JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 34, 721-732 (2018)
DOI: 10.6688/JISE.201805_34(3).0009

# Revisiting the Expansion Length of Triple-base Number System for Elliptic Curve Scalar Multiplication*

YUN-QI DOU[1,2], JIANG WENG[3], CHUAN-GUI MA[4] AND FU-SHAN WEI[1,2]
[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing*
*Zhengzhou, 450001 P.R. China*
[2]*State Key Laboratory of Cryptology*
*Beijing, 100878 P.R. China*
[3]*Information and Navigation College*
*Air Force Engineering University*
*Xi'an, 710077 P.R. China*
[4]*Department of Basic*
*Army Aviation Institution*
*Beijing, 101123 P.R. China*
*E-mail: douyunqi@126.com*

Because of its sparsity, triple-base number system is used to accelerate the scalar multiplication in elliptic curve cryptography. Yu *et al.* presented an estimate for the length of triple-base number system at Africacrypt 2013. However, the efficiency of scalar multiplication is not only associated with the length of representation but also the numbers and costs of doubling, tripling, quintupling and addition. It is necessary to set a restriction for exponents of base 2, 3 and 5, which will lead to longer expansion length. In this situation, we prove a stronger result: the upper bound on expansion length of constrained triple-base number system is still sub-linear. This result provides more practical boundary of the triple-base number system to speed up the scalar multiplication. At the same time, it also generalizes the result of Méloni *et al.* about double-base number system.

***Keywords:*** elliptic curve cryptography, scalar multiplication, constrained triple-base number system, greedy algorithm, sub-linear

## 1. INTRODUCTION

In 1985, Miller [1] and Koblitz [2] independently proposed elliptic curve cryptography (ECC), whose security relies on the computational intractability of elliptic curve discrete logarithm problem (ECDLP). In contrast with the discrete logarithm problem in finite field and the integer factorization problem, there is no known sub-exponential time algorithm to solve the discrete logarithm problem on a well-chosen elliptic curve. Therefore, ECC can offer the same security level as other public key schemes with a much smaller key. Due to the advantage of storage space, processing speed and bandwidth, ECC is now widely used in many application scenarios, such as wireless sensor networks [3], cloud computing [4-7], privacy protection [8, 9] and entity authentication [10, 11]. Scalar multiplication is the core operation in elliptic curve cryptosystems, which involves the computation of $kP$, where $k$ is an integer, and $P$ a point on the elliptic curve. The

Received December 23, 2016; revised May 23, 2017; accepted June 30, 2017.
Communicated by Hung-Min Sun.
* This work is supported by the National Natural Science Foundation of China (No. 61309016, 61379150, 61602512), the Funding of Science and Technology on Information Assurance Laboratory (No. KJ1302) and Key Scientific and Technological Project of Henan Province (No. 122102210126, 092101210502).

calculation speed of scalar multiplication determines the efficiency of elliptic curve cryptosystems. How to accelerate the scalar multiplication algorithm has always been a hot topic of elliptic curve cryptography.

In recent years, double- and multi-base representation of integers have been paid much attention. Double-base number system (DBNS) was first proposed in [12], where an integer $k$ is represented as $k = \sum_{i=1}^{l} 2^{b_i} 3^{t_i}$. Some DBNS representations for an integer are very sparse. Usually, one can use the greedy algorithm to find a fairly sparse DBNS representation. An important theoretical result [13] about DBNS is that for any large integer $k$, the length of representation returned by greedy algorithm is sub-linear. Double-base number system has been used to design fast and low power multiplier [14]. However, DBNS cannot be used directly to elliptic curve scalar multiplication efficiently. In order to use Horner scheme, double-base chain (DBC) was introduced by Dimitrov *et al.* [15]. As a special case of DBNS, double-base chain requires the restriction that $(b_i)$ and $(t_i)$ are decreasing sequences. However, the restriction significantly increases the number of terms of double-base chain. At present, the bound for the DBC is still an open problem, it seems almost sure that the length of the shortest double-base chain is linear [16]. In 2015, Méloni and Hasan [17] designed an efficient scalar multiplication algorithm by combining the double-base number system with Yao algorithm [18]. In order to reduce the computation cost, the authors proposed to set maximum bounds for $(b_i)$ and $(t_i)$. Under reasonable restrictions, they showed the number of terms of DBNS representation is still in $O(\log k/\log\log k)$.

In 2007, Mishra and Dimitrov [19] presented efficient formulas for point quintupling and introduced triple-base number system (TBNS) for computing scalar multiplication more efficiently. Longa *et al.* [20, 21] proposed a multi-base non-adjacent form (mbNAF) to speed up the computation of scalar multiplication. In 2013, Yu *et al.* [22] estimated the number of terms for TBNS and showed that sub-linear bound still holds. However, the efficiency of scalar multiplication is not only associated with the length of representation but also the numbers and costs of doubling, tripling, quintupling and addition. It is important for TBNS speeding up scalar multiplication to select reasonable restriction for exponents of base 2, 3 and 5. Recently, constrained triple-base number system is proposed to accelerate the scalar multiplication in [23]. The authors present two efficient algorithms for situations with and without precomputations. As an intermediate representation between TBNS and triple-base chain, the length of constrained TBNS must be longer than TBNS. The theoretical analysis of the expansion length for constrained TBNS is a number-theoretic problem. The completed proof for the question has not been given.

