JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **23**, No. 4, December 2010

ON SOME PROPERTIES OF A SINGLE CYCLE T-FUNCTION AND EXAMPLES

Min Surp Rhee*

Abstract. In this paper we study the structures and properties of a single cycle T-finction, whose theory has been lately proposed by Klimov and Shamir. Any cryptographic system based on T-functions may be insecure. Some of the TSC-series stream ciphers have been successfully attacked by some attacks. So it is important to analyze every aspect of a single cycle T-function. We study some properties on a single cycle T-function and we show some examples are single cycle T-functions by these properties, whose proof is easier than existing methods.

1. Introduction

Few years ago, Klimov and Shamir proposed the theory of T-functions [2-5]. T-functions are in the primitive level. A function from $(F_2)^m$ to $(F_2)^n$ is said to be a T-function(T means triangle function) if it does not propagate information from left to right, that is, each bit i of the outputs can depend only on bits $0, 1, \cdots, i$ of the inputs. It is easy to see that the boolean operations(XOR, AND, OR, NOT) and algebraic operations(addition, multiplication, substraction, negation) modulo 2^n, including left shift are all T-functions and their compositions are T-functions, too[2].

Since the use of T-functions in cryptography is so recent, not much is known about their cryptographic properties. Any cryptographic system based on T-functions may be insecure. Some of the TSC-series stream ciphers have been successfully attacked by some attacks[6]. So it is important to analyze every aspect of a single cycle T-function.

Received November 09, 2010; Accepted November 24, 2010.

2010 Mathematics Subject Classification: Primary 94A60.

Key words and phrases: T-function, n-bit words, a parameter function, a boolean function, period, a single cycle T-function, cryptographic scheme.

This research was supported by the Graduate Research Assistantship of Dankook University.

In this paper we study some properties on a single cycle T-function and we show some examples are single cycle T-functions, whose proof is easier than existing methods. The notations in this paper are standard. They are taken from [3]. Especially, $\bigoplus_{x=0}^{2^j-1} \alpha(x)$ denotes $\alpha(0) \oplus \alpha(1) \oplus \cdots \oplus \alpha(2^j - 1)$.

2. Preliminaries

In this section, we introduce some definitions which will be used later. Let F_2 be a finite field with two elements 0 and 1. Usually, the addition in F_2 is denoted by $\oplus$ and the multiplication in F_2 is denoted by $\cdot$. For any positive integer n a vector $x = (x_0, x_1, \cdots, x_{n-1})$ of $(F_2)^n$ is called **a word of length** n and x_j is called **the jth bit** of x. In particular, x_0 is called **the least significant bit** of x. Usually, the addition in $(F_2)^n$ is denoted by $\oplus$. Every word $x = (x_0, x_1, \cdots, x_{n-1})$ of $(F_2)^n$ can be written as an integer $x = \sum_{i=0}^{n-1} x_i 2^i$, which is an element of the residue class ring $\mathbb{Z}_{2^n}$ modulo 2^n. Usually, the addition and the multiplication in $\mathbb{Z}_{2^n}$ are denoted by $+$ and $\cdot$, respectively. Conversely, every integer x of $\mathbb{Z}_{2^n}$ can be written as a binary digit expression $x = [x]_{n-1}[x]_{n-2} \cdots [x]_1[x]_0$ (in other expression $x = \sum_{i=0}^{n-1} [x]_i 2^i$) and so every integer x of $\mathbb{Z}_{2^n}$ can be written as $x = ([x]_0, [x]_1, \cdots, [x]_{n-1})$ in $(F_2)^n$. In this point of view we may consider the set $(F_2)^n$ as the set $\mathbb{Z}_{2^n}$, and vice versa.

A function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is said to be **a single cycle function** if the sequence induced by its iteration $x, f(x), f^2(x) = f(f(x)), \cdots$ has a period of length 2^n, which is the maximal possible length. Every single cycle function is a bijective function since a function which is not surjective is not a single cycle T-function. A function from $(F_2)^n$ into F_2 is called **a boolean function**. For any function $f : (F_2)^n \to (F_2)^n$ defined by $f(x_0, x_1, \cdots, x_{n-1}) = (y_0, y_1, \cdots, y_{n-1})$ each y_i is a function of $x = (x_0, x_1, \cdots, x_{n-1})$ and so y_i is a boolean function for all $i = 0, 1, 2, \cdots, n-1$. A function $f : (F_2)^n \to (F_2)^n$ can be interpreted as n boolean functions.

