SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

New construction of single cycle T-function families

Shiyi ZHANG[1], Yongjuan WANG[2*] & Guangpu GAO[3]

PLA University of Foreign Language, Language Enigneering Department, Luoyang 471003, *China*

Received ; accepted

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, we present a new construction using a class of single cycle T-functions meeting certain conditions to construct a family of new single cycle T-functions, and we also give the numeration lower bound for the newly constructed single cycle T-functions.

Keywords cryptography, permutation function, single cycle T-function, numeration, dictionary order

Citation ZHANG S Y, WANG Y J, GAO G P. New construction of single cycle T-function families. Sci China Inf Sci, 2016, 59(1): , doi:

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 also has played an important role in the analysis of public key cryptography and the construction of special code in communication system. In 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, since its introduction, has gained much attention. In [2–6], researches on the cycle structure of T-functions were conducted; [7–11] examined configuration of sequences derived from T-functions; while properties of these sequences were discussed in [12–15]. However, in recent years, with further studies on T-functions, new research perspectives have been brought up. Rishakani introduced a family of T-functions similar to modular multiplication, which is called M-functions[16]; Liu proposed a fast algorithm for computing walsh spectrum and differential probability of T-functions[17], and You discussed the 2-adic complexity and the 1-error 2-adic complexity of single cycle T-functions[18], etc.

Current 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

* Corresponding author (email: pinkywyj@163.com)

[19]. By using parameters, single-word single cycle T-functions can be constructed, such as the Klimov-Shamir T-function [1] and the functions proposed by Yang [20]. 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 [21]. 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 easy-to-use. The third is polynomial functions. The necessary and sufficient conditions of a single cycle function is a polynomial function $f(x) = \sum_{k\geqslant 0} a_k x^k$ over $\mathbb{Z}/(2^n)$ was given [23–25]. The forth is multiword single cycle T-functions. It was first introduced by Klimov and Shamir in [25], then more and more multiword single cycle T-functions were proposed and had wide applications in cipher design. For example, Mir-1 uses the multiword single cycle T-function proposed in [26], while TSC series ciphers are based on the T-function introduced in [27]. 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 increase the period of single cycle T-functions[19]. Using its idea of construction, this paper discovered a new construction of single cycle T-functions. Using several single cycle T-functions which meet certain conditions, it is able to construct new single cycle T-function families. Meanwhile, we give the proof by induction and the numeration lower bound for this construction.

2 Notations and Definitions

Definition 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 $x_i = (x_{i,0}, \ldots, x_{i,m-1})$, $y_i = (y_{i,0}, \ldots, y_{i,n-1})$. Let f be a mapping from $\mathbb{F}_2^{mn}$ to $\mathbb{F}_2^{ln}$, that is

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

for $0 \leqslant j \leqslant n-1$, if the j-th column of the output $\mathbf{R}_j(y)$ depends only on the first j 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. 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 $i \geqslant 0$, 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.

Theorem 1. Let $f(x) = (f_{n-1}(x), \ldots, f_1(x), f_0(x))$ be an invertible T-function over $\mathbb{F}_2^n$, then $f(x)$ is a single cycle T-function if and only if its ANF(Algebraic Norm Form) has the following form

$$\begin{aligned} f(x) &= (f_{n-1}(x), \ldots, f_1(x), f_0(x)) \\ &= (x_{n-1} \oplus x_0 x_1 \ldots x_{n-2} \oplus \varphi_{n-1}(x_{n-2}, \ldots, x_1, x_0), \ldots, x_1 \oplus x_0 \oplus \varphi_1(x_0), x_0 \oplus 1), \end{aligned}$$

where $f_j(x) = x_j \oplus x_0 x_1 \ldots x_{j-1} \oplus \varphi_j(x_{j-1}, \ldots, x_1, x_0)$, $deg(\varphi_j \leqslant j-1)$, $j \geqslant 1$.

Theorem 2. Let 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 $\underline{x}$, $\underline{x}_j (0 \leqslant j \leqslant n-1)$ has the period of 2^{j+1}. Meanwhile, for $0 \leqslant j \leqslant n-1$, the two parts of the sequence $\underline{x}_j$ are complementary, that is $x_{i+2^j,j} = x_{i,j} \oplus 1, i \geqslant 0$.

