Distribution of RSA Number's Divisor on T3 Tree

Xingbo Wang and Hongqiang Guo

Abstract—**The article investigates the detail distribution of RSA modulus' small divisor in the T3 tree in terms of the divisor-ratio. It proves that, the distribution of the small divisor in T3 tree is completely determined by the divisor-ratio and the parity of the level where the RSA modulus lies, the small divisor of a RSA modulus lying on an even level lies on the same level as where the square root of the modulus is clamped, whereas that of a modulus on an odd level possibly lies on the same level or the higher adjacent level of the square root. Through mathematical induction, it shows that a smaller divisor-ratio results in a closer position of the small divisor to the square root of a RSA modulus.**

Index Terms—**Cryptography, RSA modulus, divisor ratio, binary tree.**

I. Introduction

The RSA modulus, which is also called a RSA number, is a big semiprime composed of two distinct prime divisors, say p and q with $3 \le p < q$ such that $1 < q/p < \sqrt{2}$, according to the American Digital Signature Standard (DSS) [1]. As stated in [2], the RSA numbers have been essentially important in cryptography ever since the RSA public cryptosystem was established. It is believed that, a systematic theory or method that can factorize the RSA numbers means the failure of the RSA public cryptosystem. Thus factorization of the RSA numbers has been a dream filled with fantasies of researchers and engineers working on information security. Nevertheless, the list of unfactroized RSA numbers gets longer and longer on the bulletin.

Recently, a $\boldsymbol{T}_3$-tree approach has revealed activities in studying the integers. The approach originates from paper [3], followed by a series of papers, as list in the references from [4]-[13].

In the paper [13], a theorem, which was marked with Proposition 1 in the paper, was proved to show the scopes of the divisors p and q in accordance with the variation of the divisor-ratio by $1 < q/p < \sqrt{2}$, $1 < q/p < 1.5$ and $1 < q/p < 2$. The paper also proposed three interval-subdivisions that could indicate which subinterval the two divisors lie in. However, that paper was lack of mathematical analysis to show why the proposed subdivision should be those ones. It seemed that the proposed subdivisions were coming suddenly from the heaven and accordingly a question whether there is better one is naturally asked by readers. To make it clear, this paper proves in detail where the small divisor of a RSA modulus should be in a $\boldsymbol{T}_3$ tree, and thereby provides theoretically foundations to the results in paper [13].

Manuscript received December 5, 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).

II. Helpful Hints

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 terms respectively; an integer x is said to *be clamped* in S if $s_0 \le x \le s_n$. Symbol $x \triangleq S$ 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 $x-1 < \lfloor x \rfloor \le x$, or equivalently $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$. Let $N = pq$ be an odd integer with $1 < p < q$; then $k = \dfrac{q}{p}$ is called the *divisor-ratio* of *N*.

In this whole paper, symbol $\boldsymbol{T}_3$ is the $\boldsymbol{T}_3$ tree that was introduced in [3], [7] and symbol $N_{(k,j)}$ is by default the node at position j on level k of $\boldsymbol{T}_3$, where $k \ge 0$ and $0 \le j \le 2^k - 1$. 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 $\boldsymbol{T}_3$ if $2^{k+1} \le X \le 2^{k+2} - 1$ and symbol $X \triangleq k$ indicates X is clamped on level k. An odd integer O satisfying $2^{k+1} + 1 \le O \le 2^{k+2} - 1$ is said to be on level k of T_3, and use symbol $O \urcorner k$ to express it. Symbol $(p \overset{\circ}{=} q) = k$ means integers p and q are on the same level k or clamped on the same level k. 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.

B. Lemmas

Lemma 1 (See in [3] & [7]). $\boldsymbol{T}_3$ Tree has the following fundamental properties.

(**P1**). Every node is an odd integer and every odd integer bigger than 1 must be on the T_3 tree. Odd integer N with N>1 lies on level $\lfloor \log_2 N \rfloor - 1$.

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

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

and thus

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

(**P3**) The biggest node on level k of the left branch is $2^{k+1}+2^{k}-1$ whose position is $j=2^{k-1}-1$, and the smallest node on level k of the right branch is $2^{k+1}+2^{k}+1$ whose position is $j=2^{k-1}$. On the same level, there is not a node that is a multiple of another one.

