JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **24**, No. 4, December 2011

ON A T-FUNCTION $f(x) = x + h(x)$ WITH A SINGLE CYCLE ON $\mathbb{Z}_{2^n}$

Min Surp Rhee*

Abstract. Invertible transformations over n-bit words are essential ingredients in many cryptographic constructions. When n is large (e.g., $n = 64$) such invertible transformations are usually represented as a composition of simpler operations such as linear functions, S-P networks, Feistel structures and T-functions. Among them we study T-functions which are probably invertible and are very useful in stream ciphers. In this paper we study some conditions on a T-function $h(x)$ such that $f(x) = x + h(x)$ has a single cycle on $\mathbb{Z}_{2^n}$.

1. Introduction

Let $\mathbb{B}^n = \{(x_{n-1}, x_{n-2}, \cdots, x_0) | x_i \in \mathbb{B}\}$ be the set of all n-tuples of elements in $\mathbb{B}$, where $\mathbb{B} = \{0, 1\}$. Then an element of $\mathbb{B}$ is called a bit and an element of $\mathbb{B}^n$ is called an n-bit word. An element x of $\mathbb{B}^n$ can be represented as $([x]_{n-1}, [x]_{n-2}, \cdots, [x]_0)$, where $[x]_{i-1}$ is the i-th component from the right end of x. In particular, the first component $[x]_0$ of x is called the least bit of x. It is often useful to express an element $([x]_{n-1}, [x]_{n-2}, \cdots, [x]_0)$ of $\mathbb{B}^n$ as an element $\sum_{i=0}^{n-1} [x]_i 2^i$ of $\mathbb{Z}_{2^n}$ and $\sum_{i=0}^{n-1} [x]_i 2^i$ of $\mathbb{Z}_{2^n}$ as $([x]_{n-1}, [x]_{n-2}, \cdots, [x]_0)$ of $\mathbb{B}^n$. In this expression every element of $\mathbb{B}^n$ is considered as an element of $\mathbb{Z}_{2^n}$ and vice versa, where $\mathbb{Z}_{2^n}$ is the congruence ring modulo 2^n. Consequently $\mathbb{B}^n$ is considered as $\mathbb{Z}_{2^n}$ and vice versa. For example, an element $(0, 1, 1, 0, 1, 0, 1, 1)$ of $\mathbb{B}^8$ is considered as an element 107 of $\mathbb{Z}_{2^8} = \mathbb{Z}_{256}$ and 75 of $\mathbb{Z}_{2^8}$ is considered as $(0, 1, 0, 0, 1, 0, 1, 1)$ of $\mathbb{B}^8$.

Received October 25, 2011; Accepted November 18, 2011.
2010 Mathematics Subject Classification: Primary 94A60.
Key words and phrases: a T-function, an n-bit word, period, a single cycle.
The present research was conducted by the research fund of Dankook University in 2010.

DEFINITION 1.1. For any n-bit words $x = (x_{n-1}, x_{n-2}, \cdots, x_0)$ and $y = (y_{n-1}, y_{n-2}, \cdots, y_0)$ of $\mathbb{B}^n$, we define the following:

(1) $x \pm y$ and xy are defined as $x \pm y \mod 2^n$ and $xy \mod 2^n$, respectively.

(2) $x \oplus y$ is defined as $(z_{n-1}, z_{n-2}, \cdots, z_0)$, where $z_i = 0$ if $x_i = y_i$ and $z_i = 1$ if $x_i \neq y_i$ for each i.

(3) $x \vee y$ is defined as $(z_{n-1}, z_{n-2}, \cdots, z_0)$, where $z_i = 0$ if $x_i = y_i = 0$ and $z_i = 1$ otherwise for each i.

