New Construction of Single Cycle T-function Families

Shiyi ZHANG[1], Yongjuan WANG*, Guangpu GAO

Luoyang Foreign Language University, Luoyang, Henan Province, China

Abstract

The single cycle T-function is a particular permutation function with complex algebraic structures, maximum period and efficient implementation in software and hardware. In this paper, on the basis of existing methods, by using a class of single cycle T-functions that satisfy some certain conditions, we first present a new construction of single cycle T-function families. Unlike the previous approaches, this method can construct multiple single cycle T-functions at once. Then the mathematical proof of the feasibility is given. Next the numeration for the newly constructed single cycle T-functions is also investigated. Finally, this paper is end up with a discussion of the properties which these newly constructed functions preserve, such as linear complexity and stability (k-error complexity), as well as a comparison with previous construction methods.

Keywords: cryptography; permutation function; single cycle T-function; numeration; linear complexity

1. Introduction

Permutation functions are widely used in cryptography. It can be used for the construction and analysis of symmetric cryptography such as the stream cipher, block cipher, hash function and PRNG (Pseudo Random Number Generator). It has also played an important role in the analysis of public key cryptography and the construction of special code in communication system. In

*Corresponding author

Email addresses: syzhang1352@163.com (Shiyi ZHANG), pinkywyj@163.com (Yongjuan WANG), gaohuangpu@yahoo.com.cn (Guangpu GAO)

2002, Klimov and Shamir proposed a new class of particular permutation functions called T-function [1]. As it is able to mix arithmetic operations (negation, addition, subtraction, multiplication) and boolean operations (not, xor, and, or), it has a naturally complex nonlinear structure. In addition, T-functions can generate maximum period sequences and have high software and hardware implementation speed. Since T-functions have so many desirable cryptographic properties, the sequence derived from T-functions is a good type of nonlinear sequence source for stream cipher design, which has a promising prospect in practice.

T-function has gained much attention since its introduction. New construction methods and discussions of their cryptographic properties are presented[2, 3, 4, 5, 6]. Configuration and properties of derived sequences from T-functions are carefully examined[7, 8, 9, 10]. The design and analysis of the new cryptographic system based on T-functions is also flourishing[11], such as Mir-1[12], TSC series ciphers[13].

Current construction methods of single cycle T-functions mainly fall into the following several categories. The first uses parameters. Parameter as an important tool for the research on T-functions was proposed by Klimov and Shamir[14]. By using parameters, single-word single cycle T-functions can be obtained, such as the Klimov-Shamir T-function [1] and the functions proposed by Yang[15]. The second uses algebraic dynamical system. Anashin described a method using current T-functions to construct single cycle T-functions, which used p-aidc analysis and infinite power series[16]. The method is also a necessary and sufficient condition to determine whether a T-function has a single cycle. Practically, however, this method is not so easy-to-use. The third uses polynomial functions. The necessary and sufficient conditions of a single cycle function is a polynomial function $f(x) = \sum_{k\geq 0} a_k x^k$ over $\mathbb{Z}/(2^n)$ was given[17, 18]. The forth is multiword single cycle T-functions. It was first introduced by Klimov and Shamir in[18]. As the characteristics of multiword single cycle T-functions can also be reflected in single-word single cycle T-functions, and single-word single cycle T-functions have high algebraic degree, good stability and other excellent properties, nowadays researches mainly focus on single-word single cycle T-functions.

Klimov and Shamir presented a method to get a larger cycle from single cycle T-functions[14]. Using its idea of construction, this paper discovered a new construction of single cycle T-functions. Using several single cycle T-functions which satisfy certain conditions, it is able to construct new single cycle T-function families. Meanwhile, we give the proof by induction and also the numeration for this construction, and analysis the properties these newly constructed functions preserve at the meantime

2. Notations and Definitions

Definition 1. [1] Let $\underline{x} = (x_0, \ldots, x_{m-1})^T \in \mathbb{F}_2^{mn}$, $\underline{y} = (y_0, \ldots, y_{l-1})^T \in \mathbb{F}_2^{ln}$, where $x_i = (x_{i,0}, \ldots, x_{i,n-1})$, $y_i = (y_{i,0}, \ldots, y_{i,n-1})$. Let f be a mapping from $\mathbb{F}_2^{mn}$ to $\mathbb{F}_2^{ln}$, that is

$$f : \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,n-1} \\ \vdots & \vdots & \ldots & \vdots \\ x_{m-1,0} & x_{m-1,1} & \cdots & x_{m-1,n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} y_{0,0} & y_{0,1} & \cdots & y_{0,n-1} \\ y_{1,0} & y_{1,1} & \cdots & y_{1,n-1} \\ \vdots & \vdots & \ldots & \vdots \\ y_{l-1,0} & y_{l-1,1} & \cdots & y_{l-1,n-1} \end{pmatrix},$$

for $0 \leq j \leq n-1$, if the j-th column of the output $\mathbf{R}_j(y)$ depends only on the first $j+1$ columns of the input: $\mathbf{R}_j(x), \ldots, \mathbf{R}_0(x)$, then f is called a T-function.