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. The mapping $f(x) = x + (x^2 \vee C)\ mod\ 2^n$ is invertible if and only if $[C]_0 = 1$. For $n \geqslant 3$, $f(x)$ 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 [19]. 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

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

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

Lemma 2. 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, $[C_k]_0 = 1$, $\oplus_{k=0}^{m-1}[C_k]_2 = 1$.

3 The New Construction

Unlike [19], which used odd invertible functions to increase the period of T-functions, during our study on the construction of single cycle T-functions, 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 meeting certain conditions of period 2^n, we can construct m pairwise different new single cycle T-functions of period 2^n.

Assume $F(x)$ is the corresponding function to the sequence $\{(x_i)\}$ defined by (1), the component functions are $f_{k_i}(x_i) = x_{i+1}$, $k_{i+1} = k_i + 1\ mod\ m$, $k = 0, \ldots, m-1$.

Theorem 3 (New Construction). When $m = 2^l$, if each component function $f_{k_i}(x_i)$ is a single cycle T-function and the ordered set $< C_k >$ simultaneously satisfies

1) for all k, C_k is congruence modulo 8;

2) for $i = 0, 1, \ldots, m-1$, $[C_{k_i}]_3 \oplus [C_{k_{i+1}}]_3 = 1$, $\oplus_{j=0}^{2^{r-1}-1}[C_{k_{i+j}}]_{r+1} = 0 (2 < r < l)$, $\oplus_{i=0}^{m-1}[C_{k_i}]_{n-2} = 0$; then for different input initial state x_0 modulo m, $F(x)$ can generate m pairwise different single cycle T-functions of period 2^n, where $n \geqslant 4$, $1 \leqslant l \leqslant n-3$.

Proof. First we determine the ranges of n and l.

Note that each $f_{k_i}(x_i)$ is a single cycle T-function and is congruence modulo 8, so for all k, C_k simultaneously satisfies $C_k\ mod\ 8 = 5$ or 7, thus $n \geqslant 3$. Trivially, $l \geqslant 1$, that is $m \geqslant 2$. Also, since C_k is different from each other, $l \leqslant n-3$, $n \geqslant 4$, thus we have $1 \leqslant l \leqslant n-3$.

Then, 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 $i + j$ needs modulo m. To prove $F(x)$ is a single cycle T-function, we only need to prove that $x_{i+2^{n-1}} \neq x_i\ mod\ 2^n$. And as the property of the sequence generated by single cycle T-functions, it's only necessary to prove that$\sum_{j=0}^{2^{n-1}-1}(x_{i+j}^2 \vee C_{k_{i+j}}) = 2^{n-1}\ mod\ 2^n$.

For $\sum_{j=0}^{2^{n-1}-1}(x_{i+j}^2 \vee C_{k_{i+j}}) = \sum_{t=0}^{2^{n-l-1}-1}\sum_{j=0}^{2^l-1}(x_{2^l t+j}^2 \vee C_{k_j}) = \sum_{j=0}^{2^l-1}\sum_{t=0}^{2^{n-l-1}-1}(x_{2^l t+j}^2 \vee C_{k_j})\ mod\ 2^n$, it suffices to show that $\sum_{t=0}^{2^{n-l-1}-1}\sum_{j=0}^{2^l-1}(x_{2^l t+j}^2 \vee C_{k_j}) = \sum_{j=0}^{2^l-1}\sum_{t=0}^{2^{n-l-1}-1}(x_{2^l t+j}^2 \vee C_{k_j}) = 2^{n-1}\ mod\ 2^n$.

1. Firstly we prove that when theorem conditions are met, for any initial state, $F(x)$ can always generate single cycles. We prove it by dual induction on n and l. Let s and l denote the value of n and l, respectively.

1) When $s=4$, $l=1$, we have the conclusion by enumeration.

2) Assume by the induction that the conclusion is true when $s=n$ and $r=l$, that is $\sum_{t=0}^{2^{n-l-1}-1}\sum_{j=0}^{2^l-1}(x^2_{2^l t+j}\vee C_{k_j})=\sum_{j=0}^{2^l-1}\sum_{t=0}^{2^{n-l-1}-1}(x^2_{2^l t+j}\vee C_{k_j})=2^{n-1}\ mod\ 2^n$,

a) when $s=n+1$, $r=l$,

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

where x_i is modulo 2^{n+1} and the subscript j of C_{k_j} is modulo 2^l. Hence the conclusion is true for $s=n+1$, $r=l$.

b) When $s=n$, $r=l+1$,

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

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

It should be noted that due to the theorem condition $l\leqslant n-3$, in this part of the proof, we require $l-1\leqslant n-3$. We might as well let $l-1=n-3$, then for $s>n$, we can have the conclusion by induction on n.