A function $f : \mathbb{B}^n \to \mathbb{B}^n$ is said to be a T-function(short for a triangular function) if for each $k \in \{0, 1, 2, \cdots, n-1\}$ the k-th bit of an n-bit word $f(x)$ depends only on the first k bits of an n-bit word x. In particular, a function $f : \mathbb{B}^n \to \mathbb{B}^n$ is said to be a parameter if for each $k \in \{1, 2, \cdots, n-1\}$ the k-th bit of an n-bit word $f(x)$ depends only on the first $k-1$ bits of an n-bit word x.

EXAMPLE 1.2. *Let* $f(x) = x + (x^2 \vee 1)$ *on* $\mathbb{Z}_{2^n}$. *If* $x = \sum_{i=0}^{n-1} [x]_i 2^i$, *then* $x^2 = [x]_0 + ([x]_1^2 + [x]_0[x]_1)2^2 + \cdots$, *and since* $[x]_i^2 = [x]_i$ *we have*

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

Hence $f(x)$ *is a T-function. But* $f(x)$ *is not a parameter. Also, for any given word* $f(x) = ([f(x)]_{n-1}, \cdots, [f(x)]_1, [f(x)]_0)$ *we can find* $[x]_0, [x]_1, \cdots, [x]_{n-1}$ *in order. Hence* $f(x)$ *is an invertible T-function.*

Let $a_0, a_1, \cdots, a_m, \cdots$ be a sequence of numbers(or words) in $\mathbb{Z}_{2^n}$. If there is the least positive integer l such that $a_{i+l} = a_i$ for each nonnegative integer i, then the sequence $a_0, a_1, \cdots, a_m, \cdots$ is said to have a cycle of period l. In this case we say that $a_0, a_1, \cdots, a_{l-1}$ is called a cycle of period l. In general $a_i, a_{i+1}, \cdots, a_{i+l-1}$ is a cycle of period l for every nonnegative integer i.

Now, for any function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$, let's define $f^i : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ by

$$f^i(x) = \begin{cases} x & \text{if } i = 0 \\ f(f^{i-1}(x)) & \text{if } i \geq 1 \end{cases}$$

It is easy to show that $f^i(x)$ is a T-function for every positive integer i if $f(x)$ is a T-function. Hence, if $f(x)$ is a bijective T-function then so does $f^i(x)$ for every positive integer i.

Now, let $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ be a bijective T-function. An element(or word) α of $\mathbb{Z}_{2^n}$ is said to have a cycle of period l in f if l is the least positive integer such that $f^l(\alpha) = \alpha$. If α has a cycle of period l and $\alpha_i = f^i(\alpha)$, then α generates a sequence which has a cycle $\alpha = \alpha_0, \alpha_1, \cdots, \alpha_{l-1}$ of period l. Also, in this case every word α_i for any nonnegative integer i has a cycle of period l. In particular, a word which has a cycle of period 1 is called a fixed word. That is, an element α of $\mathbb{Z}_{2^n}$ is a fixed word if $f(\alpha) = \alpha$. Also, f is said to have a single cycle if there is a word which has a cycle of period 2^n. In this case every word of $\mathbb{Z}_{2^n}$ has a cycle of period 2^n.

EXAMPLE 1.3. *Let* $f(x) = x + (x^2 \vee 1)$ *be a function on* $\mathbb{Z}_{2^3}$. *Then* $f(0) = 1, f(1) = 2, f(2) = 7, f(3) = 4, f(4) = 5, f(5) = 6, f(6) = 3$ *and* $f(7) = 0$. *Hence* 0 *has a cycle* $0, 1, 2, 7$ *of period* 4 *and* 3 *has a cycle* $3, 4, 5, 6$ *of period* 4.