A parameter is a function $g(x_1, \cdots, x_n; \alpha_1, \cdots, \alpha_m)$ whose arguments are split by a semicolon into inputs $x_1, x_2, \cdots, x_n$ and parameters $\alpha_1, \alpha_2, \cdots, \alpha_m$ which do not depend on their inputs. A function $f : (F_2)^n \to (F_2)^n$ defined by $f(x_0, x_1, \cdots, x_{n-1}) = (y_0, y_1, \cdots, y_{n-1})$ is said to be **a $\mathbf{T-}$function** if $y_0 = f_0(x_0)$ and each ith output y_i of $f(x)$ is a parameter $y_i = f_i(x_i; x_0, x_1, \cdots, x_{i-1})$ for all $i = 1, 2, \cdots, n-1$.

It is from [2] that a single cycle T-function f can be written either in the form $f(x) = x + r_1(x)$ or in the form $f(x) = x \oplus r_2(x)$, where $r_1(x)$ and $r_2(x)$ are parameter satisfying conditions as in [5].

Let $f : (F_2)^n \to (F_2)^n$ be a function, and define a function $f^i : (F_2)^n \to (F_2)^n$ by $f^0(x) = x$ and $f^i(x) = f(f^{i-1}(x))$ for every positive integer i. Let $x = ([x]_0, [x]_1, \cdots, [x]_{n-1})$ and $f(x) = ([f(x)]_0, [f(x)]_1, \cdots, [f(x)]_{n-1})$. When we use the notation $f^i(x) = ([f^i(x)]_0, [f^i(x)]_1, \cdots, [f^i(x)]_{n-1})$ for every positive integer i, we get

$$f^i(x) = f(f^{i-1}(x)) = f([f^{i-1}(x)]_0, [f^{i-1}(x)]_1, \cdots, [f^{i-1}(x)]_{n-1}).$$

Example 2.1. *Let $f(x) = x+(x^2 \vee 1)$ on $\mathbb{Z}_{2^n}$, and let $x = \sum_{i=0}^{n-1}[x]_i 2^i$. Then $x^2 = [x]_0 + ([x]_1^2 + [x]_0[x]_1)2^2 + \cdots$ and we have*

$$\begin{aligned}
&[f(x)]_0 = [x]_0 + [x]_0 \vee 1 \\
&[f(x)]_1 = [x]_1 \\
&[f(x)]_2 = [x]_2 + [x]_1 + [x]_0[x]_1 \\
&\qquad \vdots \\
&[f(x)]_i = [x]_i + \alpha_i, \ \ \alpha_i \text{ is a function of } [x]_0, \cdots, [x]_{i-1} \\
&\qquad \vdots
\end{aligned}$$

Hence $f(x)$ is a T-function. For any given word $f(x)$ we can find $[x]_0, [x]_1, \cdots, [x]_{n-1}$ in order. Therefore $f(x)$ is an invertible T-function.

A polynomial $f(x)$ over $\mathbb{Z}_{2^n}$ may be considered as a T-function. A polynomial over $\mathbb{Z}_{2^n}$ is a permutation polynomial if it is invertible on $\mathbb{Z}_{2^n}$. The following results are well known in [3].

Proposition 2.2. *Let $f(x) = a_0 + a_1x + \cdots + a_dx^d$ be a polynomial over $\mathbb{Z}_{2^n}$. Then $f(x)$ is a permutation polynomial over $\mathbb{Z}_{2^n}$ if and only if a_1 is odd, $a_2 + a_4 + \cdots$ is even and $a_3 + a_5 + \cdots$ is even.*

Proposition 2.3. *If $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is a single cycle T-function, then $\mathbb{Z}_{2^n} = \{f^i(x) | i \in \mathbb{Z}_{2^n}\}$ for each $x \in \mathbb{Z}_{2^n}$. In particular, $\mathbb{Z}_{2^n} = \{f^i(0) | i \in \mathbb{Z}_{2^n}\}$. Consequently, f is an invertible function on $\mathbb{Z}_{2^n}$.*