In this paper, we give an estimate for the length of constrained triple-base representation with bases $\{2, 3, 5\}$ of an integer $k$, which is $O(\log k/\log\log k)$ by the greedy algorithm. The result provides the theoretical basis for selecting optimal parameters and has more practical significance than the result in [22].

The sequel of the paper is organized as follows: In Section 2, some main results about DBNS and TBNS are presented. We review the concept of constrained triple-base number system in Section 2.2. In Section 3, we present a detailed theoretical analysis about the expansion length of constrained triple-base number system. Finally, we conclude the paper in Section 4.

## 2. PRELIMINARIES

### 2.1 Multi-base Representation of an Integer

In this section, we present the concepts of double-base number system and triple-base number system, along with some main properties and results. Details can be found in [19, 24].

**Definition 1 (*S*-integer):** Given a set of primes *S*, an *S*-integer is a positive integer whose prime factors all belong to *S*.

**Definition 2 (DBNS):** Given two relatively prime positive integers $p$ and $q$, the DBNS is a representation scheme of integer in which every integer $k$ is represented as

$$k = \sum_{i=1}^{l} p^{b_i} q^{t_i},$$

with $b_i, t_i \geq 0$. The number of terms $l$ is also called the length of DBNS representation, $p$ and $q$ are usually chosen as 2 and 3 in practice.

The double-base number system is highly redundant, some possible DBNS representations for a given integer are extremely sparse. Although it is always difficult to find the canonical (shortest) representations, one can use greedy algorithm (Algorithm 1) to compute near canonical DBNS expansions.

**Algorithm 1:** Greedy algorithm to compute DBNS representation

Input: a positive integer $k$
Output: $(b_i, t_i)_{i\geq 1}$ such that $k = \sum_{i=1}^{l} 2^{b_i} 3^{t_i}$ with $b_i, t_i \geq 0$
1. $i \leftarrow 1$
2. while $k > 0$ do
3. find $\{2, 3\}$-integer $c = 2^b 3^t$ the best approximation of $k$
4. $b_i \leftarrow b$, $t_i \leftarrow t$, $i \leftarrow i+1$
5. $k \leftarrow |k - c|$
6. end while
7. return $(b_i, t_i)_{i\geq 1}$

**Definition 3 (TBNS):** Given three relatively prime positive integers $p_1$, $p_2$ and $p_3$, the TBNS is a representation scheme of integer in which every integer $k$ is represented as

$$k = \sum_{i=1}^{l} p_1^{b_i} p_2^{t_i} p_3^{e_i},$$

with $b_i, t_i, e_i \geq 0$. Similarly, the number of terms $l$ is also called the length of TBNS representation, $p_1$, $p_2$ and $p_3$ are usually chosen as 2, 3 and 5 respectively in practice. The TBNS representations are sparser and more redundant than the DBNS.

In 1998, Dimitrov *et al.* [13] presented an important theoretical result about DBNS, they gave an estimate for the length of DBNS (See Theorem 1 below).

**Theorem 1:** The greedy Algorithm 1 terminates after $O(\log k/\log\log k)$ steps.

In 2013, Yu *et al.* [22] estimated the number of terms for TBNS and showed that sub-linear bound still holds: the greedy algorithm to compute TBNS representations terminates after $O(\log k/\log\log k)$ steps. Lemma 1 [25] makes analysis of the maximum distance between $S$-integers, the result is used in the proofs of Theorem 1 [13, 22] and Theorem 2 below.

**Lemma 1:** There exist two constants $C, N > 0$ such that when $x > N$, there is an $S$-integer between $x - \frac{x}{(\log x)^C}$ and $x$.

### 2.2 Constrained Triple-Base Number System

**Definition 4 (Constrained TBNS):** Given three relatively prime positive integers $p_1$, $p_2$ and $p_3$, the constrained TBNS is a special TBNS representation scheme, where every integer $k$ is represented as

$$k = \sum_{i=1}^{l} p_1^{b_i} p_2^{t_i} p_3^{e_i} ,$$

with $b_i, t_i, e_i \geq 0$, but meanwhile with the restrictions $b_i \leq b_{\max}$, $t_i \leq t_{\max}$, and $e_i \leq e_{\max}$ for all $i$.

In [23], the authors present efficient algorithms for elliptic curve scalar multiplication using constrained triple-base expansions instead of the triple-base chains. By imposing a maximum bound on $(b_i)$, $(t_i)$ and $(e_i)$, constrained triple-base number system is clearly less restrictive than the TBC condition. Their algorithms outperform DB chain, TB chain and 4-NAF methods. In this paper, we will present a detailed theoretical analysis about the expansion length of constrained TBNS, and demonstrate the length of constrained TBNS is sub-linear in Section 3. We mainly focus on the constrained triple-base number system with $S=\{2, 3, 5\}$. However, the Algorithm 2 and Theorem 2 below can be generalized to other selections of the three bases.