EXAMPLE 1.4. *Let* $f(x) = x + (x^2 \vee 5)$ *be a function on* $\mathbb{Z}_{2^3}$. *Then* $f(0) = 5, f(1) = 6, f(2) = 7, f(3) = 0, f(4) = 1, f(5) = 2, f(6) = 3$ *and* $f(7) = 4$. *Hence* 0 *has a cycle* $0, 5, 2, 7, 4, 1, 6, 3$ *of period* 8. *Hence* f *has a single cycle.*

EXAMPLE 1.5. *Let* $f(x) = x + (2x + 1)^2$ *be a function on* $\mathbb{Z}_{2^3}$. *Then* $f(0) = 1, f(1) = 2, f(2) = 3, f(3) = 4, f(4) = 5, f(5) = 6, f(6) = 7$ *and* $f(7) = 0$. *Hence* 0 *has a cycle* $0, 1, 2, 3, 4, 5, 6, 7$ *of period* 8. *Hence* f *has a single cycle.*

From above three examples we show that $f(x) = x + (x^2 \vee 5)$ and $f(x) = x + (2x + 1)^2$ have a single cycle. In [8], the author showed that the function $f(x) = x + (g(x)^2 \vee C)$ on $\mathbb{Z}_{2^n}$ has a single cycle if $g(x)$ is a bijective T-function and C is a constant satisfying $[C]_0 = [C]_2 = 1$.

If a word a of $\mathbb{Z}_{2^n}$ has a cycle of period l, then the l words $a_0 = f^0(a) = a, a_1 = f(a), \cdots, a_i = f^i(a), \cdots, a_{l-1} = f^{l-1}(a)$ are repeated in the sequence $a_0, a_1, \cdots, a_m, \cdots$. Since a word of $\mathbb{Z}_{2^n}$ can be expressed as n bits, we may consider that a word a of $\mathbb{Z}_{2^n}$ which has a cycle of period l in f generates a binary sequence of period $n \cdot l$. Hence a T-function f with a single cycle generates a binary sequence of period $n \cdot 2^n$, which is the longest period in f. Binary sequences of large period enough are important in a stream cipher. In this paper we study some conditions on $h(x)$ such that $f(x) = x + h(x)$ has a single cycle on $\mathbb{Z}_{2^n}$, where $h(x)$ is a T-function on $\mathbb{Z}_{2^n}$.

2. Even parameters and T-functions with a single cycle

Let $r : \mathbb{B}^n \to \mathbb{B}^n$ be a parameter. Then from the definition of a parameter the $(n-1)$th bit of output $r(x)$ is independent of the $(n-1)$th bit of input x. Hence $r(x) \equiv r(x + 2^{n-1}) \bmod 2^n$ for every word x of $\mathbb{B}^n$. Thus, we can express it as $r(x) \equiv r(x + 2^{n-1}) + 2^n b(x) \bmod 2^{n+1}$ for some function $b : \mathbb{B}^n \to \mathbb{B}$. That is, $b(x) \equiv 2^{-n}\{r(x + 2^{n-1}) - r(x)\}$ mod 2. Let $\mathbb{B}[r(x), n]$ be a function defined by

$$\mathbb{B}[r(x), n] \equiv 2^{-n} \sum_{x=0}^{2^{n-1}-1} \{r(x + 2^{n-1}) - r(x)\} \equiv \bigoplus_{x=0}^{2^{n-1}-1} b(x) \bmod 2.$$

Then we have the following definition:

Definition 2.1. A parameter $r(x)$ on $\mathbb{Z}_{2^n}$ is said to be even (resp., odd) if $\mathbb{B}[r(x), n]$ is 0 (resp., 1).

Example 2.2. *Let* $r(x) = 2x$ *on* $\mathbb{Z}_{2^n}$. *Since* $r(x + 2^{n-1}) \equiv r(x) + 2^n \cdot 1$ *mod* 2^{n+1}, *we get* $b(x) \equiv 2^{-n}\{2(x + 2^{n-1}) - 2x\} \equiv 1$ *mod* 2 *and* $\mathbb{B}[r(x), n] \equiv 0$ *mod* 2 *for all* $n \geq 2$. *So* $r(x)$ *is an even parameter.*

By a similar method as above, $r(x) = x^2$ and $r(x) = C$ are even parameters for all $n \geq 3$ and for all $n \geq 1$ on $\mathbb{Z}_{2^n}$, respectively, where C is the constant function. From the definition of an even parameter we get the following proposition.