Proposition 2.4. *Let $f : (F_2)^n \to (F_2)^n$ be a function on $(F_2)^n$. Then f is invertible T-function if and only if for all $j < n$ the jth bit of the output can be represented as*

$$[f(x)]_j = f([x]_j; [x]_0, [x]_1, \cdots, [x]_{j-1}) = [x]_j \oplus \alpha([x]_0, [x]_1, \cdots, [x]_{j-1}).$$

3. Some propositions and examples

In this section we prove some properties and give examples related to them

Proposition 3.1. *A T-function $f : (F_2)^n \to (F_2)^n$ is a single cycle if and only if for all $j < n$ the jth bit of the output can be represented as*

$$[f(x)]_j = [x]_j \oplus \alpha([x]_0, [x]_1, \cdots, [x]_{j-1}) \text{ and } \bigoplus_{x=0}^{2^j-1} \alpha(x) = 1.$$

Proof. Suppose that a T-function $f : (F_2)^n \to (F_2)^n$ is a single cycle. Since f is a bijective T-function, by Proposition 2.4 the jth bit of the output can be represented as

$$[f(x)]_j = f([x]_j; [x]_0, [x]_1, \cdots, [x]_{j-1}) = [x]_j \oplus \alpha([x]_0, [x]_1, \cdots, [x]_{j-1})$$

for all $j < n$. Consider a sequence $(*)$ as follows:

$$([x]_0, \cdots, [x]_j),\ ([f(x)]_0, \cdots, [f(x)]_j),\ ([f^2(x)]_0, \cdots, [f^2(x)]_j), \cdots,$$
$$([f^{i-1}(x)]_0, \cdots, [f^{i-1}(x)]_j), ([f^i(x)]_0, \cdots, [f^i(x)]_j), \cdots \qquad (*)$$

Since $f(x)$ is a single cycle T-function this sequence $(*)$ has a period of length 2^{j+1}. If $j = 0$, then $[f(x)]_0 = [x]_0 \oplus 1$ and so $\bigoplus_{x=0} \alpha(x) = 1$. Consider the sequence $\{[f^i(x)]_k\} : [x]_k, [f(x)]_k, [f^2(x)]_k, \cdots, [f^i(x)]_k, \cdots$. Then we get

$$\begin{aligned}
[f(x)]_k &= [x]_k \oplus \alpha([x]_0, [x]_1, \cdots, [x]_{k-1}),\\
[f^2(x)]_k &= [f(x)]_k \oplus \alpha([f(x)]_0, [f(x)]_1, \cdots, [f(x)]_{k-1})\\
&= [x]_k \oplus \alpha([x]_0, [x]_1, \cdots, [x]_{k-1})\\
&\qquad \oplus \alpha([f(x)]_0, [f(x)]_1, \cdots, [f(x)]_{k-1}),\\
[f^i(x)]_k &= [x]_k \oplus \bigoplus_{l=0}^{i-1} \alpha([f^l(x)]_0, [f^l(x)]_1, \cdots, [f^l(x)]_{k-1}).
\end{aligned}$$

Note that $[f^{2^j}(x)]_m = [x]_m \oplus \bigoplus_{k=0}^{2^j-1} \alpha([f^k(x)]_0, [f^k(x)]_1, \cdots, [f^k(x)]_{m-1})$ $= [x]_m$ for each positive integer $m < j$. Hence for each positive integer $m < j$ we get

$$\bigoplus_{x=0}^{2^j-1} \alpha(x) = \bigoplus_{x=0}^{2^j-1} \alpha([f^k(x)]_0, [f^k(x)]_1, \cdots, [f^k(x)]_{m-1}) = 0.$$

Consider the (2^j+1)th term of sequence $(*)$ $([f^{2^j}(x)]_0, \cdots, [f^{2^j}(x)]_{j-1}$, $[f^{2^j}(x)]_j)$. By the above argument and the fact that the sequence $(*)$ has a period of length 2^{j+1} we get $([f^{2^j}(x)]_0, \cdots, [f^{2^j}(x)]_{j-1}, [f^{2^j}(x)]_j\ ) = ([x]_0, \cdots, [x]_{j-1}, [f^{2^j}(x)]_j)$ and $[f^{2^j}(x)]_j = [x]_j \oplus 1$. Since f is a single cycle function we get $\{([f^k(x)]_0, [f^k(x)]_1, \cdots, [f^k(x)]_{j-1}) \mid k = 0, 1, 2, \cdots, 2^j - 1\} = (F_2)^j$ and $\bigoplus_{x=0}^{2^j-1} \alpha(x) = \bigoplus_{x=0}^{2^j-1} \alpha([f^k(x)]_0, [f^k(x)]_1, \cdots, [f^k(x)]_{j-1}) = 1$.