Definition 2. A T-function $f(x) : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ is called invertible if $f(x) = f(y) \Longleftrightarrow x = y$.

Definition 3. [1] Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ be a T-function. Given the initial state $x_0 = (x_{0,n-1}, x_{0,n-2}, \ldots, x_{0,0})^T$, for $i \geq 0$, let $x_{i+1} = f(x_i)$. If the sequence $\underline{x} = (x_0, x_1, \ldots)$ has the period of 2^n, then $f(x)$ is called a single cycle T-function and sequence $\underline{x}$ is called to be generated by the single cycle T-function $f(x)$ and the initial state x_0.

Definition 4. [14] $\underline{x} = (x_0, x_1, \ldots)$ is a sequence over $\mathbb{F}_2^n$, where

$$x_i = (x_{i,n-1}, x_{i,n-2}, \ldots, x_{i,0})^T, i \geq 0.$$

For $0 \leq j \leq n-1$, $\underline{x_j} = (x_{0,j}, x_{1,j}, \ldots)$ is called as the j-th coordinate sequence of $\underline{x}$.

Theorem 1. [14] Given a sequence $\underline{x} = (x_0, x_1, \ldots)$ generated by single cycle T-function $f(x)$ and x_0 is the initial state. Then the j-th coordinate sequence of $\underline{x}$, $\underline{x}_j (0 \leq j \leq n-1)$ has the period of 2^{j+1}. Meanwhile, for $0 \leq j \leq n-1$, the two parts of the sequence $\underline{x}_j$ are complementary, that is $x_{i+2^j,j} = x_{i,j} \oplus 1, i \geq 0$.

Definition 5. ([19], linear complexity) The linear complexity of a sequence S refers to the minimum order of the linear feedback shift register that produces it, denoted as $LC(S)$.

Definition 6. ([20], k-error linear complexity) For a periodic sequence S, after changing at most k bits in a period of S, and the minimum linear complexity of all the sequences obtained is called as the k-error linear complexity of S, denoted as $LC_k(S)$, and the minimum error $minerror(S) = mink|LC_k(S) < LC(S)$.

Theorem 2. [21] For the output sequence $\{(\underline{x})\}$ of a single cycle T-function over $\mathbb{F}_2^n$, its linear complexity $LC(\{(\underline{x})\}) = n \times 2^{n-1} + n$, and its minimum polynomial is $x^{n\times 2^{n-1}+n} + x^{n\times 2^{n-1}} + x^n + 1$, meanwhile, $minerror(\{(\underline{x})\}) \leq 2^{n-1}$(when $n = 2^t$,the equality holds).

In [1], T-functions like $f(x) = x + (x^2 \vee C) mod 2^n$ were studied, and the authors presented the equivalency conditions of this type is invertible or has a single cycle.

Lemma 1. ([1],K-S single cycle T-function) The mapping $f(x) = x + (x^2 \vee C)\ \ mod\ \ 2^n$ is invertible if and only if $[C]_0 = 1$. For $n \geq 3$, $f(x)$ is a single cycle T-function if and only if $[C]_0 = [C]_2 = 1$, that is $C\ mod\ 8 = 5$ or 7, where x is a n-bit word and C is some constant.

Before multiword single cycle T-functions were introduced, Klimov and Shamir presented a method to increase the period of single-word single cycle T-functions [14]. By using m (m is odd) invertible functions over $\mathbb{F}_2^n$, it can construct sequences of period $m2^n$.

Consider the sequence $\{(x_i)\}$ defined by iterating

$$x_{i+1} = x_i + (x_i^2 \vee C_{k_i}) \ mod \ 2^n, k_{i+1} = k_i + 1 \ mod \ m \qquad (1)$$

where for any $k = 0, \ldots, m-1$, C_k is some constant.

Lemma 2. [14] For the sequence $\{(x_i)\}$ defined in (1), the sequence of pairs $\{(x_i, k_i)\}$ has the maximal period $m2^n$ if and only if m is odd, and for all k, $[C_k]_0 = 1$, $\oplus_{k=0}^{m-1}[C_k]_2 = 1$.

Unfortunately , authors of [14] claimed that the proof of Lemma 2 is quite difficult, and due to the limitations of space, they omitted it.

3. The New Construction

Unlike [14], which used odd invertible functions to get a larger period cycle(not a single cycle T-function), we found that when m is an even number, in particular, $m = 2^l (l \in \mathbb{N}^+)$, by using m single cycle T-functions satisfying certain conditions of period 2^n, we can construct m pairwise different new single cycle T-functions of period 2^n.