Proposition 2.3. *Let* $r_1(x)$ *and* $r_2(x)$ *be even parameters on* $\mathbb{Z}_{2^n}$ *for all* $n \geq k_1$ *and* $n \geq k_2$, *respectively. Then* $r_1(x) + r_2(x)$ *is an even parameter for all* $n \geq k$, *where* $k = \max\{k_1, k_2\}$.

Example 2.4. *Let* $r_i(x) = x^{2i}$ *on* $\mathbb{Z}_{2^n}$, *where* i *is a nonnegative integer. Note that* $r_i(x + 2^{n-1}) \equiv (x + 2^{n-1})^{2i} \equiv r(x) + 2i \cdot x \cdot 2^{n-1}$ *mod* 2^{n+1} *for all* $n \geq 3$ *and* $b(x) = [i]_0 \cdot [x]_0$. *Hence* $r_i(x)$ *is an even parameter for all* $n \geq 3$. *By Proposition 2.3* $r(x) = \sum_{i=0}^{m} a_i r_i(x)$ *is an even parameter for all* $n \geq 3$. *That is, if* $g(x)$ *is a polynomial on* $\mathbb{Z}_{2^n}$, *then* $g(x^2)$ *is an even parameter for all* $n \geq 3$.

Let $g(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$ be a polynomial on $\mathbb{Z}_{p^n}$, where p is a prime, $n \geq 1$ and $m \geq 1$. Then the polynomial

$$m a_m x^{m-1} + (m-1) a_{m-1} x^{m-2} + \cdots + 2a_2 x + a_1$$

is called the formal derivative of $g(x)$ and is denoted by $g'(x)$.

For example, if $g(x) \equiv x^4 + 3x^2 + x + 3 \bmod 2^2$, then $g'(x) \equiv 2x + 1 \bmod 2^2$. Now, we show that $g(x)^2$ is an even parameter if $g(x)$ is a polynomial.

THEOREM 2.5. *Let $g(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ be a polynomial on $\mathbb{Z}_{2^n}$. Then $g(x)^2$ is an even parameter for all $n \geq 3$.*

Proof. Note

$$\begin{aligned} g(x + 2^{n-1}) &\equiv a_m(x + 2^{n-1})^m + a_{m-1}(x + 2^{n-1})^{m-1} + \\ &\quad \cdots + a_2(x + 2^{n-1})^2 + a_1(x + 2^{n-1}) + a_0 \mod 2^{n+1} \\ &\equiv a_m[x^m + m \cdot x^{m-1} \cdot 2^{n-1}] \\ &\quad + a_{m-1}[x^{m-1} + (m-1) \cdot x^{m-2} \cdot 2^{n-1}] \\ &\quad + \cdots + a_2[x^2 + 2 \cdot x \cdot 2^{n-1}] \\ &\quad + a_1[x + 2^{n-1}] + a_0 \bmod 2^{n+1} \\ &\equiv g(x) + g'(x) \cdot 2^{n-1} \bmod 2^{n+1}. \end{aligned}$$

for every integer $n \geq 3$. Hence

$$\begin{aligned} g(x + 2^{n-1})^2 - g(x)^2 &\equiv \{g(x) + g'(x)2^{n-1}\}^2 - g(x)^2 \bmod 2^{n+1} \\ &\equiv g(x)g'(x) \cdot 2^n \bmod 2^{n+1}. \end{aligned}$$

for every integer $n \geq 3$. Since the degree of $g(x)g'(x) \leq 2m - 1$, we may let $g(x)g'(x) = b_{2m-1}x^{2m-1} + \cdots + b_2x^2 + b_1x + b_0$. Then