From the induction on l, we can separate $<C_{k_j}>$ and $<C_{k_{j'+2^l}}>$ into two independent constant sets which both meet the suppose, and their values are different from each other. Therefore, both $x_{2^{l+1}t+j}$ and $x_{2^{l+1}t+j'+2^l}$ can traverse all the states modulo 2^{n-1}, which makes the value of (2) irrelevant to the order of the subscript of x_i. And according to the induction on n, we have

$$\sum_{t=0}^{2^{n-l-2}-1}\sum_{j=0}^{2^l-1}(x^2_{2^{l+1}t+j}\vee C_{k_j})=\sum_{t=0}^{2^{n-l-2}-1}\sum_{j'=0}^{2^l-1}(x^2_{2^{l+1}t+j'+2^l}\vee C_{k_{j'+2^l}})=2^{n-2}\ mod\ 2^{n-1},$$

thus the left part of (2) equals to $2^{n-2}+2^{n-2}+\alpha(2^{n-1})=2^{n-1}+\alpha(2^{n-1})\ mod\ 2^n$, where $\alpha(2^{n-1})$ stands for the carry carried by $\sum_{t=0}^{2^{n-l-2}-1}\sum_{j=0}^{2^l-1}(x^2_{2^{l+1}t+j}\vee C_{k_j})$ and $\sum_{t=0}^{2^{n-l-2}-1}\sum_{j'=0}^{2^l-1}(x^2_{2^{l+1}t+j'+2^l}\vee C_{k_{j'+2^l}})$ after 2^{n-2} iterative additions respectively. Note that C_k is congruence modulo 8, it is also required to consider that after iterative additions whether there will be a carry generated by the $3rd$ bit to the $(n-2)$-*th* bit. (Remark the least bit is the 0-*th* bit)

Apparently, when $<C_k>$ meets the theorem conditions, there won't be a carry to the $(n-1)$-*th* bit. Meanwhile, it's easy to show for any $x\in\mathbb{Z}$, the binary expansion of x^2 must have $[x^2]_1=0$, thus $[x^2\vee C]_0=[x^2\vee C]_2=1$, $[x^2\vee C]_1=[C]_1$. At the same time, different adjacent $[C_{k_i}]_3$ ensures the next state differs from the previous state.

So when $s = n$, $r = l + 1$,

$$\sum_{t=0}^{2^{s-r-1}-1} \sum_{j=0}^{2^r-1} (x^2_{2^{l+1}t+j} \vee C_{k_j}) = \sum_{t=0}^{2^{n-l-2}-1} \sum_{j=0}^{2^{l+1}-1} (x^2_{2^{l+1}t+j} \vee C_{k_j}) = 2^{n-1} \ mod \ 2^n,$$

and the conclusion is true for the case $s = n$, $r = l + 1$.

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

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

Make the residue system $\{x^0_0, x^1_0, \ldots, x^{m-1}_0\}$ modulo m initial states, where $x^i_0 = 0, 1, \ldots, m-1 (i = 0, 1, \ldots, m-1)$, when $i \neq j \ mod \ m$, $x^i_0 \neq x^j_0 \ mod \ m$. Consider $F(x)$ is a single cycle T-function, so all the states modulo m will appear on the cycle generated by $F(x)$). We might as well assume these states are in dictionary order, then the state x^i_0 will always be the input of the component function $f_{k_{imodm}}(x_i)$. Thus in a single cycle, we can always make an arbitrary state the initial sate, it generates a single cycle. So, for the same initial states x^i_0 modulo m, they generate the exactly same single cycle.

Since each component function is different T-function, we can at least find two states x_i, x_j, so that $f_{k_i}(x_i) \neq f_{k_j}(x_i)(i \neq j \ mod \ m)$. Thus for different initial states x^i_0, x^j_0, we are able to find such a state which has different subsequent states on the two cycles they generated. Therefore, for different initial states x^i_0 and x^j_0 modulo m, they generate totally different single cycles.