Theorem 3. (New Construction) Consider the sequence $\{(x_i)\}$ defined by iterating

$$F(x) : x_{i+1} = f_{k_i}(x_i) \ mod \ 2^n, k_{i+1} = k_i + 1 \ mod \ m$$

where the component function defined as $f_{k_i}(x_i) = x_i + (x_i^2 \vee C_{k_i}) mod 2^n, n \geq 4$, and note here C_k is an arrangement of different ordered elements.

When $m = 2^l (l = 1, 2, \ldots, n-3)$, if for each element of $< C_k >$, all the conditions below could be satisfied simultaneously:

1) for all k, $C_k \equiv 5 \ mod \ 8$ simultaneously or $C_k \equiv 7 \ mod \ 8$ simultaneously;

2) for $i = 0, 1, \ldots, m-1, [C_{k_i}]_3 \oplus [C_{k_{i+1}}]_3 = 1, \oplus_{i=0}^{m-1}[C_{k_i}]_{l+1} = 0$;

3) when $3 \leq l \leq n-3$, for each t which satisfies $2 < t < l, \oplus_{j=0}^{2^t-1}[C_{k_{i+j}}]_{t+1} = 0$, where $i + j$ is module m.

Then for any different input initial state x_0 modulo m, $F(x)$ is a single cycle T-function, and it can generate m pairwise different single cycle T-functions of period 2^n in total.

Proof. From the iterative relation we have,

$$
\begin{aligned}
x_{i+1} &= x_i + (x_i^2 \vee C_{k_i}) \ mod \ 2^n, \\
x_{i+2} &= x_i + (x_i^2 \vee C_{k_i}) + (x_{i+1}^2 \vee C_{k_{i+1}}) \ mod \ 2^n, \\
&\vdots \\
x_{i+2^{n-1}} &= x_i + (x_i^2 \vee C_{k_i}) + (x_{i+1}^2 \vee C_{k_{i+1}}) + \ldots + (x_{i+2^{n-1}-1}^2 \vee C_{k_{i+2^{n-1}-1}}) \\
&= x_i + \sum_{j=0}^{2^{n-1}-1} (x_{i+j}^2 \vee C_{k_{i+j}}) \ mod \ 2^n,
\end{aligned}
$$

where $i+j$ is modulo m. To prove $F(x)$ is a single cycle T-function, it only needs to prove $x_{i+2^{n-1}} \neq x_i \ mod \ 2^n$, which equals to testify

$$\sum_{j=0}^{2^{n-1}-1} (x_{i+j}^2 \vee C_{k_{i+j}}) = \sum_{t=0}^{2^{n-l-1}-1} \sum_{j=0}^{2^l-1} (x_{2^l t+j}^2 \vee C_{k_j}) = \sum_{j=0}^{2^l-1} \sum_{t=0}^{2^{n-l-1}-1} (x_{2^l t+j}^2 \vee C_{k_j}) = 2^{n-1} \ mod \ 2^n.$$

Firstly we prove that when theorem conditions are met, for any initial state, $F(x)$ can always generate single cycles. We prove it by using dual induction on n and l.

1) When $n=4, l=1$ and $n=5, l=2$, using enumeration, it can be verified that the conclusion is established.

2) Assume the conclusion holds when it comes to $n(n>5)$ and $l(2<l\leq n-3)$, then

$$\sum_{t=0}^{2^{n-l-1}-1} \sum_{j=0}^{2^l-1} (x_{2^l t+j}^2 \vee C_{k_j}) = \sum_{j=0}^{2^l-1} \sum_{t=0}^{2^{n-l-1}-1} (x_{2^l t+j}^2 \vee C_{k_j}) = 2^{n-1} \ mod \ 2^n.$$

At this time $F(x) \ mod \ 2^n$ is a single cycle T-function for some fixed initial state, and the sequence $\{(x_i)\}$ generated by $F(x)$ satisfies $x_{i+2^{n-1}} = x_i \oplus 1$.

a) when it comes to $n+1$ and l,

$$
\begin{aligned}
&\sum_{j=0}^{2^l-1} \sum_{t=0}^{2^{n-l}-1} (x_{2^l t+j}^2 \vee C_{k_j}) \\
&= \sum_{j=0}^{2^l-1} \left(\sum_{t=0}^{2^{n-l-1}-1} (x_{2^l t+j}^2 \vee C_{k_j}) + \sum_{t=2^{n-l-1}}^{2^{n-l}-1} (x_{2^l t+j}^2 \vee C_{k_j}) \right) \\
&= \sum_{j=0}^{2^l-1} \sum_{t=0}^{2^{n-l-1}-1} (x_{2^l t+j}^2 \vee C_{k_j}) + \sum_{j=0}^{2^l-1} \sum_{t'=0}^{2^{n-l-1}-1} (x_{2^l t'+j+2^{n-1}}^2 \vee C_{k_j}) \qquad \text{(I)}
\end{aligned}
$$

where x_i is modulo 2^{n+1} and the subscript j of C_{k_j} is modulo 2^l.

