmp1[inData[[i]]], {i, 5}];
r6 = Table[cmp2[inData[[i]]], {i, 5}];
t = {r1, r2, r3, r4, r5, r6} // MatrixForm

```

Out[224]//MatrixForm=

1517	16 637	66 049	809 933	2 129 189
38	128	257	899	1459
9	13	15	18	20
4	6	7	8	9
32	128	256	512	1024
33	129	257	513	1025

Fig. 1. Screenshot of the programs and output.

VI. CONCLUSION

The quantity $\lfloor \sqrt{N} \rfloor$ is surely a very important cut-off quantity between the small divisor and the big divisor of a composite integer. Since odd integers are positioned level-by-level, it is necessary to make clear how $\lfloor \sqrt{N} \rfloor$ affects the distribution of a semiprime's divisors because it is a computable quantity. The study of this paper gives certain results that are helpful to judge if a small divisor of a semiprime on certain level, but the results may be more improvable. Hope it is improved in the future.

ACKNOWLEDGEMENT

The research work is supported by the State Key Laboratory of Mathematical Engineering and Advanced Computing under Open Project Program No.2017A01, the Youth Innovative Talents Project (Natural Science) of Education Department of Guangdong Province under grant 2016KQNCX192, 2017KQNCX230. The authors sincerely present thanks to them all.

REFERENCES

- [1] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *Notices of the American Mathematical Society*, vol. 46, no. 2, pp. 203-213, 1999.
- [2] Y. Y. Song, *Cryptanalytic Attacks on RSA*, Springer-Verlag New York Inc, 2008.

- [3] K. Aoki, "Advances in integer factoring technique: The way to factor RSA-768," *Ipsj Magazine*, vol. 51, pp. 1030-1038, 2010.
- [4] A. Kruppa and P. Leyland, "Number field sieve for factoring," *Encyclopedia of Cryptography and Security*, pp. 862-867, 2011.
- [5] A. W. Wanambisi, S. Aywa, C. Maende, et al., "Advances in composite integer factorization," *Materials & Structures*, vol. 48, no. 5, pp. 1-12, 2013.
- [6] M. S. Lambert, T. T. Mariam, and F. H. Susan, *RSA*, Betascript Publishing, 2013.
- [7] G. C. Kessler, "An overview of cryptography," *ERAU Scholarly Commons*, 2016.
- [8] X. B. Wang, "Valuated binary tree: A new approach in study of integers," *International Journal of Scientific and Innovative Mathematical Research*, vol. 4, no. 3, pp. 63-67, 2016.
- [9] X. B. Wang, "T3 tree and its traits in understanding integers," *Advances in Pure Mathematics*, vol. 8, no. 5, pp. 494-507, 2018.
- [10] X. B. Wang, "Amusing properties of odd numbers derived from valuated binary tree," *IOSR Journal of Mathematics*, vol. 12, no. 6, pp. 53-57, 2016.
- [11] X. B. Wang, "Genetic traits of odd numbers with applications in factorization of integers," *Global Journal of Pure and Applied Mathematics*, vol. 13, no. 2, pp. 493-517, 2017.
- [12] X. B. Wang, "Strategy for algorithm design in factoring RSA numbers," *IOSR Journal of Computer Engineering*, vol. 19, no. 3-ver.II, pp. 1-7, 2017.
- [13] D. B. Fu, "A parallel algorithm for factorization of big odd numbers," *IOSR Journal of Computer Engineering*, vol. 19, no.2- Ver-V, pp. 51-54, 2017.
- [14] J. H. Li, "A parallel probabilistic approach to factorize a semiprime," *American Journal of Computational Mathematics*, vol. 8, no. 2, pp. 153-162, 2018.
- [15] X. B. Wang, "Influence of divisor-ratio to distribution of semiprime's divisor," *Journal of Mathematics Research*, vol. 10, no. 4, pp. 54-61, 2018.
- [16] G. Chen and J. Li, "Brief investigation on square root of a node of T3 tree," *Advances in Pure Mathematics*, vol. 8, no. 7, pp. 666-671, 2018.
- [17] X. B. Wang, "More on square and square root of a node on T3 tree," *International Journal of Mathematics and Statistics Study*, vol. 6, no. 3, pp. 1-7, 2018.
- [18] X. B. Wang, "Some inequalities on T3 tree," *Advances in Pure Mathematics*, vol. 8, no. 8, pp. 711-719, 2018.
- [19] X. B. Wang, "Traits of a RSA modulus on T3 tree," *Journal of Mathematics Research*, vol. 10, no. 6, pp. 10-20, 2018.
- [20] X. B. Wang, "Brief summary of frequently-used properties of the floor function," *IOSR Journal of Mathematics*, vol. 13, no. 5, pp. 46-48, 2017.

Xingbo Wang was born in Hubei, China. He got his master and doctor's degree at National University of Defense Technology of China and had been a staff in charge of researching and developing CAD/CAM/NC technologies in the university. Since 2010, he has been a professor in Foshan University with research interests in computer application and information security. He is now the chief of Guangdong engineering center of information security for intelligent manufacturing system. Prof. Wang was in charge of more than 40 projects including projects from the National Science Foundation Committee, published 8 books and over 90 papers related with mathematics, computer science and mechatronic engineering, and invented 30 more patents in the related fields.

Yanjie Miao is a student. She was born in Henan, She graduated from Henan Institute of Science and Technology with a bachelor's degree and became a graduate student of Foshan University in 2017. Now her major is mechanical and electronic engineering.