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

Corollary 1. When $< C_k >, k = 0, 1, \ldots, m-1$ is in dictionary order, $F(x)$ generates m new pairwise different single cycles.

Proof. Apparently, dictionary order satisfies the conditions in **Theorem 3**, so the conclusion is true. ♯

According to **Theorem 3**, we can give a numeration lower bound N for this construction. Easy to know when we construct cycles in dictionary order, the lower bound is reached.

Theorem 4. Given the same conditions as **Theorem 3**, sort m in dictionary order, we can get $C^m_{2^n}$ cases. Consider rotation, we have $N \geqslant mC^m_{2^n}$.

Obviously, a large number of single cycle T-functions can be constructed though this method.

Corollary 2. When $m = 2^l$, if for all k,

1) each component function $f_{k_i}(x_i)$ is a single cycle T-function,

2) C_k is congruence modulo 2^m,

then, for different initial state x_0 modulo m, $F(x)$ can generate m pairwise different single cycle T-functions of period 2^n, where $n \geqslant 4$, $1 \leqslant l \leqslant n - m$. Note here $\{C_k\}$ is out-of-order.

Proof. Similar to the proof procedure of **Theorem 2**, it only needs to consider the induction part on l. According to the induction hypothesis, if and only if for all k, C_k is congruence modulo 2^m, when we take 2^l C_{k_i} in arbitrary order, it won't carry 2^{n-1} from the $3rd$ bit to the $(n-2)$-th bit after iterative additions. ♯

Through the method proposed in **Corollary 2**, $2 \cdot 2^{m-3} \cdot C^m_{2^{n-m}} = 2^{m-2} C^m_{2^{m-3}}$ new single cycles can be constructed.

Theorem 5. For any m, might as well let $m = 2^l m'$, $0 \leqslant l \leqslant n - m$, where m' is an odd number. If each component function $f_{k_i}(x_i)$ is a single cycle T-function and for all k, C_k is congruence modulo 2^m, then the sequence of pairs $\{(x_i, k_i)\}$ has the maximal period of $m'2^n$. At the same time, for different initial state x_0 modulo 2^l, there are 2^l pairwise different cycles.