(**P4**) Multiplication of arbitrary two nodes of $\boldsymbol{T}_3$, say $N_{(m,\alpha)}$ and $N_{(n,\beta)}$, is a third node of $\boldsymbol{T}_3$. 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

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

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 $\boldsymbol{T}_3$; 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 $\boldsymbol{T}_3$.

Lemma 2(See in [10]). Let $N>3$ be an odd integer and $k=\lfloor\log_2 N\rfloor-1$; then $\lfloor\sqrt{N}\rfloor\triangleq\left\lfloor\frac{k+1}{2}\right\rfloor-1$. Particularly, $(\lfloor\sqrt{N}\rfloor\leq\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}\sqrt{2}\right\rfloor)\triangleq\left\lfloor\frac{k+1}{2}\right\rfloor-1$ when k is odd, whereas $(\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}\sqrt{2}\right\rfloor\leq\lfloor\sqrt{N}\rfloor)\triangleq\left\lfloor\frac{k+1}{2}\right\rfloor-1$ when k is even.

Lemma 3(See in [13]). Let $N=pq$ be an odd integer with $1<p<q$ and $1<\frac{q}{p}<\chi$; then

$$\left\lfloor\frac{3-\chi}{2}\sqrt{N}\right\rfloor<p\leq\lfloor\sqrt{N}\rfloor\otimes\lfloor\sqrt{N}\rfloor\leq q\leq\left\lfloor\frac{\chi+1}{2}\sqrt{N}\right\rfloor$$

where $\lfloor x\rfloor=0$ if $x\leq 0$.

Particularly, when $\chi=2$, it yields

$$\left\lfloor\frac{\sqrt{N}}{2}\right\rfloor<p\leq\lfloor\sqrt{N}\rfloor\otimes\lfloor\sqrt{N}\rfloor\leq q\leq\left\lfloor\frac{3}{2}\sqrt{N}\right\rfloor$$

when $\chi=\frac{3}{2}$, it yields

$$\left\lfloor\frac{3}{4}\sqrt{N}\right\rfloor<p\leq\lfloor\sqrt{N}\rfloor\otimes\lfloor\sqrt{N}\rfloor\leq q\leq\left\lfloor\frac{5}{4}\sqrt{N}\right\rfloor$$

and when $\chi=\sqrt{2}$ it holds

$$\left\lfloor(1-\frac{\sqrt{2}-1}{2})\sqrt{N}\right\rfloor<p\leq\lfloor\sqrt{N}\rfloor\otimes\lfloor\sqrt{N}\rfloor\leq q\leq\left\lfloor\frac{\sqrt{2}+1}{2}\sqrt{N}\right\rfloor$$

Lemma 4 (**See in [14]**). For real numbers *x* and *y*, it holds

(**P13**) $x\leq y\Rightarrow\lfloor x\rfloor\leq\lfloor y\rfloor$

(**P14**) $\lfloor n+x\rfloor=n+\lfloor x\rfloor$

Lemma 5 (See in [15]). Let α and x be a positive real numbers; then it holds

$$\alpha\lfloor x\rfloor-1<\lfloor\alpha x\rfloor<\alpha(\lfloor x\rfloor+1)$$

Particularly, if α is a positive integer, say $\alpha=n$, then it yields

$$n\lfloor x\rfloor\leq\lfloor nx\rfloor\leq n(\lfloor x\rfloor+1)-1$$

III. Main Results and Proofs

Proposition 1. Let $N>3$ be an odd integer and $k=\lfloor\log_2 N\rfloor-1$; then

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

when *k* is even, whereas

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

when *k* is odd.

Proof. Direct calculation yields

$$2^{k+1}<N<2^{k+2}\Rightarrow 2^{\frac{k+1}{2}}<\sqrt{N}<2^{\frac{k+2}{2}}$$
$$\Rightarrow 2^{\frac{k+1}{2}-1}<\frac{\sqrt{N}}{2}<2^{\frac{k+2}{2}-1}$$

By Lemma 4 (P13) it holds

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

Let $2^{\frac{k+1}{2}-1}=B$; then $2^{\frac{k+2}{2}-1}=B\sqrt{2}$ and thus

$$\lfloor B\rfloor\leq\left\lfloor\frac{\sqrt{N}}{2}\right\rfloor\leq\lfloor B\sqrt{2}\rfloor\tag{3}$$