**Algorithm 2:** Greedy algorithm to compute constrained TBNS representation

Input: a positive integer $k$, the exponent restriction $b_{\max}$, $t_{\max}$, $e_{\max}$ of $\{2,3,5\}$

Output: $(b_i, t_i, e_i)_{i\geq 1}$ such that $k = \sum_{i=1}^{l} 2^{b_i} 3^{t_i} 5^{e_i}$ with $b_i, t_i, e_i \geq 0$

1. $i \leftarrow 1$
2. while $k > 0$ do
3. find $\{2,3,5\}$-integer $c = 2^b 3^t 5^e$ the best approximation of $k$, with $b \leq b_{\max}$, $t \leq t_{\max}$, $e \leq e_{\max}$
4. $b_i \leftarrow b$, $t_i \leftarrow t$, $e_i \leftarrow e$, $i \leftarrow i+1$
5. $k \leftarrow |k-c|$
6. end while
7. return $((b_i, t_i, e_i))_{i\geq 1}$

## 3. THE LENGTH OF CONSTRAINED TRIPLE-BASE NUMBER SYSTEM

In this section, we give an estimate for the length of constrained triple-base representation of an integer. We use similar proof of Theorem 1 to prove Theorem 2. However, the proof of Theorem 2 is more complex since it involves three bases. In order to use the conclusion of Theorem 1, we first define two sets, which are related to TBNS and constrained TBNS respectively. Then, we prove Theorem 2 by examining the relationship between the two sets.

**Theorem 2:** Let $c_1$, $c_2$, $c_3$ be three positive real numbers such that $c_1 + c_2 + c_3 \geq 1$. Then, for $k$ large enough, Algorithm 2 with parameter $k$ and bounds $b_{\max} = \lfloor c_1 \log_2 k \rfloor + 1$, $t_{\max} = \lfloor c_2 \log_3 k \rfloor + 1$ and $e_{\max} = \lfloor c_3 \log_5 k \rfloor + 1$ terminates in $O(\log k / \log \log k)$ steps.

***Proof*:** Let us define $T_{2,3,5}(k) = \{2^b 3^t 5^e \leq k\}$ and $\overline{T}_{2,3,5}(k) = \{2^b 3^t 5^e \leq k: b \leq b_{\max}, t \leq t_{\max}, e \leq e_{\max}\}$. Without loss of generality, we can assume that $5^{e_{\max}} < 3^{t_{\max}} < 2^{b_{\max}}$. According to the value of $k$, the proof of this theorem will be split into four cases. For ease of understanding, we first give our intuitions before the proof:

- Case 1 is the most simplest and can be proved directly using the conclusion of Theorem 1.
- The proofs of Cases 2 and 3 are similar, the problem can be transformed into the case of Theorem 1 to prove.
- Case 4 is more complex. We firstly show that every integer $k > 2^{b_{\max}}$ can be reduced to integer $k_{n+m+1} < 2^{b_{\max}}$ after $O(\log k / \log \log k)$ steps, then use the previous three cases to prove.

**Case 1:** $k \leq 5^{e_{\max}} < 3^{t_{\max}} < 2^{b_{\max}}$

Due to $k \leq \min(5^{e_{\max}}, 3^{t_{\max}}, 2^{b_{\max}})$, we have $T_{2,3,5}(k) = \overline{T}_{2,3,5}(k)$. Hence, the greedy algorithm and algorithm 2 return the same results. By Theorem 1, our conclusion holds.

**Case 2:** $5^{e_{\max}} \leq k < 3^{t_{\max}} < 2^{b_{\max}}$

**Case 3:** $5^{e_{\max}} < 3^{t_{\max}} \leq k \leq 2^{b_{\max}}$

Let $B$ be the smallest integer such that $\frac{5^{e_{\max}}}{2} \leq \frac{k}{2^B} \leq 5^{e_{\max}}$. For $k$ large enough, we apply Lemma 2 to integer $K = \frac{k}{2^B}$. There exists absolute constant $C > 0$ and $2^b 3^t 5^e \in T_{2,3,5}(K)$ such that

$$0 \leq K - 2^b 3^t 5^e \leq \frac{K}{(\log K)^C}.$$

We claim that $2^{B+b} 3^t 5^e \in \overline{T}_{2,3,5}(k)$. By definition of $B$ and $K$, we know $k \leq 2^B 5^{e_{\max}}$ and $k \geq 2^{B+b} 3^t 5^e$.

- If $b+B > b_{\max}$, then $2^{B+b} 3^t 5^e \geq 2^{B+b} > 2^{b_{\max}} > k$, resulting in a contradiction.
- If $t > t_{\max}$, then $2^{B+b} 3^t 5^e > 2^B 3^t > 2^B 3^{t_{\max}} > k$, a contradiction.
- If $e > e_{\max}$, then $2^{B+b} 3^t 5^e > 2^B 5^{e_{\max}} \geq k$, a contradiction.