Proof. It's easy to prove by **Lemma 2** and **Corollary 2**. ♯

4 Conclusion

In this paper, we summarize the existing construction methods of single cycle T-functions, and propose a method using m single cycle T-functions meeting certain conditions of period 2^n to construct m new and distinct pairwise single cycle T-functions of period 2^n, where $m = 2^l (l \in \mathbb{N}^+)$. The newly constructed single cycle T-functions have preserved all the information inherited from the original component functions, 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 No. 61502524).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Klimov A, Shamir A. A new class of invertible mappings. In: Proceedings of Cryptographic Hardware and Embedded Systems Workshop, CHES 2002. Berlin: Springer-Verlag, 2003, 470-483
2 Zhang W Y, Wu C K. The Algebraic Normal Form, Linear Complexity and k-error Linear Complexity of Single Cycle T-function. In: Proceedings of SETA 2006. LNCS, Vol. 4086. Berlin, Springer-Verlag, 2006, 391-401.
3 Luo Y L, Qi W F. On the Algebraic Structure of Klimov-Shamir T-function. J China Institute Commun, 2008, 29(10): 143-148
4 Min S R. On Some Properties of a Single Cycle T-function and Examples. J Chungcheong Math Soc, 2010, 23(4): 885-892
5 Shi T, Anashin V, Lin D D. Linear Relation on General Ergodic T-function. 2011, http://arxiv.org/abs/1111.4635v1
6 Luo X J, Hu B. Cycle Structure Characteristic of T-functions. Comput Sci, 2011, 38(4): 137-140
7 Wang J S. Research on the Design and Analysis of Several Classes of Pseudorandom Sequence and Sequence Families. Dissertation for Ph.D. Degree. Zhengzhou: PLA Information Engineering University, 2007
8 Luo Y L, Qi W F. Pattern Distributions of Sequences Based on Single Cycle T-function. J Wuhan Univ (Nat. Sci. Ed), 2009, 55(4): 395-398
9 Luo Y L, Qi W F. DeBruijn Sequences Generated by Single Cycle T-function. J Inf Eng Univ, 2009, 10(4): 429-433
10 You W. Construction and Analysis of Sequences Derived from Single Cycle T-functions. Dissertation for Ph.D. Degree. Zhengzhou: PLA Information Engineering University, 2013
11 Liu Y, Hu B. A Class of Improved Sequences Generated by T-functions. J Cryptol Res, 2014, 1(6): 513-524
12 Zhao L, Wen Q Y. Linear Complexity and Stability of Output Sequences of Single Cycle T-function. J Beijing Univ Posts and Telecommun, 2008, 31(4): 62-65
13 Wang Y, Hu Y P, Yuan F. Autocorrelation Properties of Nonlinear Pseudorandom Sequences Output by T-functions. J Beijing Univ Posts and Telecommun, 2011, 34(2): 105-108
14 Luo X J, Hu B, Hao S S, et al. The Stability of Output Sequences of Single Cycle T-function. J Electro Inf Technol, 2011, 33(10): 2328-2333
15 Wang Y, Hu Y P, Zhang W Z. Cryptographic Properties of Truncated Sequence Generated by Single Cycle T-function. J Info Comput Sci, 2013, 10(2): 461-468
16 Rishakani A M, Dehnavi S M, Mirzaee M R, et al. Statistical Properties of Multiplication mod 2^n. http://eprint.iacr.org.2015/201
17 Liu Y, Hu B, Xu L P. Efficient algorithm for Computing Walsh Spectrum and Differential Probability. J China Institute Commun, 2015, 36(5): 1-7
18 You W, Qi W F. The 2-adic Complexity and the 1-error 2-adic Complexity of Single Cycle T-functions. J China Institute Commun, 2014, 35(3): 136-139
19 Klimov A, Shamir A. Cryptographic applications of T-functions. In: Proceedings of Selected Areas in Cryptography Workshop, SAC 2003. Berlin: Springer-Verlag, 2004, 248-261
20 Yang X, Wu C K, Wang Y X. On the Construction of Single Cycle T-functions. J China Institute Commun, 2011, 32(5): 162-168
21 Anashin V. Uniformly distributed sequences over p-adic integers, II. Discret Math Appl, 2002, 12(6): 527-590
22 Kolokotronis N. Cryptographic properties of stream ciphers based on T-functions. IEEE Trans Inf Theory, 2006, 1604-1608
23 Larin M V. Transitive polynomial transformations of residue class rings. Discret Math Appl, 2002, 12(2): 127-140
24 Wang J S, Qi W F. Linear equation on polynomial single cycle T-functions. In: Proceedings of SKLOIS Conference on Information Security and Cryptology Workshop, Inscrypt 2007. Berlin: Springer-Verlag, 2008, 256-270
25 Klimov A, Shamir A. New cryptographic primitives based on multiword T-functions. In: Proceedings of Fast Software Encryption Workshop, FSE 2004. Berlin: Springer-Verlag, 2004, 1-15
26 Blue Book 131.0-B-1. TM Synchronization and Channel Coding. USA: CCSDS, 2003
27 Hong J, Lee D, Yeom Y, et al. A new class of single cycle T-functions. In: Proceedings of Fast Software Encryption Workshop, FSE 2005. Berlin: Springer-Verlag, 2005, 68-82

Appendix A

Appendix A.1

Taking $m = 2$, $n = 4$ as an example, the construction is given as follows. Select $C_k =< 5, 13 >$, then the component functions are

$$f_{k_0} = x + (x^2 \vee 5)\ mod\ 2^4, f_{k_1} = x + (x^2 \vee 13)\ mod\ 2^4.$$

Sequences generated by f_{k_0} and f_{k_1} are as follows. **Figure 1** which has red figures with black solid circle is generated by f_{k_0}, **Figure 2** which has blue figures with black hollow circle is generated by f_{k_1}. Figures in brackets outside the cycles are the current states, and figures inside the cycles are the numbers of the states (0 stands for the initial state).