Conversely, suppose that the jth bit of the output can be represented as $[f(x)]_j = [x]_j \oplus \alpha([x]_0, [x]_1, \cdots, [x]_{j-1})$ and $\bigoplus_{x=0}^{2^j-1} \alpha(x) = 1$ for all $j < n$. By first assumption f is a bijective T-function. We prove that f is a single cycle T-function by induction. If $j = 0$, then $[f(x)]_0 = [x]_0 \oplus 1$ and f has a sequence which has a period of length 2 modulo 2. Assume that it holds for $j-1$. Then f has a sequence which has a period of length 2^j modulo 2^j. That is, we get $\{([f^k(x)]_0, [f^k(x)]_1, \cdots, [f^k(x)]_{j-1}) | k = 0, 1, 2, \cdots, 2^j - 1\} = (F_2)^j$.

Consider $\{([f^k(x)]_0, [f^k(x)]_1, \cdots, [f^k(x)]_{j-1}) | k = 0, 1, 2, \cdots, 2^{j+1} - 1\}$. Suppose $([f^k(x)]_0, [f^k(x)]_1, \cdots, [f^k(x)]_{j-1}, [f^k(x)]_j) = ([f^l(x)]_0, [f^l(x)]_1, \cdots, [f^l(x)]_{j-1}, [f^l(x)]_j)$ for some distinct k and l in $\mathbb{Z}_{2^{j+1}}$. Then $[f^k(x)]_i = [f^l(x)]_i$ for all $i < j$ and $[f^k(x)]_j = [f^l(x)]_j$. By our assumption $k \equiv l \bmod 2^j$ and $[f^k(x)]_j = [f^l(x)]_j$. Hence $k = l + 2^j$ in $\mathbb{Z}_{2^{j+1}}$ and we get

$$\begin{aligned}[f^k(x)]_j = [f^{l+2^j}(x)]_j &= [f^l(x)]_j \oplus \bigoplus_{x=0}^{2^j-1} \alpha(f^l(x)) \\ &= [f^l(x)]_j \oplus \bigoplus_{x=0}^{2^j-1} \alpha(x) = [f^l(x)]_j \oplus 1 \\ &\neq [f^l(x)]_j\end{aligned}$$

which is a contradiction. So $\{([f^k(x)]_0, [f^k(x)]_1, \cdots, [f^k(x)]_{j-1}, [f^k(x)]_j) |k = 0, 1, 2, \cdots, 2^{j+1} - 1\} = (F_2)^{j+1}$ and f has a sequence which has a period of length 2^{j+1}. Thus f is a single cycle T-function. □

From Proposition 3.1 we get the following proposition.

Proposition 3.2. *Let $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ be a polynomial. Then f is a single cycle if and only if for all $j < n$ the jth bit of the output can be represented as $[f(x)]_j = [x]_j \oplus [g(y)]_j$ and $\sum_{x=0}^{2^j-1} g(x) \equiv 2^j \bmod 2^{j+1}$, where $g(x) = f(x) - x$ is a parameter, $x = 2^j[x]_j + \cdots + 2[x]_1 + [x]_0$ and $y = 2^{j-1}[x]_{j-1} + \cdots + 2[x]_1 + [x]_0$.*

Proof. Let $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ be a polynomial defined by $f(x) = \sum_{i=0}^m a_i x^i$. Then f is a T-function. Suppose that a T-function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is a single cycle. When we consider $\mathbb{Z}_{2^n}$ as $(F_2)^n$ a T-function $f : (F_2)^n \to (F_2)^n$ is a single cycle. Then by Proposition 3.1 for all $j < n$ the jth bit of the output can be represented as

$$[f(x)]_j = [x]_j \oplus \alpha([x]_0, [x]_1, \cdots, [x]_{j-1}) \text{ and } \bigoplus_{x=0}^{2^j-1} \alpha(x) = 1.$$