Hence $b+B \le b_{\max}$, $t \le t_{\max}$, $e \le e_{\max}$ and $2^{B+b}3^t5^e \in \overline{T}_{2,3,5}(k)$.

On the other hands, $\log K = \log \frac{k}{2^B} \ge \log \frac{5^{e_{\max}}}{2} = e_{\max} \log 5 - \log 2$. Since $\frac{k}{2^B} \le 5^{e_{\max}}$, it follows that $\log \log k - B\log 2 \le e_{\max}\log 5$. So $e_{\max}\log 5 - \log 2 \ge \log k - (B+1)\log 2$,

$$k - 2^{B+b}3^t5^e \le \frac{k}{(\log K)^C} \le \frac{k}{(e_{\max} \log 5 - \log 2)^C} \le \frac{k}{(\log k - (B+1)\log 2)^C}.$$

Hence, there exists constant $c$ such that

$$0 \le k - 2^{B+b}3^t5^e \le \frac{k}{(c \log k)^C}.$$

In other words, there always exists a number $2^{B+b}3^t5^e \in \overline{T}_{2,3,5}(k)$. Note that the biggest integer from $\overline{T}_{2,3,5}(k)$ satisfies the previous propriety. By Theorem 1, we conclude that the constrained greedy algorithm terminates in $O(\log k / \log \log k)$ steps.

**Case 4:** $5^{e_{\max}} < 3^{t_{\max}} > 2^{b_{\max}} \le k$

Let $k_0 = k$. By Algorithm 2, we can construct a sequence $k_0 > k_1 > \ldots > k_l$ such that $k_{i+1} = k_i - 2^{b_{i+1}}3^{t_{i+1}}5^{e_{i+1}}$. By the definition of $b_{\max}$, $t_{\max}$, $e_{\max}$, we know $2^{b_{\max}}3^{t_{\max}}5^{e_{\max}} \ge k^{c_1+c_2+c_3} \ge k$. So there exists $d = 2^B3^T5^E \in \overline{T}_{2,3,5}(k)$ such that $k/2 \le d \le k$. More generally, the sequence $(k_i)$ satisfies $k_{i+1} \le k_i/2$, then $k_i \le k/2^i$. Let $n = \left\lfloor \frac{\log k}{\log \log k} \right\rfloor$. For $k$ large enough, we can apply Lemma 1 to any integer larger than $\frac{1}{30}\sqrt{2^{n-1}}$. To complete the proof of Theorem 2, we first prove Lemma 2 below.

**Lemma 2:** For any integer $k'$ smaller than $k_n$, there exists $d \in \overline{T}_{2,3,5}(k')$ and constants $A$, $C > 0$ such that

$$k' - d \le \frac{k'}{An^C}.$$

***Proof*:** Since $k' \le k_n$ and $k_n \le k/2^n$, it follows that $\frac{k}{k'} \ge 2^n$. For $0 \le b \le B$, $0 \le t \le T$ and $0 \le e \le E$, we define

$$K(b,t,e) = \frac{k'}{2^{B-b}3^{T-t}5^{E-e}} \text{ and } F_{B,T,E} = \{K(b, t, e) \le \min(2^b, 3^t, 5^e)\}.$$

Obviously, $K(0,0,0) = \frac{k'}{2^B3^T5^E} \le \frac{k}{2^n2^B3^T5^E} \le 1$, then $K(0,0,0) \in F_{B,T,E}$ and the set $F_{B,T,E}$ is not empty. Let $K(\bar{b}, \bar{t}, \bar{e})$ be the maximum of the set $F_{B,T,E}$, then $K(\bar{b}+1, \bar{t}, \bar{e}) \notin F_{B,T,E}$ which means that $K(\bar{b}+1, \bar{t}, \bar{e}) > \min(2^{\bar{b}+1}, 3^{\bar{t}}, 5^{\bar{e}})$. We remark that $2^{\bar{b}+1}$ must be larger than $3^{\bar{t}}$ and $5^{\bar{e}}$, otherwise $K(\bar{b}+1, \bar{t}, \bar{e}) > 2^{\bar{b}+1}$ and thus $K(\bar{b}, \bar{t}, \bar{e}) > 2^{\bar{b}}$, which contradicts with the definition of $K(\bar{b}, \bar{t}, \bar{e})$.

Below, we show that $K(\bar{b},\bar{t},\bar{e}) > \frac{1}{30}\sqrt{\frac{2^B3^T5^E}{k'}}$, of which the proof can be divided into six cases according to the relationship between $2^{\bar{b}}$, $3^{\bar{t}}$ and $5^{\bar{e}}$.