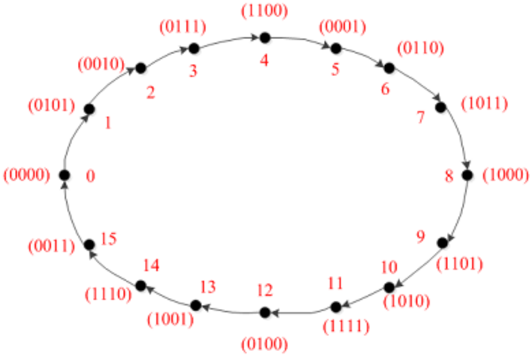

Figure 1 Cycle structure of f_{k_0}

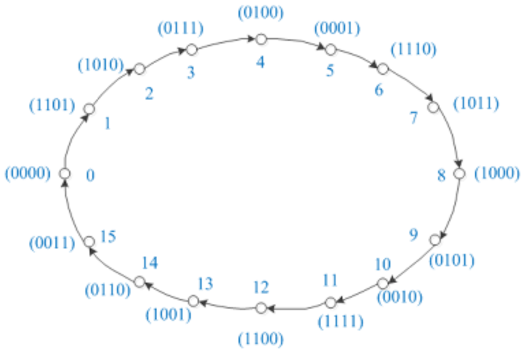

Figure 2 Cycle structure of f_{k_1}

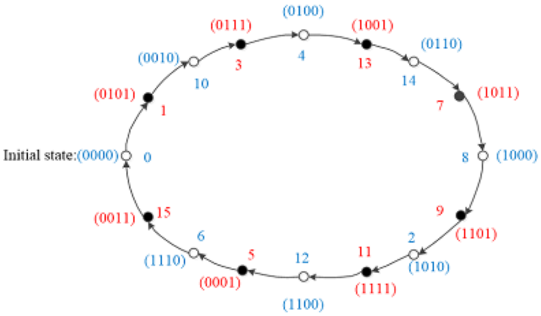

Figure 3 Output when initial state 0

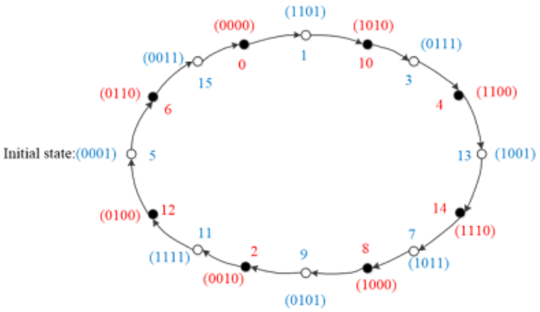

Figure 4 Output when initial state 1

When $x_{i+1} = x_i + (x_i^2 \vee C_{k_i})\ mod\ 2^4, C_k =< 5, 13 >, k_{i+1} = k_i + 1\ mod\ 2$ respectively takes (0000) and (0001) as its initial state, it generates cycles as **Figure 3** and **Figure 4** above. Red figures with black solid circle are output from f_{k_0}, blue figures with hollow circle are output from f_{k_1}, and figures inside the cycles are numbers in their original component functions. We can tell that the newly constructed cycles are recombination of the original component functions' output.

Appendix A.2

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 5** which has red figures with black solid circle is generated by f_{k_0}, **Figure 6** which has blue figures with black hollow circle is generated by f_{k_1}, **Figure 7** which has yellow figures with grey solid circle is generated by f_{k_2}, **Figure 8** which has green figures with green hollow circle is generated by f_{k_3}. Figures in brackets outside the cycle are the current states, and figures inside the cycle are the numbers of the states (0 stands for the initial state).