$$\begin{aligned} \mathbb{B}[g(x)^2, n] &\equiv 2^{-n} \sum_{x=0}^{2^{n-1}-1} \{g(x + 2^{n-1})^2 - g(x)^2\} \bmod 2 \\ &\equiv \sum_{x=0}^{2^{n-1}-1} g(x)g'(x) \bmod 2 \\ &\equiv \sum_{x=0}^{2^{n-1}-1} \{b_{2m-1}x^{2m-1} + \cdots + b_2x^2 + b_1x + b_0\} \bmod 2 \\ &\equiv \sum_{x=0}^{2^{n-1}-1} [b_{2m-1} + \cdots + b_2 + b_1]_0[x]_0 + [b_0] \bmod 2 \\ &\equiv \sum_{x=0}^{2^{n-1}-1} \{\alpha[x]_0 + [b_0]_0\} \bmod 2 \\ &\equiv 0 \bmod 2, \end{aligned}$$

for every integer $n \geq 3$, where $\alpha = [b_{2m-1} + \cdots + b_2 + b_1]_0$ is a multiplication parameter. Therefore, $g(x)^2$ is an even parameter for every integer $n \geq 3$. $\square$

Proposition 2.6. *Let $f(x) = ax + b$ be a polynomial on $\mathbb{Z}_{2^n}$. Then $g(x)$ has a single cycle on $\mathbb{Z}_{2^n}$ if and only if $a \equiv 1$ mod 4 and $b \equiv 1$ mod 2.*

Proof. The proof follows from [7]. □

If $f(x)$ has a single cycle on $\mathbb{Z}_{2^n}$, then by definition of a single cycle it has a single cycle on $\mathbb{Z}_{2^k}$ for every $k \leq n$. So we have following two propositions.

Proposition 2.7. *Let $f(x) = x + g(x)^2$ be a T-function on $\mathbb{Z}_{2^n}$, where $g(x) = 2q(x) + 1$ for some T-function $q(x)$ on $\mathbb{Z}_{2^n}$. Then $f(x)$ has a single cycle for all $n \leq 3$.*

Proof. Since $g(x) \equiv 1 \bmod 2$ for every element x of $\mathbb{Z}_{2^n}$ we get $g(x)^2 = 1$ for every element x of $\mathbb{Z}_{2^3}$. Hence $f(x) = x + 1$ for every element x of $\mathbb{Z}_{2^3}$. So by Proposition 2.6 $f(x)$ has a single cycle on $\mathbb{Z}_{2^3}$. Therefore $f(x)$ has a single cycle on $\mathbb{Z}_{2^n}$ for all $n \leq 3$. □

Proposition 2.8. *Let $f(x) = x + (g(x)^2 \vee C)$ be a T-function on $\mathbb{Z}_{2^n}$, where $g(x)$ is a function on $\mathbb{Z}_{2^n}$ and C is a constant such that $[C]_0 = [C]_2 = 1$. Then $f(x)$ has a single cycle for all $n \leq 3$.*

Proof. If C is a constant such that $[C]_0 = [C]_2 = 1$, then $C \equiv 5 \bmod 8$ or $C \equiv 7 \bmod 8$. Note that $g(x)^2 = 0, g(x)^2 = 1$ or $g(x)^2 = 4$ for every element x of $\mathbb{Z}_{2^3}$. Hence $g(x)^2 \vee C = C$ for every element x of $\mathbb{Z}_{2^3}$. So by Proposition 2.6 $f(x) = x + C$ has a single cycle on $\mathbb{Z}_{2^3}$. Therefore $f(x)$ has a single cycle on $\mathbb{Z}_{2^n}$ for all $n \leq 3$. □

Proposition 2.9. *Let $r(x)$ be a parameter and $f(x)$ be a function defined by $f(x) = x + r(x)$. Let N_e be a positive integer such that $f(x)$ has a single cycle modulo 2^{N_e}. Then $f(x)$ has a single cycle modulo 2^n for all n if and only if $r(x)$ is an even parameter for all $n \geq N_e$.*

Proof. The proof may be found in [6]. □

Theorem 2.10. *Let $f(x) = x + h(x)$ be a function on $\mathbb{Z}_{2^n}$. Suppose that $h(x)$ satisfies one of following forms:*

(1) $\{2g(x) + 1\}^2$ for every T-function $g(x)$ on $\mathbb{Z}_{2^n}$.