**1. Suppose** $2^{\bar{b}} < 3^{\bar{t}} < 5^{\bar{e}}$. Since $K(\bar{b}+1, \bar{t}, \bar{e}) > \min(2^{\bar{b}+1}, 3^{\bar{t}}, 5^{\bar{e}}) = 3^{\bar{t}}$, it follows that

$$\frac{k'}{2^{B-\bar{b}-1}3^{T-\bar{t}}5^{E-\bar{e}}} = \frac{k'}{2^B3^T5^E}\cdot 2^{\bar{b}+1}3^{\bar{t}}5^{\bar{e}} > 3^{\bar{t}} \Rightarrow 2^{\bar{b}+1}5^{\bar{e}} > \frac{2^B3^T5^E}{k'}.$$

Since $K(\bar{b}, \bar{t}+1, \bar{e}) > \min(2^{\bar{b}}, 3^{\bar{t}+1}, 5^{\bar{e}}) = 2^{\bar{b}}$, then

$$\frac{k'}{2^{B-\bar{b}}3^{T-\bar{t}-1}5^{E-\bar{e}}} = \frac{k'}{2^B3^T5^E}\cdot 2^{\bar{b}}3^{\bar{t}+1}5^{\bar{e}} > 2^{\bar{b}} \Rightarrow 3^{\bar{t}+1}5^{\bar{e}} > \frac{2^B3^T5^E}{k'}.$$

Due to $2^{\bar{b}} < 3^{\bar{t}} < 3\cdot 2^{\bar{b}}$, we explain according to the relationship between $5^{\bar{e}}$ and $3\cdot 2^{\bar{b}}$.

– if $2^{\bar{b}} < 3^{\bar{t}} < 5^{\bar{e}} < 3\cdot 2^{\bar{b}}$, because we have known $2^{\bar{b}+1}5^{\bar{e}} > \frac{2^B3^T5^E}{k'}$, then

$$\left(2^{\bar{b}}\right)^2 > \frac{2^B3^T5^E}{6k'} \Rightarrow 2^{\bar{b}} > \sqrt{\frac{2^B3^T5^E}{6k'}}.$$

– if $2^{\bar{b}} < 3^{\bar{t}} < 3\cdot 2^{\bar{b}} < 5^{\bar{e}}$, then $\frac{3}{5}2^{\bar{b}} < 5^{\bar{e}-1}$. Hence

$$K(\bar{b},\bar{t}+1,\bar{e}-1) = \frac{3}{5}K(\bar{b},\bar{t},\bar{e}) \le \frac{3}{5}\min(2^{\bar{b}},3^{\bar{t}},5^{\bar{e}}) \le \min(2^{\bar{b}},3^{\bar{t}+1},5^{\bar{e}-1}),$$

that is $K(\bar{b}, \bar{t}+1, \bar{e}-1) \in F_{B,T,E}$. Since $K(\bar{b}, \bar{t}+1, \bar{e}-1) > K(\bar{b}, \bar{t}, \bar{e})$ and $K(\bar{b}, \bar{t}, \bar{e})$ be the maximum of the set $F_{B,T,E}$, it follows that $K(\bar{b}+1, \bar{t}+1, \bar{e}-1) > \min(2^{\bar{b}+1}, 3^{\bar{t}+1}, 5^{\bar{e}-1})$, then $2^{\bar{b}+1}$ must be larger than $5^{\bar{e}-1}$. Otherwise, $K(\bar{b}+1, \bar{t}+1, \bar{e}-1) > 2^{\bar{b}+1}$, so $K(\bar{b}, \bar{t}+1, \bar{e}-1) > 2^{\bar{b}}$. But due to $K(\bar{b}, \bar{t}+1, \bar{e}-1) \in F_{B,T,E}$, then $K(\bar{b}, \bar{t}+1, \bar{e}-1) \le 2^{\bar{b}}$, which leads to a contradiction. Hence

$$\left(2^{\bar{b}+1}\right)^2 > \frac{2^B3^T5^E}{5k'} \Rightarrow 2^{\bar{b}} > \frac{1}{2}\sqrt{\frac{2^B3^T5^E}{5k'}}.$$

So regardless of the relationship between $5^{\bar{e}}$ and $3\cdot 2^{\bar{b}}$, there is always $2^{\bar{b}} > \frac{1}{2}\sqrt{\frac{2^B3^T5^E}{5k'}}$. Hence

$$K(\bar{b},\bar{t},\bar{e}) = \frac{k'}{2^{B-\bar{b}}3^{T-\bar{t}}5^{E-\bar{e}}} = \frac{1}{3}\cdot\frac{k'}{2^B3^T5^E}\cdot 2^{\bar{b}}\cdot 3^{\bar{t}+1}5^{\bar{e}} > \frac{1}{2}\cdot\frac{1}{3}\sqrt{\frac{2^B3^T5^E}{5k'}} = \frac{1}{6}\sqrt{\frac{2^B3^T5^E}{5k'}}.$$

**2. Suppose** $2^{\bar{b}} < 5^{\bar{e}} < 3^{\bar{t}}$. Since $K(\bar{b}+1, \bar{t}, \bar{e}) > \min(2^{\bar{b}+1}, 3^{\bar{t}}, 5^{\bar{e}}) = 5^{\bar{e}}$, it follows that

$$2^{\bar{b}+1}3^{\bar{t}} > \frac{2^B3^T5^E}{k'}.$$

Since $K(\bar{b}, \bar{t}+1, \bar{e}) > \min(2^{\bar{b}}, 3^{\bar{t}+1}, 5^{\bar{e}}) = 2^{\bar{b}}$, then $3^{\bar{t}+1}5^{\bar{e}} > \frac{2^B3^T5^E}{k'}$.