Let $\frac{k+1}{2}-\left\lfloor\frac{k+1}{2}\right\rfloor=\varepsilon$; then $\varepsilon=0$ when k is odd and $\varepsilon=0.5$ when *k* is even. By Lemma 4 (P14), it holds

$$\lfloor B\rfloor-2^{\left\lfloor\frac{k+1}{2}\right\rfloor}=\left\lfloor B-2^{\left\lfloor\frac{k+1}{2}\right\rfloor}\right\rfloor=\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(2^{\varepsilon-1}-1)\right\rfloor\tag{4}$$

and

$$\lfloor B\sqrt{2}\rfloor-2^{\left\lfloor\frac{k+1}{2}\right\rfloor}=\left\lfloor B\sqrt{2}-2^{\left\lfloor\frac{k+1}{2}\right\rfloor}\right\rfloor=\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(2^{\varepsilon-\frac{1}{2}}-1)\right\rfloor\tag{5}$$

Now suppose *k* is even; then (4) becomes

$$\lfloor B\rfloor-2^{\left\lfloor\frac{k+1}{2}\right\rfloor}=\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(2^{0.5-1}-1)\right\rfloor$$
$$=\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(\frac{\sqrt{2}}{2}-1)\right\rfloor\geq\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(\frac{1}{2}-1)\right\rfloor=-2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1}$$

and (5) becomes

$$\lfloor B\sqrt{2}\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} = \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{\frac{1}{2}-\frac{1}{2}}-1)\right\rfloor = 0$$

which says an even k yields

$$2^{\lfloor\frac{k+1}{2}\rfloor} - 2^{\lfloor\frac{k+1}{2}\rfloor-1} \le \left\lfloor\frac{\sqrt{N}}{2}\right\rfloor \le 2^{\lfloor\frac{k+1}{2}\rfloor} \tag{6}$$

If k is odd; then (4) becomes

$$\lfloor B\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} = \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{0-1}-1)\right\rfloor = -2^{\lfloor\frac{k+1}{2}\rfloor-1} \tag{7}$$

and (5) becomes

$$\begin{aligned}\lfloor B\sqrt{2}\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{0-\frac{1}{2}}-1)\right\rfloor \\ &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(\frac{\sqrt{2}}{2}-1)\right\rfloor \le \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(\frac{3}{4}-1)\right\rfloor = -2^{\lfloor\frac{k+1}{2}\rfloor-2}\end{aligned} \tag{8}$$

That is, an odd k leads to

$$2^{\lfloor\frac{k+1}{2}\rfloor} - 2^{\lfloor\frac{k+1}{2}\rfloor-1} \le \left\lfloor\frac{\sqrt{N}}{2}\right\rfloor \le 2^{\lfloor\frac{k+1}{2}\rfloor} - 2^{\lfloor\frac{k+1}{2}\rfloor-2} \tag{9}$$

Corollary 1. Let $(N = pq) > 3$ be an odd integer with $1 < \frac{q}{p} < 2$ and $k = \lfloor\log_2 N\rfloor - 1$; then it holds

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

Proof. By Lemma 2, it always holds $\lfloor\sqrt{N}\rfloor \triangleq \left\lfloor\frac{k+1}{2}\right\rfloor - 1$. By Lemma 3, $\left\lfloor\frac{\sqrt{N}}{2}\right\rfloor < p \le \lfloor\sqrt{N}\rfloor$ when $1 < \frac{q}{p} < 2$. By Proposition 1, $\left\lfloor\frac{\sqrt{N}}{2}\right\rfloor \triangleq \left\lfloor\frac{k+1}{2}\right\rfloor - 2$. Consequently, $p \triangleq \left\lfloor\frac{k+1}{2}\right\rfloor - 2 \oplus p \triangleq \left\lfloor\frac{k+1}{2}\right\rfloor - 1$.

Proposition 2. Let $N > 3$ be an odd integer and $k = \lfloor\log_2 N\rfloor - 1$; then

$$2^{\lfloor\frac{k+1}{2}\rfloor} + 2^{\lfloor\frac{k+1}{2}\rfloor-5} \le \left\lfloor\frac{3}{4}\sqrt{N}\right\rfloor \le 2^{\lfloor\frac{k+1}{2}\rfloor} + 2^{\lfloor\frac{k+1}{2}\rfloor-1} \tag{10}$$

when k is even, whereas

$$2^{\lfloor\frac{k+1}{2}\rfloor} - 2^{\lfloor\frac{k+1}{2}\rfloor-2} \le \left\lfloor\frac{3}{4}\sqrt{N}\right\rfloor \le 2^{\lfloor\frac{k+1}{2}\rfloor} + 2^{\lfloor\frac{k+1}{2}\rfloor-4} \tag{11}$$

when k is odd.