By the induction hypothesis, $\sum_{j=0}^{2^l-1}\sum_{t=0}^{2^{n-l-1}-1}(x^2_{2^l t+j} \vee C_{k_j}) = 2^{n-1}\ mod\ 2^{n+1}$, and $x_{2^l t+2^{n-1}+j} = x_{2^l t+j} \oplus 1$. So $\{(x_{2^l t'+j+2^{n-1}})\}\ mod\ 2^n$ is also a single cycle T-function,(I)$= 2^{n-1} + 2^{n-1} = 2^n\ mod\ 2^{n+1}$. Hence the conclusion is true for $n+1$ and l.

b) When it comes to n and $l+1$,

$$\begin{aligned}
&\sum_{t=0}^{2^{n-l-1}-1}\sum_{j=0}^{2^{l+1}-1}(x^2_{2^{l+1}t+j} \vee C_{k_j}) \\
&= \sum_{t=0}^{2^{n-l-2}-1}\Big(\sum_{j=0}^{2^l-1}(x^2_{2^{l+1}t+j} \vee C_{k_j}) + \sum_{j=2^l}^{2^{l+1}-1}(x^2_{2^{l+1}t+j} \vee C_{k_j})\Big) \\
&= \sum_{t=0}^{2^{n-l-2}-1}\sum_{j=0}^{2^l-1}(x^2_{2^{l+1}t+j} \vee C_{k_j}) + \sum_{t=0}^{2^{n-l-2}-1}\sum_{j'=0}^{2^l-1}(x^2_{2^{l+1}t+j'+2^l} \vee C_{k_{j'+2^l}})\ mod\ 2^n
\end{aligned} \tag{II}$$

where x_i is modulo 2^n, and the subscript j of C_{k_j} is modulo 2^{l+1}.

Noted here requires $l-1 \le n-3$, might as well let $l-1 = n-3$. Then for $s > n$, the conclusion can be obtained by using induction on n.

It is easy to know, there are $2^l t$ elements between $x_{2^l t+j}$ and $x_{2^{l+1}t+j}$, and m is a factor of $2^l t$. Thus $\sum_{t=0}^{2^{n-l-2}-1}\sum_{j=0}^{2^l-1}(x^2_{2^{l+1}t+j} \vee C_{k_j}) = 2^{n-2}\ mod\ 2^n$, $x_{2^l t+2^{n-1}+j} = x_{2^l+j} \oplus 1$, and for the same reason, $\sum_{t=0}^{2^{n-l-2}-1}\sum_{j'=0}^{2^l-1}(x^2_{2^{l+1}t+j'+2^l} \vee C_{k_{j'+2^l}}) = 2^{n-2}\ mod\ 2^n$.

Note that in condition 2) , different adjacent $[C_{k_i}]_3$ ensures the next state differs from the previous, and at this time $l-1 \le n-3$, so these $< C_k >$ would not carry 2^{n-2}. Condition 3) is set to meet the definition of induction. Thus when it comes to n and $l+1$, (II)$= 2^{n-2} + 2^{n-2} = 2^{n-1}\ mod\ 2^n$, and the conclusion is true.

Therefore, for any positive integer n and l, $\sum_{j=0}^{2^{n-1}-1}(x^2_{i+j} \vee C_{k_{i+j}}) = 2^{n-1}\ mod\ 2^n$. $F(x)$ is a single cycle T-function of period 2^n for any initial state.

Secondly, we give the proof that these m cycles are pairwise different.

Make the residue system $\{x_0^0, x_0^1, \dots, x_0^{m-1}\}$ modulo m initial states, where $x_0^i = 0, 1, \dots, m-1 (i = 0, 1, \dots, m-1)$, when $i \ne j\ mod\ m$, $x_0^i \ne x_0^j\ mod\ m$.

Consider $F(x)$ is a single cycle T-function, so all the states modulo m will appear on the cycle generated by $F(x)$). Therefore, any arbitrary state can be the initial sate, and for the same initial states x_0^i modulo m, they generate the exactly same single cycle.

Since every component function is pairwise different, at least two states x_i, x_j might be found which satisfy $f_{k_i}(x_i) \neq f_{k_j}(x_i)(i \neq j\ mod\ m)$. Thus for different initial states x_0^i, x_0^j, it is able to find such a state which has different subsequent states on the two cycles they generated. Therefore, for different initial states x_0^i and x_0^j modulo m, they generate totally different single cycles.

In summary, these m single cycles are different from each other. ♯ □

We give an explanation of Theorem 3: The key to the new construction lies in the elements of ordered array $< C_k >=< C_0, C_1, \ldots, C_{m-1} >$. Let $C_k = 2^{n-1}C_k^{n-1} + 2^{n-2}C_k^{n-2} + \ldots + 2C_k^1 + C_k^0$. We call $C_k^i(i = 0, 1, \ldots, n-1)$ as the i-th bit of C_k.