Due to $2^{\bar{b}} < 5^{\bar{e}} < 5\cdot 2^{\bar{b}}$, similarly we explain according to the relationship between $3^{\bar{t}}$ and $5\cdot 2^{\bar{b}}$.

– if $2^{\bar{b}} < 5^{\bar{e}} < 5\cdot 2^{\bar{b}}$, because we have known $2^{\bar{b}+1}3^{\bar{t}} > \frac{2^B 3^T 5^E}{k'}$, then

$$\left(2^{\bar{b}}\right)^2 > \frac{2^B 3^T 5^E}{10k'} \Rightarrow 2^{\bar{b}} > \sqrt{\frac{2^B 3^T 5^E}{10k'}}.$$

– if $2^{\bar{b}} < 5^{\bar{e}} < 5\cdot 2^{\bar{b}} < 3^{\bar{t}}$, then $\frac{5}{9}2^{\bar{b}} < 3^{\bar{t}-2}$. Hence

$$K(\bar{b},\bar{t}-2,\bar{e}+1) = \frac{5}{9}K(\bar{b},\bar{t},\bar{e}) \le \frac{5}{9}\min(2^{\bar{b}},3^{\bar{t}},5^{\bar{e}}) \le \min(2^{\bar{b}},3^{\bar{t}-2},5^{\bar{e}+1}),$$

that is, $K(\bar{b}, \bar{t}-2, \bar{e}+1)\in F_{B,T,E}$.

Since $K(\bar{b}+1, \bar{t}-2, \bar{e}+1) > K(\bar{b}, \bar{t}, \bar{e})$ and $K(\bar{b}, \bar{t}, \bar{e})$ be the maximum of the set $F_{B,T,E}$, it follows that $K(\bar{b}+1, \bar{t}-2, \bar{e}+1) > \min(2^{\bar{b}+1}, 3^{\bar{t}+1}, 5^{\bar{e}+1})$, then $2^{\bar{b}+1}$ must be larger than $3^{\bar{t}-2}$. Otherwise, $K(\bar{b}+1, \bar{t}-2, \bar{e}+1) > 2^{\bar{b}+1}$, so $K(\bar{b}, \bar{t}-2, \bar{e}+1) > 2^{\bar{b}}$. But due to $K(\bar{b}, \bar{t}-2, \bar{e}+1) \in F_{B,T,E}$, then $K(\bar{b}, \bar{t}-2, \bar{e}+1) \le 2^{\bar{b}}$, which leads to a contradiction. Hence

$$\left(2^{\bar{b}+1}\right)^2 > \frac{2^B 3^T 5^E}{9k'} \Rightarrow 2^{\bar{b}} > \frac{1}{6}\sqrt{\frac{2^B 3^T 5^E}{k'}}.$$

So regardless of the relationship between $3^{\bar{t}}$ and $5\cdot 2^{\bar{e}}$, there is always $2^{\bar{b}} > \frac{1}{6}\sqrt{\frac{2^B 3^T 5^E}{k'}}$. Hence

$$K(\bar{b},\bar{t},\bar{e}) = \frac{k'}{2^{B-\bar{b}}3^{T-\bar{t}}5^{E-\bar{e}}} = \frac{1}{3}\cdot\frac{k'}{2^B 3^T 5^E}\cdot 2^{\bar{b}}\cdot 3^{\bar{t}+1}5^{\bar{e}} > \frac{1}{3}\cdot\frac{1}{6}\sqrt{\frac{2^B 3^T 5^E}{k'}} = \frac{1}{18}\sqrt{\frac{2^B 3^T 5^E}{k'}}.$$

**3. Suppose** $3^{\bar{t}} < 2^{\bar{b}} < 5^{\bar{e}}$. Then $K(\bar{b},\bar{t},\bar{e}) > \frac{1}{6}\sqrt{\frac{2^B 3^T 5^E}{5k'}}$.

**4. Suppose** $3^{\bar{t}} < 5^{\bar{e}} < 2^{\bar{b}}$. Then $K(\bar{b},\bar{t},\bar{e}) > \frac{1}{12}\sqrt{\frac{2^B 3^T 5^E}{5k'}}$.

**5. Suppose** $5^{\bar{e}} < 2^{\bar{b}} < 3^{\bar{t}}$. Then $K(\bar{b},\bar{t},\bar{e}) > \frac{1}{30}\sqrt{\frac{2^B 3^T 5^E}{5k'}}$.

**6. Suppose** $5^{\bar{b}} < 3^{\bar{t}} < 2^{\bar{b}}$. Then $K(\bar{b},\bar{t},\bar{e}) > \frac{1}{20}\sqrt{\frac{2^B 3^T 5^E}{5k'}}$.