Proof. Direct calculation yields

$$\begin{aligned}&2^{k+1} < N < 2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}} \\ &\Rightarrow 2^{\frac{k+1}{2}-2}(2+1) < \frac{3}{4}\sqrt{N} < 2^{\frac{k+2}{2}-2}(2+1) \\ &\Rightarrow 2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} < \frac{3}{4}\sqrt{N} < 2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2}\end{aligned}$$

By Lemma 4 (P13) it holds

$$\left\lfloor 2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2}\right\rfloor \le \left\lfloor\frac{3}{4}\sqrt{N}\right\rfloor \le \left\lfloor 2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2}\right\rfloor$$

Let $2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} = \Lambda$; then $2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} = \Lambda\sqrt{2}$ and thus

$$\lfloor\Lambda\rfloor \le \left\lfloor\frac{3}{4}\sqrt{N}\right\rfloor \le \lfloor\Lambda\sqrt{2}\rfloor \tag{12}$$

Note that, by Lemma 4 (P14), it holds

$$\lfloor\Lambda\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} = \left\lfloor\Lambda - 2^{\lfloor\frac{k+1}{2}\rfloor}\right\rfloor = \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{\varepsilon-1} + 2^{\varepsilon-2} - 1)\right\rfloor \tag{13}$$

and

$$\lfloor\Lambda\sqrt{2}\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} = \left\lfloor\Lambda\sqrt{2} - 2^{\lfloor\frac{k+1}{2}\rfloor}\right\rfloor = \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{\varepsilon-\frac{1}{2}} + 2^{\varepsilon-\frac{3}{2}} - 1)\right\rfloor \tag{14}$$

By $\frac{3\sqrt{2}}{4} - 1 > \frac{1}{32}$, it can see by Lemma 5 that, when $k > 0$ is even

$$\begin{aligned}\lfloor\Lambda\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{0.5-1} + 2^{0.5-2} - 1)\right\rfloor \\ &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(\frac{1}{\sqrt{2}} + \frac{1}{2\sqrt{2}} - 1)\right\rfloor = \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(\frac{3\sqrt{2}}{4} - 1)\right\rfloor \ge 2^{\lfloor\frac{k+1}{2}\rfloor-5}\end{aligned}$$

and

$$\begin{aligned}\lfloor\Lambda\sqrt{2}\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{\frac{1}{2}-\frac{1}{2}} + 2^{\frac{1}{2}-\frac{3}{2}} - 1)\right\rfloor \\ &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(1 + \frac{1}{2} - 1)\right\rfloor = 2^{\lfloor\frac{k+1}{2}\rfloor-1}\end{aligned}$$

Thereby an even k yields

$$2^{\lfloor\frac{k+1}{2}\rfloor} + 2^{\lfloor\frac{k+1}{2}\rfloor-5} \le \left\lfloor\frac{3}{4}\sqrt{N}\right\rfloor \le 2^{\lfloor\frac{k+1}{2}\rfloor} + 2^{\lfloor\frac{k+1}{2}\rfloor-1} \tag{15}$$

On the other hand, when $k > 2$ is odd

$$\begin{aligned}\lfloor\Lambda\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{0-1} + 2^{0-2} - 1)\right\rfloor \\ &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(\frac{1}{2} + \frac{1}{4} - 1)\right\rfloor = \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(\frac{3}{4} - 1)\right\rfloor \\ &= -2^{\lfloor\frac{k+1}{2}\rfloor-2}\end{aligned}$$

and

$$\begin{aligned}\lfloor\Lambda\sqrt{2}\rfloor - 2^{\lfloor\frac{k+1}{2}\rfloor} &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(2^{0-\frac{1}{2}} + 2^{0-\frac{3}{2}} - 1)\right\rfloor \\ &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(\frac{1}{\sqrt{2}} + \frac{1}{2\sqrt{2}} - 1)\right\rfloor \\ &= \left\lfloor 2^{\lfloor\frac{k+1}{2}\rfloor}(\frac{3\sqrt{2}}{4} - 1)\right\rfloor\end{aligned}$$

Since $\frac{1}{32} < \frac{3\sqrt{2}}{4} - 1 < \frac{1}{16}$, it holds

$$\lfloor \Lambda\sqrt{2} \rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} \le 2^{\lfloor \frac{k+1}{2} \rfloor - 4}$$

Accordingly an odd k yields

$$2^{\lfloor \frac{k+1}{2} \rfloor} - 2^{\lfloor \frac{k+1}{2} \rfloor - 2} \le \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \le 2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 4} \quad (16)$$

Corollary 2. Let $(N = pq) > 3$ be an odd integer with $1 < \frac{q}{p} < \frac{3}{2}$ and $k = \lfloor \log_2 N \rfloor - 1$; then

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

when k is even, whereas

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

when k is odd.