Condition 1) $\Longleftrightarrow$ $f_{k_i}(x_i)$ is a single cycle T-function of modulo 8 congruence, which is equivalent to weaving the sequences generated by component single cycle T-functions to obtain a new one.

Condition 2) $\Longleftrightarrow$ In the $3rd$-bit of C_k, "0" and "1" appears alternately, and for the $l+1$-th bit of all the C_k, their xor sum is 0. The former is to change the parity of the $3rd$-bit to ensure a state transition; the latter is to guarantee that when the induction is made from l to $l+1$, it would not result in a carry 2^{n-2}.

Condition 3)$\Longleftrightarrow$ When $3 \leq l \leq n-3$, for the remaining $l-3$ bits in the middle, divide C_k into m groups according to the j-th bit, and every group has $t(2 < t < l)$ elements. It is satisfied that from any C_k, the xor sum of t consecutive j-th bits is 0.

In fact, to achieve the target above, the order of bit "0" and "1" in every group should be exactly the same. However, we can compare t to the size of sliding window.

Example 1: Let $n = 7, m = 15, l = 4$. For

$$< C_k >=< 21, 61, 101, 45, 53, 93, 69, 13, 85, 125, 37, 109, 117, 29, 5, 77 >,$$

every component function $f_{k_i}(x_i) = x_i + (x_i^2 \vee C_{k_i})\ mod\ 2^n$ is a single cycle T-function, and for any initial state $0, 1, \ldots, 2^n - 2, 2^n - 1$,

$$F(x) : x_{i+1} = x_i + (x_i^2 \vee C_{k_i})\ mod\ 2^n, k_{i+1} = k_i + 1\ mod\ m$$

is always a single cycle T-function. See Figure 1.

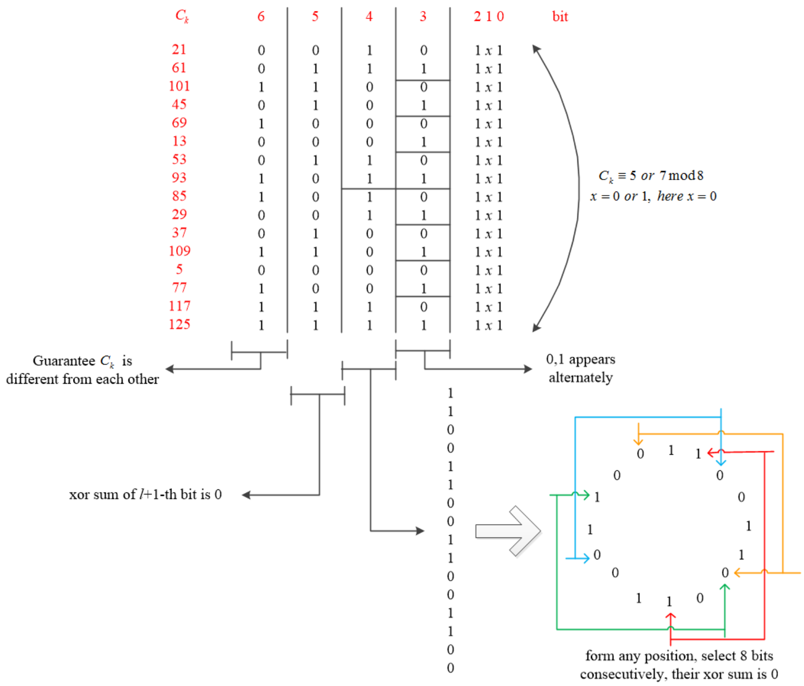


Figure 1: example of new construction

Corollary 1. For the sequence $\{(x_i)\}$ defined as (1) and $m \in N^*, m = 2^l m' (0 \leq l \leq n-3)$, where m' is an odd number. If one of the following situations is true, then the sequence of pairs $\{(x_i, k_i)\}$ has the maximal period $m' 2^n$. And at the same time, for different initial state x_0 modulo 2^l, there are 2^l pairwise different cycles:

1) arrangement $< C_k >$ can be divided into m' groups $< C_k^{i_0} >, < C_k^{i_1} >, \ldots, < C_k^{i_{m'-1}} >$ with each group has 2^l elements, and in any group of $< C_k^{i_t} >$ $(t = 0, 1, \ldots, m'-1)$, $C_k^{i_t}$ satisfies conditions in Theorem 3, meanwhile, these m' functions determined by $< C_k^{i_t} >$ satisfy conditions in Lemma 2;

2) arrangement $< C_k >$ can be divided into 2^l groups $< C_k^{j_0} >, < C_k^{j_1} >, \ldots, < C_k^{j_{2^l-1}} >$ with each group has m elements, and in any group of $< C_k^{j_s} >$ $(s = 0, 1, \ldots, 2^{l-1})$, satisfies conditions in Lemma 2, meanwhile, these 2^l functions determined by $< C_k^{j_s} >$ satisfy conditions in Theorem 3.