In a word, regardless of the relationship between $2^{\bar{b}}$, $3^{\bar{t}}$, and $5^{\bar{e}}$, there must be

$$K(\bar{b},\bar{t},\bar{e}) > \frac{1}{30}\sqrt{\frac{2^B 3^T 5^E}{k'}} \ge \frac{1}{30}\sqrt{\frac{k}{2k'}} \ge \frac{1}{30}\sqrt{2^{n-1}}.$$

Now we can apply Lemma 1 to $K(\bar{b}, \bar{t}, \bar{e})$, then there exist constant $C$ and $b'$, $t'$, $e'$ such that

$$0 \le K(\bar{b},\bar{t},\bar{e}) - 2^{b'}3^{t'}5^{e'} \le \frac{K(\bar{b},\bar{t},\bar{e})}{(\log K(\bar{b},\bar{t},\bar{e}))^C}.$$

Due to $K(\bar{b}, \bar{t}, \bar{e}) \le \min(2^{\bar{b}}, 3^{\bar{t}}, 5^{\bar{e}})$, there must be $b' \le \bar{b}$, $t' \le \bar{t}$, and $e' \le \bar{e}$. Thus there exists constant $A$ such that

$$0 \le k' - 2^{B+b'-\bar{b}}3^{T+t'-\bar{t}}5^{E+e'-\bar{e}} \le \frac{k'}{(\log K(\bar{b},\bar{t},\bar{e}))^C} \le \frac{k'}{\left(\frac{n-1}{2}\log 2 - \log 30\right)^C} \le \frac{k'}{An^C}.$$

Hence $d = 2^{B+b'-\bar{b}}3^{T+t'-\bar{t}}5^{E+e'-\bar{e}} \in \bar{T}_{2,3,5}(k')$ is what we are looking for. ❑

By Lemma 2, we know the sequence $k_n > k_{n+1} > \ldots > k_{n+m}$ returned by Algorithm 2 satisfies

$$k_{n+i+1} = k_{n+i} - 2^{b_{n+i+1}}3^{t_{n+i+1}}5^{e_{n+i+1}} \le \frac{k_{n+i}}{An^C}.$$

Hence

$$k_{n+m+1} \le \frac{k_n}{A^m n^{m\cdot C}} \le \frac{k}{2^n \cdot A^m n^{m\cdot C}}.$$

To complete the proof of Theorem 2, we show there exists a function $f$: $k \to f(k)$ such that the integer $m = \lfloor f(k) \rfloor + 1$ satisfies $k_{n+m+1} \le 2^{b_{\max}}$. So every integer belonging to $[1, k_{n+m+1}]$ can be represented by the sum or difference of at most $O\left(\frac{\log k}{\log\log k}\right)$ $\{2,3,5\}$-integers. Since

$$\log k_{n+m+1} \le \log\left(\frac{k}{2^n \cdot A^m n^{m\cdot C}}\right) = \log k - n\log 2 - m\log A - Cm\log n,$$

in order to make $k_{n+m+1}$ smaller than $2^{b_{\max}}$, we can let

$$\log k - n\log 2 - m\log A - n\log 2 - m\log A - Cm\log n < c_1 \log k,$$

so $\log k_{n+m+1} < c_1 \log k \le b_{\max}\log 2$.

The condition above is equivalent to

$$(1-c_1)\log k - \left\lfloor \frac{\log k}{\log\log k} \right\rfloor \log 2 < m\left(\log A + C\log\left(\left\lfloor \frac{\log k}{\log\log k} \right\rfloor\right)\right).$$

Then for $k$ large enough and some real number $C'$,

$$C' \frac{\log k}{\log\log k - \log\log\log k} < m.$$

Let $f(k) = C' \frac{\log k}{\log\log k - \log\log\log k}$. To show $f(k) = O\left(\frac{\log k}{\log\log k}\right)$, that is, there exists constant $D$ such that

$$f(k) = C' \frac{\log k}{\log\log k - \log\log\log k} < D \frac{\log k}{\log\log k}.$$

We only need to prove that $C'\log\log k < D\log\log k - D\log\log\log k$. However, when $D >$

$C'$ and $k$ large enough, this condition is established. So we have $f(k) = O\left(\frac{\log k}{\log\log k}\right)$. ❑

## 4. CONCLUSION

In this paper, we have studied constrained triple-base number system, and shown that an integer $k$ can be represented using at most $O\left(\frac{\log k}{\log\log k}\right)$ $\{2,3,5\}$-integers under reasonable restriction of exponents. Compared with the result of Theorem 1, this result is more practical and provides a theoretical basis for selecting appropriate parameters in practical application.