Proof. By Lemma 2, it always holds $\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$. By Lemma 3, $\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor < p \le \lfloor \sqrt{N} \rfloor$ when $1 < \frac{q}{p} < \frac{3}{2}$. By Proposition 2, $\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when k is even whereas $\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when k is odd.

Proposition 3 Let $N > 3$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$; then

$$2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 3} \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le 2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 2^{\lfloor \frac{k+1}{2} \rfloor - 2} \quad (17)$$

when k is even, whereas

$$2^{\lfloor \frac{k+1}{2} \rfloor} - 2^{\lfloor \frac{k+1}{2} \rfloor - 3} \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le 2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 2^{\lfloor \frac{k+1}{2} \rfloor - 4} \quad (18)$$

when k is odd.

Proof. Direct calculation yields

$$\begin{aligned}
&2^{k+1} < N < 2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}} \\
&\Rightarrow 2^{\frac{k+1}{2}-3}(2^2+2+1) < \frac{7}{8}\sqrt{N} < 2^{\frac{k+2}{2}-3}(2^2+2+1) \\
&\Rightarrow 2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} + 2^{\frac{k+1}{2}-3} < \frac{7}{8}\sqrt{N} < 2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} + +2^{\frac{k+2}{2}-3} \\
&\Rightarrow \left\lfloor 2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} + 2^{\frac{k+1}{2}-3} \right\rfloor \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} + 2^{\frac{k+2}{2}-3} \right\rfloor
\end{aligned}$$

Let $2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} + 2^{\frac{k+1}{2}-3} = \Pi$; then $2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} + 2^{\frac{k+2}{2}-3} = \Pi\sqrt{2}$ and thus

$$\lfloor \Pi \rfloor \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le \lfloor \Pi\sqrt{2} \rfloor \quad (19)$$

Letting $\frac{k+1}{2} - \left\lfloor \frac{k+1}{2} \right\rfloor = \varepsilon$ yields

$$\begin{aligned}
\lfloor \Pi \rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} &= \left\lfloor \Pi - 2^{\lfloor \frac{k+1}{2} \rfloor} \right\rfloor \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(2^{\varepsilon-1} + 2^{\varepsilon-2} + 2^{\varepsilon-3} - 1) \right\rfloor
\end{aligned} \quad (20)$$

and

$$\begin{aligned}
\lfloor \Pi\sqrt{2} \rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} &= \left\lfloor \Pi\sqrt{2} - 2^{\lfloor \frac{k+1}{2} \rfloor} \right\rfloor \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(2^{\varepsilon-\frac{1}{2}} + 2^{\varepsilon-\frac{3}{2}} + 2^{\varepsilon-\frac{5}{2}} - 1) \right\rfloor
\end{aligned} \quad (21)$$

By $\frac{1}{8} < \frac{7\sqrt{2}}{8} - 1 < \frac{1}{4}$, it can see by Lemma 4 (P13) that, when $k > 0$ is even

$$\begin{aligned}
\lfloor \Pi \rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} &= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(2^{0.5-1} + 2^{0.5-2} + 2^{0.5-3} - 1) \right\rfloor \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(\frac{1}{\sqrt{2}} + \frac{1}{2\sqrt{2}} + \frac{1}{2^2\sqrt{2}} - 1) \right\rfloor \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(\frac{7\sqrt{2}}{8} - 1) \right\rfloor \ge 2^{\lfloor \frac{k+1}{2} \rfloor - 3}
\end{aligned}$$

and

$$\begin{aligned}
\lfloor \Pi\sqrt{2} \rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} &= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(2^{\frac{1}{2}-\frac{1}{2}} + 2^{\frac{1}{2}-\frac{3}{2}} + 2^{\frac{1}{2}-\frac{5}{2}} - 1) \right\rfloor \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(\frac{1}{2} + \frac{1}{4}) \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 2^{\lfloor \frac{k+1}{2} \rfloor - 2}
\end{aligned}$$

which says,

$$2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 3} \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le 2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 2^{\lfloor \frac{k+1}{2} \rfloor - 2} \quad (22)$$