The proof is quite apparently due to Lemma 2 together with Theorem 3.

4. Analysis of the newly constructed T-function families

4.1. Numeration

Next we give a numeration of the newly constructed single cycle T-function families. Every bit of C_k and its count of corresponding feasible options according to Theorem 3 are as Table 1:

Table 1: numeration of newly constructed single cycle T-functions

$[C_k]_j$	0,1,2	3	4	5	$\ldots$	j	$\ldots$	l	$l+1$	$l+2,\ldots,n-1$
options	2	2	C_8^4	C_{16}^8	$\ldots$	$C_{2^{l-1}}^{2^{j-2}}$	$\ldots$	$C_{2^{l-1}}^{2^{l-2}}$	$C_{2^l}^{2^{l-1}}$	2^{n-3-l}

Theorem 4. (Numeration) Using Theorem 3,

$$2 \cdot 2 \cdot C_8^4 \cdot C_{16}^8 \cdot \cdots C_{2^l}^{2^{l-1}} \cdot 2^{n-3-l} = 2^{n-1-l} \prod_{i=3}^{l} C_{2^i}^{2^{i-1}}$$

single cycle T-functions can be obtained.

4.2. Cryptographic Properties

Theorem 3 is a construction method based on K-S single cycle T-functions, using only two arithmetic operations(addition and multiplication) and one logical operation(OR). And three primitive operations is also the lower bound of a nonlinear single cycle T-function could have[1]. At the same time, a number of single cycle T-functions can be obtained at one time according to the selection of $< C_k >$ and initial input states. The essence of this method is to weave and re-arrange the output sequences of multiple original component single cycle

T-functions. In addition, the multiplication operation enhances the statistical properties, and the logical operation increases the algebraic order of the square operation, which both better guarantee the security of the newly get functions.

For a sequence output from some general single cycle T-function, Theorem 2 gives its linear complexity and the upper bound of the minimum error of k-error linear complexity. This conclusion also applies to the newly constructed functions from Theorem 3. That is, for any single cycle T-function obtained by Theorem 3, its linear complexity is $n \times 2^{n-1} + n$, and its minimum error $\leq 2^{n-1}$(when $n = 2^t$,the equality holds).

In summary, the construction of only three primitive operations makes the new methods in Theorem 3 more efficient in software, and in the meantime, the newly generated sequences preserve quite high linear complexity and good stability as well.

4.3. Comparison with other construction methods

At last, we give an comparison about our method and the other existing T-function construction methods as Table 2.

Table 2: comparisons with currently known other four methods

Method	Ideal	Advantages	Shortcomings
Parameter	Recursive thought, the parameter is actually a particular T-function whose j-th output bit only related to the previous j bits input	Perfect theoretical basis	Depends on the elaborate construction of parameters
Algebraic dynamical system	Using non - Archimedes analysis theory	Broader theoretical vision and more general approach	Difficult practical implementation
Polynomial	It is widely used and requires large cycles; addition and multiplication are natural T-functions	Large optional space and easy to get	Poor non-linearity with significant security weaknesses
Multiword single cycle T-function	Promotion of single circle T-functions	Widely used in practical algorithm's design	Same as parameter method
Theorem 3	Re-weave of the existing T-function's output sequence	Fast software implementation, high efficiency, not bad security	A storage of single cycle T-functions is needed

5. Conclusion

In this paper, we propose a method using m single cycle T-functions satisfying certain conditions of period 2^n to construct m new and distinct pairwise single cycle T-functions of period 2^n, where $m = 2^l (l \in N^+)$. Then, the numeration, linear complexity and stability of the newly constructed functions is investigated. Finally, we compare our method with the existing construction approaches. It is a kind of efficient, simple and easy-to-do method, and is provided with a large optional parameter space. Furthermore, by applying this construction method for other functions, we may get a lot of new function families.

Acknowledgements. This work was supported by the National Natural Science Foundation of China [grant numbers 61502524].

References

[1] *A. Klimov, A. Shamir, A new class of invertible mappings, in: Proceedings of Cryptographic Hardware and Embedded Systems Workshop, CHES 2002, Springer-Verlag, Berlin, 2003, pp. 470–483.*

[2] *D. Magnus, Narrow t-functions, in: H.Gilbert, H.Handschuh (Eds.), Fast Software Encryption, Vol. 3557, FSE 2005, Springer-Verlag, Berlin, 2005, pp. 50–67.*

[3] *W. Y. Zhang, C. K. Wu, The algebraic normal form, linear complexity and k-error linear complexity of single cycle t-function, in: Proceedings of SETA 2006, Vol. 4086, SETA 2006, Springer-Verlag, Berlin, 2006, pp. 391–401.*

[4] *T. Shi, V. Anashin, D. D. Lin, Linear Relation on General Ergodic T-function.* doi:https://arxiv.org/abs/1111.4635v1.