## REFERENCES

1. V. S. Miller, "Uses of elliptic curves in cryptography," in *Proceedings of CRYPTO'85*, 1986, pp. 417-428.
2. N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, Vol. 48, 1987, pp. 203-209.
3. Y. Zhang, X. Sun, and B. Wang, "Efficient algorithm for K-Barrier coverage based on integer linear programming," *China Communications*, Vol. 13, 2016, pp. 16-23.
4. Q. Liu, W. Cai, J. Shen, Z. Fu, X. Liu, and N. Linge, "A speculative approach to spatial temporal efficiency with multi objective optimization in a heterogeneous cloud environment," *Security and Communication Networks*, Vol. 9, 2016, pp. 4002-4012.
5. Y. Kong, M. Zhang, and D. Ye, "A belief propagation-based method for task allocation in open and dynamic cloud environments," *Knowledge-based Systems*, Vol. 115, 2016, pp. 123-132.
6. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, Vol. 11, 2016, pp. 2594-2608.
7. Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Transactions on Information Forensics and Security*, Vol. 11, 2016, pp. 2706-2716.
8. Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Computers and Electrical Engineering*, 2017, DOI:10.1016/j.compeleceng.2017.03.016.
9. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 27, 2015, pp. 340-352.
10. Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, Vol. 5, 2017, pp. 3376-3392.
11. C. Yuan, X. Sun, and R. Lv, "Fingerprint liveness detection based on multi-scale LPQ and PCA," *China Communications*, Vol. 13, 2016, pp. 60-65.

12. V. Dimitrov and T. Cooklev, "Two algorithms for modular exponentiation using nonstandard arithmetics," *IEICE Transactions on Fundamentals Electronics*, *Communications and Computer Sciences*, Vol. E78-A, 1995, pp. 82-87.
13. V. Dimitrov, G. A. Julien, and W. C. Miller, "An algorithm for modular exponentiation," *Information Processing Letters*, Vol. 66, 1998, pp. 155-159.
14. V. Dimitrov, K. Jarvinen, and J. Adikari, "Area efficient multipliers based on multiple-raidx representations," *IEEE Transactions on Computers*, Vol. 60, 2011, pp. 189-201.
15. V. Dimitrov, L. Imbert, and P. K. Mishra, "Efficient and secure elliptic curve point multiplication using double-base chains," in *Proceedings of ASIACRYPT*, 2005, pp. 59-78.
16. P. Chalermsook, H. Imai, and V. Suppakitpaisarn, "Two lower bounds on the shortest double-base number system," *IEICE Transactions on Fundamentals Electronics*, *Communications and Computer Sciences*, Vol. E98-A, 2015, pp. 1310-1312.
17. N. Méloni and M. A. Hasan, "Efficient double bases for scalar multiplication," *IEEE Transactions on Computers*, Vol. 64, 2015, pp. 2204-2212.
18. A. C. Yao, "On the evaluation of powers," *SIAM Journal on Computing*, Vol. 5, 1976, pp. 100-103.
19. P. K. Mishra and V. Dimitrov, "Efficient quintuple formulas for elliptic curves and efficient scalar multiplication using multibase number representation," in *Proceedings of International Conference on Information Security*, 2007, pp. 390-406.
20. P. Longa and C. Gebotys, "Fast multibase methods and other several optimization for elliptic curve scalar multiplication," in *Proceedings of International Workshop on Public Key Cryptography*, 2009, pp. 443-462.
21. P. Longa, "Accelerating the scalar multiplication on elliptic curve cryptosystems over prime fields," Master Thesis, Department of Information Technology and Engineering, University of Ottawa, 2007.
22. W. Yu, K. Wang, B. Li, and S. Tian, "On the expansion length of triple-base number systems," in *Proceedings of AFRICACRYPT*, 2013, pp. 424-432.
23. Y. Dou, J. Weng, C. Ma, and F. Wei, "Secure and efficient ECC speeding up algorithms for wireless sensor networks," *Soft Computing*, 2016, DOI: 10.1007/s00500-016-2142-x.
24. V. Dimitrov, L. Imbert, and P. K. Mishra, "The double-base number system and its application to elliptic curve cryptography," *Mathematics of Computation*, Vol. 77, 2008, pp. 1075-1104.
25. R. Tijdeman, "On the maximal distance between integers composed of small primes," *Compositio Mathematica*, Vol. 28, 1974, pp. 159-162.

**Yun-Qi Dou (豆允旗)** received his Ph.D. degree in State Key Laboratory of Mathematical Engineering and Advanced Computing, China in 2017. His research fields include Elliptic curve cryptography and side-channel attack.

**Jiang Weng (翁江)** received his Ph.D. degree in State Key Laboratory of Mathematical Engineering and Advanced Computing, China in 2016. His research focuses on elliptic curve cryptography and discrete logarithm problem.

**Chuan-Gui Ma (馬传贵)** received his Ph.D. degree in Applied Mathematics from Zhejiang University, China in 1999. He is currently a Professor in the State Key Laboratory of Mathematical Engineering and Advanced Computing. His main research interests include information security and public key cryptography.

**Fu-Shan Wei (魏福山)** received the Ph.D. degree in the Zhengzhou Information Science and Technology Institute, China. He is currently a Lecturer in State Key Laboratory of Mathematical Engineering and Advanced Computing. His current research interest includes gateway protocol and code analysis.