When $k > 2$ is odd

$$\begin{aligned}
\lfloor \Pi \rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} &= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(2^{0-1} + 2^{0-2} + 2^{0-3} - 1) \right\rfloor \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} - 1) \right\rfloor = -2^{\lfloor \frac{k+1}{2} \rfloor - 3}
\end{aligned}$$

and

$$\begin{aligned}
\lfloor \Pi\sqrt{2} \rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} &= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(2^{0-\frac{1}{2}} + 2^{0-\frac{3}{2}} + 2^{0-\frac{5}{2}} - 1) \right\rfloor \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(\frac{1}{\sqrt{2}} + \frac{1}{2\sqrt{2}} + \frac{1}{2^2\sqrt{2}} - 1) \right\rfloor = \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}(\frac{7\sqrt{2}}{8} - 1) \right\rfloor
\end{aligned}$$

By $\frac{1}{8} < \frac{7\sqrt{2}}{8} - 1 < \frac{1}{4}$, it knows

$$\lfloor \Pi\sqrt{2} \rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} \le 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$$

Accordingly an odd k yields

$$2^{\lfloor \frac{k+1}{2} \rfloor} - 2^{\lfloor \frac{k+1}{2} \rfloor - 3} \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le 2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 2} \quad (23)$$

Corollary 3. Let $(N = pq) > 3$ be an odd integer with $1 < \frac{q}{p} < \frac{5}{4}$ and $k = \lfloor \log_2 N \rfloor - 1$; then

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

when k is even, whereas

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

when k is odd.

Proof. By Lemma 2, it always holds $\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$. By Lemma 3, $\left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor < p \le \lfloor \sqrt{N} \rfloor$ when $1 < \frac{q}{p} < \frac{5}{4}$. By Proposition 3, $\left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when k is even whereas $\left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when k is odd.

Proposition 4. Let $N > 3$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$ be an odd integer; then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5} \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \quad (24)$$

when k is even, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \quad (25)$$

when k is odd.

Proof. The inequality $\frac{3}{4} < 1 - \frac{\sqrt{2}-1}{2} < \frac{7}{8}$ immediately yields

$$\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \quad (26)$$

When k is even, referring to (15) and (18), it leads to

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5} \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \quad (27)$$

and when k is odd, referring to (16) and (22), it leads to

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \quad (28)$$

Corollary 3. Let $(N = pq) > 3$ be an odd integer with $1 < \frac{q}{p} < \sqrt{2}$ and $k = \lfloor \log_2 N \rfloor - 1$; then

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

when k is even, whereas

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

when k is odd.

Proof. By Lemma 2, it always holds $\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$. By Lemma 3, $\left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor < p \le \lfloor \sqrt{N} \rfloor$ when $1 < \frac{q}{p} < \sqrt{2}$. By Proposition 2, $\left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when k is even whereas $\left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when k is odd.

Theorem 1. For a RSA modulus $N = pq$ with $1 < p < q$, the distribution of divisor p in $\boldsymbol{T}_3$ tree is completely determined by the divisor-ratio $1 < \frac{q}{p} = \chi < 2$ and integer $k = \lfloor \log_2 N \rfloor - 1$. When k is even, there is an χ_0 with $\frac{3}{2} < \chi_0 < 2$ such that $p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when $1 < \frac{q}{p} \le \chi_0$ whereas $p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2$ when $\chi_0 < \frac{q}{p} < 2$. When k is odd, $p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ and the smaller χ is the closer p is to $\lfloor \sqrt{N} \rfloor$.

Proof. A simple summarization of the cases proved in Proposition 1, Proposition 2 and Proposition 3 immediately conclusions of the theorem.