(2) $g(x)^2 \vee C$ for every bijective T-function $g(x)$ on $\mathbb{Z}_{2^n}$ and C is a constant such that $[C]_0 = [C]_2 = 1$.

(3) $g(x)^2 \vee C$ for every polynomial $g(x)$ on $\mathbb{Z}_{2^n}$ and C is a constant such that $[C]_0 = [C]_2 = 1$.

Then $f(x)$ has a single cycle on $\mathbb{Z}_{2^n}$ for all n.

Proof. Suppose that (1) holds. Then it follows from Proposition 2.7 that $f(x)$ has a single cycle for all $n \leq 3$. Also, by Theorem 2.5 $g(x)^2$ is an even parameter for all $n \geq 3$. Hence by Proposition 2.9 $f(x)$ has a single cycle on $\mathbb{Z}_{2^n}$ for all n.

Suppose that (2) holds. Then the proof follows from [8].

Finally, suppose that (3) holds. Then it follows from Proposition 2.8 that $f(x)$ has a single cycle for all $n \leq 3$. Also, by Theorem 2.5 $g(x)^2$ is an even parameter for all $n \geq 3$ and so $g(x)^2 \vee C$ is an even parameter for all $n \geq 3$. Hence by Proposition 2.9 $f(x)$ has a single cycle on $\mathbb{Z}_{2^n}$ for all n. □

Corollary 2.11. *The function $f(x) = x + (x^2 \vee C)$ has a single cycle on $\mathbb{Z}_{2^n}$ for all n if and only if C is a constant such that $[C]_0 = [C]_2 = 1$.*

Proof. If C is a constant such that $[C]_0 = [C]_2 = 1$, it is a special case of $g(x) = x$ in Theorem 2.10. Conversely, suppose that C is a constant such that $[C]_0 = 0$ or $[C]_2 = 0$. Consider $f(x) = x + (x^2 \vee C)$ on $\mathbb{Z}_{2^3}$ such that $[C]_0 = 0$ or $[C]_2 = 0$. If $[C]_0 = 0$, then $f(x)$ is not bijective since $f(x) \equiv 0 \bmod 2$ for every x of $\mathbb{Z}_{2^3}$. Hence $f(x)$ has no single cycle on $\mathbb{Z}_{2^3}$. If $[C]_2 = 0$, there are only two cases on $\mathbb{Z}_{2^3}$: $C = 1$ and $C = 3$. By simple calculation we can show that $f(x)$ has no single cycle on $\mathbb{Z}_{2^3}$. Thus $f(x)$ has no single cycle on $\mathbb{Z}_{2^n}$. Therefore, Corollary 2.11 holds. □

Example 2.12. *Let $g(x) = x + (2x^2 + 1)^2$ and $h(x) = x + ((x^2 + x + 1)^2 \vee 5)$ be polynomials of degree 2. Then by Theorem 2.10 $g(x)$ and $h(x)$ have a single cycle modulo $\mathbb{Z}_{2^3}$. Since $(2x^2+1)^2$ and $(x^2+x+1)^2 \vee 1$ are even parameters all $n \geq 3$, $g(x)$ and $h(x)$ have a single cycle modulo 2^n for all n.*

References

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

[2] A Kilmov, *Applications of T-functions in Cryptography*,2005.

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

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

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

[6] A Kilmov and A. Shamir, *New Applications of T-function in Block Cipher and Hash Functions* , FSE 2005.

[7] M. S. Rhee, *On a characterization of T-functions with one cycle property*, J. of the Chungcheong Math Soc. **21** (2008), no. 2, 259-268.
[8] M. S. Rhee, *On secure binary sequences generated by a function* $f(x) = x + (g(x)^2 \vee C)$ *mod* 2^n , J. of the Chungcheong Math Soc. **22** (2009), no. 4, 777-789.

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