[5] *S. R. Min, On some properties of a single cycle t-function and examples, J Chungcheong Math Soc 23 (4) (2010) 885–892.*

[6] *J. S. Wang, W. F. Qi, Linear equation on polynomial single cycle t-functions, in: Proceedings of SKLOIS Conference on Information Security*

and Cryptology Workshop, Inscrypt 2007, Springer-Verlag, Berlin, 2008, pp. 256–270.

[7] *X. J. Luo, B. Hu, S. S. Hao, et al, The stability of output sequences of single cycle t-function, J Electro Inf Technol 33 (10) (2011) 2328—2333.*

[8] *Y. W. anf Y. P. Hu, W. Z. Zhang, Cryptographic properties of truncated sequence generated by single cycle t-function, J Info Comput Sci 10 (2) (2013) 461—468.*

[9] *W. You, W. F. Qi, The 2-adic complexity and the 1-error 2-adic complexity of single cycle t-functions, J China Institute Commun 35 (3) (2014) 136—139.*

[10] *A. M. Rishakani, S. M. Dehnavi, M. R. Mirzaee, et al, Statistical Properties of Multiplication mod 2^n. doi:http://eprint.iacr.org.2015/201.*

[11] *N. Kolokotronis, Cryptographic properties of stream ciphers based on t-functions, IEEE Trans Inf Theory (2006) 1604–1608.*

[12] *B. B. 131.0-B-1, Tm synchronization and channel coding (2003).*

[13] *J. Hong, D. Lee, Y. Yeom, et al, A new class of single cycle t-functions, in: Proceedings of Fast Software Encryption Workshop, FSE 2005, Springer-Verlag, Berlin, 2005, pp. 68–82.*

[14] *A. Klimov, A. Shamir, Cryptographic applications of t-functions, in: Proceedings of Selected Areas in Cryptography Workshop, SAC 2003, Springer-Verlag, Berlin, 2004, pp. 248–261.*

[15] *X. Yang, C. K. Wu, Y. X. Wang, On the construction of single cycle t-functions, J China Institute Commun 32 (5) (2011) 162–168.*

[16] *V. Anashin, Uniformly distributed sequences over p-adic integers, ii, Discret Math Appl 12 (6) (2002) 527–590.*

[17] M. V. Larin, Transitive polynomial transformations of residue class rings, Discret Math Appl 12 (2) (2002) 127–140.

[18] A. Klimov, A. Shamir, New cryptographic primitives based on multiword t-functions, in: Proceedings of Fast Software Encryption Workshop, FSE 2004, Springer-Verlag, Berlin, 2004, pp. 1–15.

[19] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, the 5th edition Edition, CRC Press, Florida, 1996.

[20] M. Stamp, C. F. Martin, An algorithm for the k-error linear complexity of binary sequences with period 2^n, IEEE Trans. Inform. Theory 39 (4) (1993) 1398–1401.

[21] J. Liu, X. B. Fan, C. K. Wu, On the linear complexity of output sequence of single cycle t-function, Journal Graduate University of Chinese Academy of Sciences 29 (3) (2012) 429–432.

Appendix A.

Taking $m = 4, n = 5$ as an example, the construction is given as follows. Select $C_k =< 5, 13, 21, 29 >$, then the component functions are

$$\begin{aligned} f_{k_0} &= x + (x^2 \vee 5)\ mod\ 2^5,\ f_{k_1} = x + (x^2 \vee 13)\ mod\ 2^5, \\ f_{k_2} &= x + (x^2 \vee 21)\ mod\ 2^5, f_{k_3} = x + (x^2 \vee 29)\ mod\ 2^5. \end{aligned}$$

Sequences generated by f_{k_0}, f_{k_1}, f_{k_2} and f_{k_3} are as follows. Figure A.2 which has red numbers with black solid circle is generated by f_{k_0}, figure A.3 which has blue numbers with black hollow circle is generated by f_{k_1}, figure A.4 which has yellow numbers with grey solid circle is generated by f_{k_2}, figure A.5 which has green numbers with green hollow circle is generated by f_{k_3}. Numbers in brackets outside the cycle are the current states, and numbers inside the cycle are the serial numbers of the states (0 stands for the initial state).