IV. Numerical Experiment in Mathematica

To test the proved conclusions, numerical experiment was made with Mathematica. The experiment first chose randomly semiprime N from the semiprime table, e.g., from *The On-Line Encyclopedia of Integer Sequences (OEIS)*, then located N's level by $k_N = \lfloor \log_2 N \rfloor - 1$, calculated $\lfloor \sqrt{N} \rfloor$ and its level $k_{sn} = \lfloor \log_2 \lfloor \sqrt{N} \rfloor \rfloor - 1$, checked N's smaller divisor p and its level by $k_p = \lfloor \log_2 p \rfloor - 1$, checked the divisor-ratio and judge the consistency to Theorem 1. Mathematica programs are list as follows.

$$flsqrt[N\_] := Floor[Sqrt[N]];$$

$$kn[N\_] := Floor[\frac{Log[N]}{Log[2]}] - 1; (*levelofN*)$$

$$ksn[N\_] := Floor[\frac{Log[Floor[Sqrt[N]] + 0.01]}{Log[2]}] - 1; (*levelofSqrt[N]*)$$

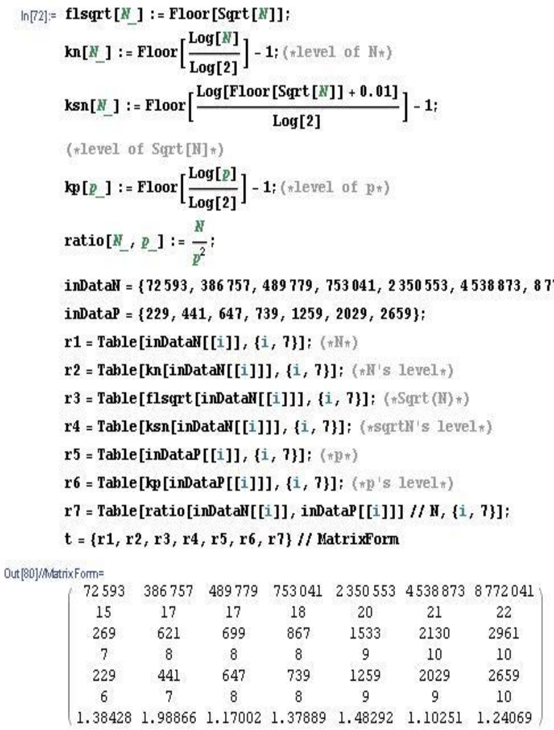
$$kp[p\_] := Floor[\frac{Log[p]}{Log[2]}] - 1; (*levelofp*)$$

$$ratio[N\_, p\_] := \frac{N}{p^2};$$

$inDataN = \{72593, 386757, 489779, 753041, 2350553, 4538873, 8772041\};$
$inDataP = \{229, 441, 647, 739, 1259, 2029, 2659\};$
$r1 = Table[inDataN[[i]], \{i, 7\}]; (*N*)$
$r2 = Table[kn[inDataN[[i]]], \{i, 7\}]; (*N's level*)$
$r3 = Table[flsqrt[inDataN[[i]]], \{i, 7\}]; (*Sqrt(N)*)$
$r4 = Table[ksn[inDataN[[i]]], \{i, 7\}]; (*sqrtN's level*)$
$r5 = Table[inDataP[[i]], \{i, 7\}]; (*p*)$
$r6 = Table[kp[inDataP[[i]]], \{i, 7\}]; (*p's level*)$
$r7 = Table[ratio[inDataN[[i]], inDataP[[i]]] // N, \{i, 7\}];$
$t = \{r1, r2, r3, r4, r5, r6, r7\} // MatrixForm$

TABLE I. NUMERICAL EXPERIMENT IN MATHEMATICA

$N \& k_N$	$\lfloor\sqrt{N}\rfloor \& k_{sn}$	$p \& k_p$	χ
$72593 \triangleq 15$	$269 \triangleq 7$	$229 \triangleq 6$	1.38428
$386757 \triangleq 17$	$621 \triangleq 8$	$441 \triangleq 7$	1.98866
$489779 \triangleq 17$	$699 \triangleq 8$	$647 \triangleq 8$	1.17002
$753041 \triangleq 18$	$867 \triangleq 8$	$739 \triangleq 8$	1.37889
$2350553 \triangleq 20$	$1533 \triangleq 9$	$1259 \triangleq 9$	1.48292
$4538873 \triangleq 21$	$2130 \triangleq 10$	$2029 \triangleq 9$	1.10251
$8772041 \triangleq 22$	$2961 \triangleq 10$	$2659 \triangleq 10$	1.24069



```
In[72]:= flsqrt[N_] := Floor[Sqrt[N]];
kn[N_] := Floor[Log[N]/Log[2]] - 1; (*level of N*)
ksn[N_] := Floor[Log[Floor[Sqrt[N]] + 0.01]/Log[2]] - 1;
(*level of Sqrt[N]*)
kp[p_] := Floor[Log[p]/Log[2]] - 1; (*level of p*)
ratio[N_, p_] := N/p^2;
inDataN = {72593, 386757, 489779, 753041, 2350553, 4538873, 8772041};
inDataP = {229, 441, 647, 739, 1259, 2029, 2659};
r1 = Table[inDataN[[i]], {i, 7}]; (*N*)
r2 = Table[kn[inDataN[[i]]], {i, 7}]; (*N's level*)
r3 = Table[flsqrt[inDataN[[i]]], {i, 7}]; (*Sqrt(N)*)
r4 = Table[ksn[inDataN[[i]]], {i, 7}]; (*sqrtN's level*)
r5 = Table[inDataP[[i]], {i, 7}]; (*p*)
r6 = Table[kp[inDataP[[i]]], {i, 7}]; (*p's level*)
r7 = Table[ratio[inDataN[[i]], inDataP[[i]]] // N, {i, 7}];
t = {r1, r2, r3, r4, r5, r6, r7} // MatrixForm

Out[80]//MatrixForm=
 72593    386757   489779   753041   2350553  4538873  8772041
 15       17       17       18       20       21       22
 269      621      699      867      1533     2130     2961
 7        8        8        8        9        10       10
 229      441      647      739      1259     2029     2659
 6        7        8        8        9        9        10
 1.38428  1.98866  1.17002  1.37889  1.48292  1.10251  1.24069
```