Note $[f(x)]_j = \left[\sum_{i=0}^m a_i x^i\right]_j = \bigoplus_{i=0}^m [a_i x^i]_j = [x]_j \oplus \bigoplus_{i=0}^m [a_i x^i]_j \oplus [x]_j$. Since $\alpha([x]_0, [x]_1, \cdots, [x]_{j-1})$ is a paremeter, $\bigoplus_{i=0}^m [a_i x^i]_j \oplus [x]_j$ is a parameter and $a_1 + 1$ is even. Let $g(x) = f(x) - x$. Then $[g(x)]_j = \alpha([x]_0, [x]_1, \cdots, [x]_{j-1})$. Note $[g(x)]_j = [g([x]_0+2[x]_1+\cdots+2^{j-1}[x]_{j-1})]_j = [g(y)]_j$, where $y = 2^{j-1}[x]_{j-1} + \cdots + 2[x]_1 + [x]_0$. Hence $\alpha(y) = \alpha([x]_0, [x]_1, \cdots, [x]_{j-1}) = [g(y)]_j$ and $1 = \bigoplus_{x=0}^{2^j-1} \alpha(y) = \left[\sum_{x=0}^{2^j-1} g(y)\right]_j$. Since $\left[\bigoplus_{x=0}^{2^j-1} g(y)\right]_j = 0$ for all $i < j$, $\bigoplus_{x=0}^{2^j-1} g(y) = (0, 0, \cdots, 0, 1)$ and $\sum_{x=0}^{2^j-1} g(y) \equiv 2^j \bmod 2^{j+1}$.

Conversely, suppose that for all $i < j$ the jth bit of the output can be represented as $[f(x)]_j = [x]_j \oplus [g(y)]_j$ and $\sum_{x=0}^{2^j-1} g(x) \equiv 2^j \bmod 2^{j+1}$, where $g(x) = f(x) - x$ is a parameter, $x = 2^j[x]_j + \cdots + 2[x]_1 + [x]_0$ and $y = 2^{j-1}[x]_{j-1} + \cdots + 2[x]_1 + [x]_0$. Since $g(x)$ is a parameter, we get

$$[g(y)]_j = [g(2^{j-1}[x]_{j-1} + \cdots + 2[x]_1 + [x]_0)]_j = \alpha([x]_0, [x]_1, \cdots, [x]_{j-1}),$$
$$[f(x)]_j = [x]_j \oplus [g(y)]_j = [x]_j \oplus \alpha([x]_0, [x]_1, \cdots, [x]_{j-1}).$$

Also, we have $\bigoplus_{x=0}^{2^j-1} \alpha(x) = \bigoplus_{x=0}^{2^j-1} [g(x)]_j = \left[\bigoplus_{x=0}^{2^j-1} g(x)\right] = \left[\sum_{x=0}^{2^j-1} g(x)\right]_j = 1$ since $\sum_{x=0}^{2^j-1} g(y) = 2^j \bmod 2^{j+1}$. Therefore, f is a single cycle. □

By Proposition 3.2 we can characterize a single cycle polynomial of degree not greater than 2 in next two examples. The proof is much easier than the one as in [7].

Example 3.3. *Let $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ be a function defined by $f(x) = ax + b$. Then f is a single cycle T-function if and only if for all $j < n$ the jth bit of the output can be represented as $[f(x)]_j = [x]_j \oplus [g(y)]_j$ and $\sum_{x=0}^{2^j-1} g(x) \equiv 2^j \bmod 2^{j+1}$, where $g(x) = f(x) - x$ is a parameter and $y = 2^{j-1}[x]_{j-1} + \cdots + 2[x]_1 + [x]_0$. Since $g(0) \equiv 1 \bmod 2$, $b \equiv 1 \bmod 2$. Hence note that $\sum_{x=0}^{2^j-1} g(x) \equiv 2^j \bmod 2^{j+1}$ if and only if $\sum_{x=0}^{2^j-1} (a-1)x + b = \frac{(a-1)(2^j-1)(2^j)}{2} + b2^j \equiv 2^j \bmod 2^{j+1}$ if and only if $\frac{(a-1)(2^j-1)(2^j)}{2} \equiv 0 \bmod 2^{j+1}$ if and only if $a \equiv 1 \bmod 4$. Therefore*

$f(x) = ax+b$ is a single cycle T-function if and only if $a \equiv 1$ mod 4 and $b \equiv 1$ mod 2.