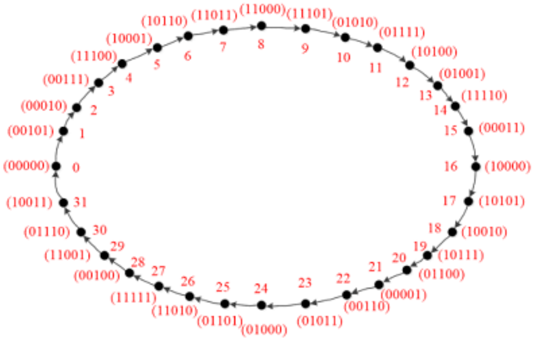

Figure 5 Cycle structure of f_{k_0}

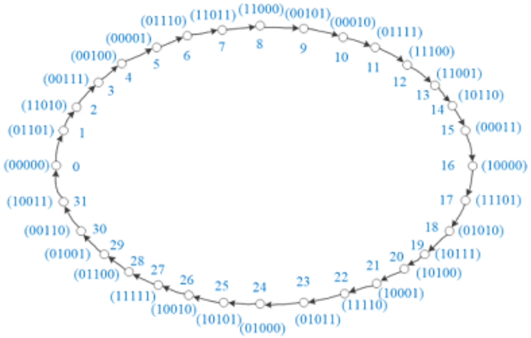

Figure 6 Cycle structure of f_{k_1}

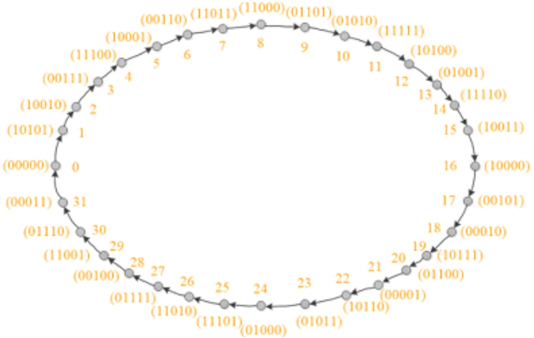

Figure 7 Cycle structure of f_{k_2}

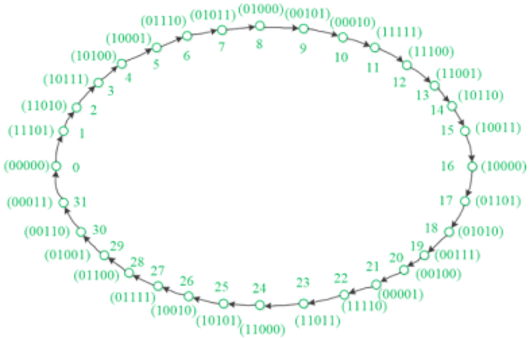

Figure 8 Cycle structure of f_{k_3}

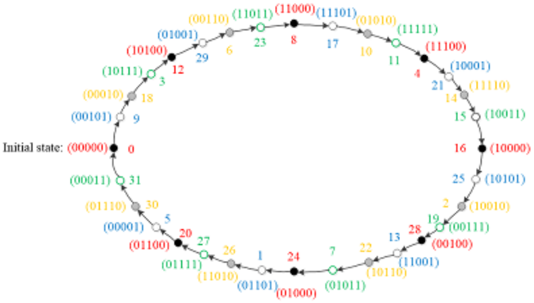

Figure 9 Output when initial state 0

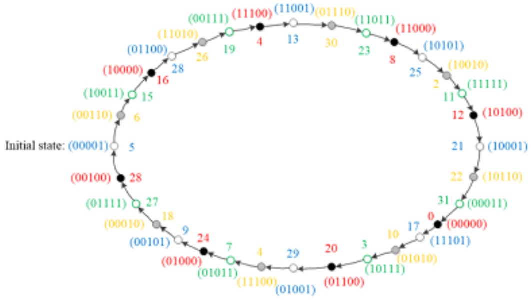

Figure 10 Output when initial state 1

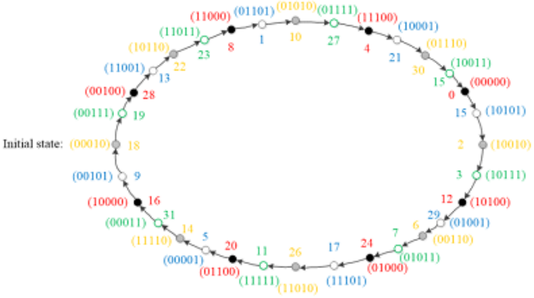

Figure 11 Output when initial state 2

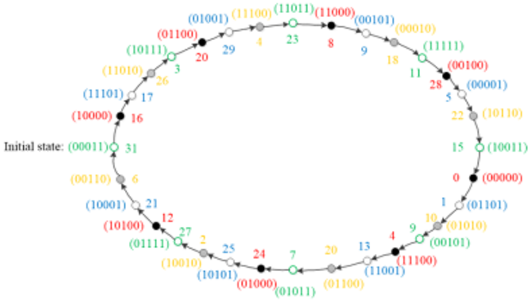

Figure 12 Output when initial state 3

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 9** , **Figure 10** , **Figure 11** and **Figure 12** above. Red figures with black solid circle are output from f_{k_0}, blue figures with hollow circle are output from f_{k_1}, yellow figures with grey solid circle are output from f_{k_2}, green figures with green hollow circle are output from f_{k_3}. And figures inside the cycles are 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 different.