Fig. 1. Screenshot of the programs and output.

The computations of running the programs are shown in Table. The screenshot of the programs and output is shown in Fig. 1. Analyzing the data in Table I, one can see that each one matches to Theorem 1. Take 386757 as an example. It can see that, $386757 \triangleq 17$ thus $k = 17$ is odd. By Theorem 1, the smaller divisor of 386757 possibly lies on level $\left\lfloor \frac{17+1}{2} \right\rfloor - 2 = 7$ or $\left\lfloor \frac{17+1}{2} \right\rfloor - 1 = 8$. Actually, $p = 441 \triangleq 7$ because $\chi = 1.98866 > 1.5$. The fact matches to the theorem. Take 489779 as another example. $489779 \triangleq 17 \otimes (\chi = 1.17002) < 1.5 \Rightarrow (p = 647) \triangleq 8$. For the numbers 753041 and 2350553, their small divisors lie on the levels as expected.

V. CONCLUSION

It is undoubtedly meaningful to know the divisors' range of a RSA modulus. The investigation in this paper discloses the deep relationship between the divisor-ratio and the distribution of the small divisor. The propositions and theorem proved in this paper indicate that, factorization of the RSA numbers may be achieved via a small search on specific level of $\boldsymbol{T}_3$ tree, and the smaller the divisor-ratio is the easier the search will be done. This discovers an opposite direction to the classics thoughts that the smaller the divisor-ratio is the harder is the factorization. Hope future work would be successful in the related researches.

ACKNOWLEDGEMENTS

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] National Institute of Standards and Technology (NIST), Digital signature standard (DSS), *FIPS Publication* 186-3, June 2009.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] X. B. Wang, "Two more symmetric properties of odd numbers," *IOSR Journal of Mathematics*, vol. 13, no. 3 (ver. II), pp. 37-40, 2017.
[7] X. B. Wang, "T3 tree and its traits in understanding integers," *Advances in Pure Mathematics*, vol. 8, no. 5, pp. 494-507, 2018.
[8] G. H. Chen and J. H. Li, "Brief investigation on square root of a node of T3 tree," *Advances in Pure Mathematics*, vol. 8, no. 7, pp. 666-671, 2018.
[9] X. B. Wang, "Some inequalities on T3 tree," *Advances in Pure Mathematics*, vol. 8, no. 8, pp. 711-719, 2018.
[10] 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.
[11] 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.
[12] J. H. Li, "A parallel probabilistic approach to factorize a semiprime," *American Journal of Computational Mathematics*, vol. 8, no. 2, pp. 153-162, 2018.
[13] X. B. Wang, "Traits of a RSA modulus on T3 tree," *Journal of Mathematics Research*, vol. 10, no. 6, pp. 10-20, 2018.
[14] 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.
[15] X. B. Wang, "Some new inequalities with proofs and comments on applications," *Journal of Mathematics Research*, vol. 11, no. 3, pp. 15-19, 2018.

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.

Guo Hongqiang was born in Hebei. He received a bachelor's degree at HeFei University of Technology and became a graduate student of Foshan University in 2017. He is now a member of Guangdong engineering center of information security for intelligent manufacturing system.