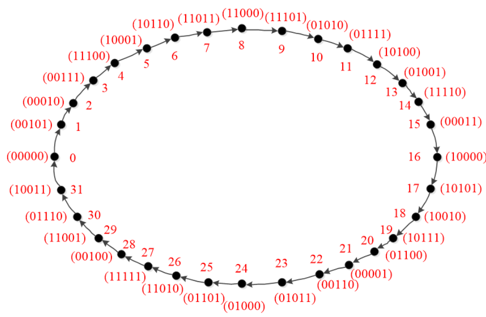


Figure A.2: cycle structure of f_{k_0}

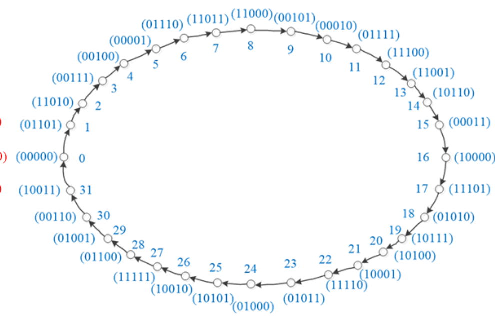


Figure A.3: cycle structure of f_{k_1}

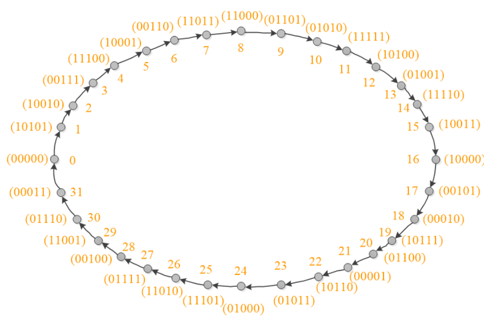


Figure A.4: cycle structure of f_{k_2}

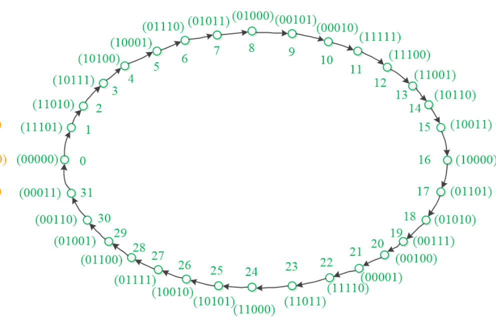
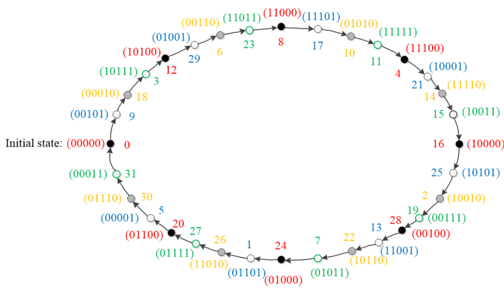


Figure A.5: cycle structure of f_{k_3}

When $x_{i+1} = x_i + (x_i^2 \vee C_{k_i}) \ mod \ 2^5, C_k =< 5, 13, 21, 29 >, k_{i+1} = k_i + 1 \ mod \ 4$ respectively takes (00000), (00001), (00010) and (00011) as its initial state, it generates cycles as figure A.6, A.7, A.8 and A.9 below. Red numbers with black solid circle are the output of f_{k_0}, blue numbers with hollow circle are the output of f_{k_1}, yellow numbers with grey solid circle are the output of f_{k_2}, green numbers with green hollow circle are the output of f_{k_3}. And numbers inside the cycles are serial numbers in their original component functions. It is obviously to see that for an ordered $< C_k >$, states selected from each component functions are fixed, it is just the combination order that different.



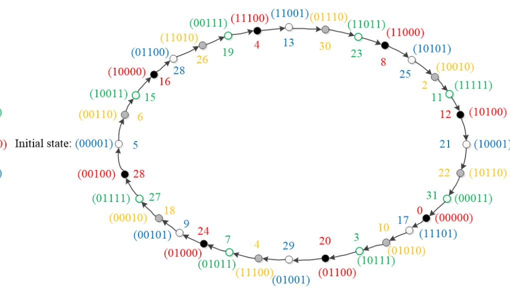
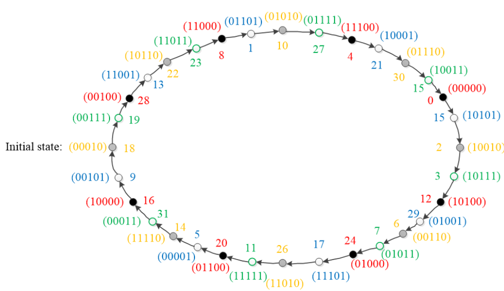


Figure A.6: output of initial state "0"

Figure A.7: output of initial state "1"



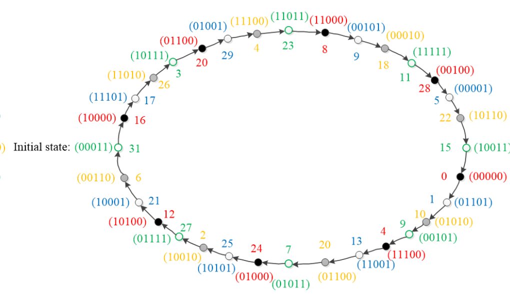


Figure A.8: output of initial state "2"

Figure A.9: output of initial state "3"