EXAMPLE 3.4. *Let $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ be a function defined by $f(x) = ax^2+bx+c$. Then f is a single cycle T-function if and only if for all $j < n$ the jth bit of the output can be represented as $[f(x)]_j = [x]_j \oplus [g(y)]_j$ and $\sum_{x=0}^{2^j-1} g(x) \equiv 2^j$ mod 2^{j+1}, where $g(x) = f(x) - x$ is a parameter and $y = 2^{j-1}[x]_{j-1} + \cdots + 2[x]_1 + [x]_0$. Since $g(0) \equiv 1$ mod 2, $c \equiv 1$ mod 2. Also, b is odd since $g(x)$ is a parameter. Note that $\sum_{x=0}^{2^j-1} g(x) \equiv 2^j$ mod 2^{j+1} if and only if $\sum_{x=0}^{2^j-1}\{ax^2+(b-1)x+c\} \equiv 2^j$ mod 2^{j+1}. Hence we get $\frac{a(2^j-1)(2^j)(2^{j+1}-1)}{6} + \frac{(b-1)(2^j-1)(2^j)}{2} + c2^j \equiv 2^j$ mod 2^{j+1}. Since $a(2^{j+1}-1) + 3(b-1) = 2a(2^j+1) + 3(-a+b-1)$, we get*

$$\begin{aligned}
&\frac{(2^j-1)(2^j)\{a(2^{j+1}-1)+3(b-1)\}}{6} \\
&\equiv \frac{a(2^j-1)(2^j)(2^j+1)}{3} + \frac{(-a+b-1)(2^j-1)2^j}{2} \\
&\equiv \frac{(-a+b-1)(2^j-1)2^j}{2} \quad mod\ 2^{j+1}
\end{aligned}$$

and so $-a+b-1 \equiv 0$ mod 4. Since b is odd, we get $a \equiv 0$ mod 4, $b \equiv 1$ mod 4 or $a \equiv 2$ mod 4, $b \equiv 3$ mod 4. Therefore, f is a single cycle T-function if and only if one of the following is satisfied:

(i) $a \equiv 0$ mod 4, $b \equiv 1$ mod 4 and $c \equiv 1$ mod 2,

(ii) $a \equiv 2$ mod 4, $b \equiv 3$ mod 4 and $c \equiv 1$ mod 2.

In this paper we have proved Proposition 3.1 using by different technic and Proposition 3.2 by using Proposition 3.1. Also, we have characterize a single cycle polynomial of degree d not greater than 2 by using Proposition 3.2. This characterization process is from easy calculation, which is much easier than the one as in [7]. Actually, we can characterize a single cycle polynomial of degree by using Proposition 2.2 and Proposition 3.2. Our future study is to apply this proposition to characterize some conditions so that a general T-function is a single cycle function.

References

[1] Jin Hong, Dong Hoon Lee, Yongjin Yeom and Daewan Han, *A New Class of Single Cycle T-functions*, FSE 2005, LNCS **3557** (2005), 68-82.

[2] A Kilmov, *Applications of T-functions in Cryptography*, Ph.D.Thesis Weizmann Institute Science, 2005.

[3] A Kilmov and A. Shamir, *A New Class of Invertible Mappings*, CHES 2002, LNCS **2523** (2003), 470-483.

[4] A Kilmov and A. Shamir, *Cryptographic Applications of T-Functions*, SAC 2003, LNCS **3006** (2004), 248-261.

[5] A Kilmov and A. Shamir, *New Cryptographic Primitives Based on Multiword T-Functions*, FSE 2004, LNCS **3017** (2004), 1-15.

[6] F. Muller and T Peyrin, *Linear Cryptanalysis of TSC Stream Ciphers Applications to the ECRYPT proposal TSC-3*, Asiacrypt 2005, LNCS **3329** (2005), 468-482.

[7] M Rhee, *On a characterization of T-functions with one cycle property*, J. of the Chungcheong Math Soc. **21** (2008), no. 2.

*
Department of Mathematics
Dankook University
Cheonan 330-714, Republic of Korea
E-mail: msrhee@dankook.ac.kr