JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **29**, No. 4, November 2016
http://dx.doi.org/10.14403/jcms.2016.29.4.573

ON A CHARACTERIZATION OF SECURE TRINOMIALS ON $\mathbb{Z}_{2^n}$

Min Surp Rhee*

Abstract. Invertible transformations over n-bit words are essential ingredients in many cryptographic constructions. 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 T-functions are probably invertible transformations and are very useful in stream ciphers. In this paper we will characterize a secure trinomial on $\mathbb{Z}_{2^n}$ which generates an n-bit word sequence without consecutive elements of period 2^n.

1. Introduction

Let n be a positive integer and $B^n = \{(x_{n-1}, x_{n-2}, \cdots, x_0) | x_i \in B\}$ be the set of all n-tuples of elements in $B = \{0, 1\}$. Then an element of B is called a **bit** and an element of B^n is called an **n-bit word**. An element x of 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. It is often useful to express an element $([x]_{n-1}, [x]_{n-2}, \cdots, [x]_0)$ of B^n as an element $\sum_{i=0}^{n-1} [x]_i 2^i$ of $\mathbb{Z}_{2^n}$ and $\sum_{i=0}^{n-1} a_i 2^i$ of $\mathbb{Z}_{2^n}$ as $(a_{n-1}, a_{n-2}, \cdots, a_0)$ of B^n, where $\mathbb{Z}_{2^n}$ is the congruence ring modulo 2^n. In this expression every element of B^n is considered as an element of $\mathbb{Z}_{2^n}$ and vice versa. Consequently B^n is considered as $\mathbb{Z}_{2^n}$ and vice versa. For example, an element $(0, 1, 1, 0, 0, 0, 1, 1)$ of B^8 is considered as an element 99 of $\mathbb{Z}_{2^8} = \mathbb{Z}_{256}$ and 71 of $\mathbb{Z}_{2^8}$ is considered as $(0, 1, 0, 0, 0, 1, 1, 1)$ of B^8.

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 B^n the following are defined:

Received July 11, 2016; Accepted October 13, 2016.
2010 Mathematics Subject Classification: Primary 94A60.
Key words and phrases: a T-function, an n-bit word, period, a single cycle property, a secure trinomial.
This work is supported by the research fund of Dankook University in 2015.

(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 $x_i \neq y_i$.

A function $f : B^n \to B^n$ 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 $k+1$ bits of an n-bit word x.

EXAMPLE 1.2. *Let $f(x) = x + 2x^2$ on $\mathbb{Z}_{2^n}$. If $x = \sum_{i=0}^{n-1} [x]_i 2^i$, then $x^2 = [x]_0 + ([x]_1 + [x]_0[x]_1)2^2 + \cdots$. Hence we have $[f(x)]_0 = [x]_0$, $[f(x)]_1 = [x]_1 + [x]_0$, $[f(x)]_2 = [x]_2$, $\cdots$, $[f(x)]_i = [x]_i + \alpha_i$, $\cdots$ where α_i is a function of $[x]_0, \cdots, [x]_{i-1}$. Hence $f(x)$ is a T-function on $\mathbb{Z}_{2^n}$. Also, $f(x)$ is an invertible T-function on $\mathbb{Z}_{2^n}$ since 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.*

It is well known in [3] that every polynomial on $\mathbb{Z}_{2^n}$ is a T-function on $\mathbb{Z}_{2^n}$. A polynomial on $\mathbb{Z}_{2^n}$ is said to be a **permutation** if it is a bijective function. A polynomial on $\mathbb{Z}_{2^n}$ with three nonzero terms is called a **trinomial**. Consequently, the degree of a trinomial is at least 2 and a trinomial of degree m is of the form $a_m x^m + a_k x^k + a_i x^i$, where a_m, a_k, a_i in $\mathbb{Z}_{2^n} - \{0\}$ with $m > k > i \geq 0$.

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 r such that $a_{i+r} = a_i$ for each nonnegative integer i, then the sequence $a_0, a_1, \cdots, a_m, \cdots$ is said to have a cycle of period r. In this case we say that $a_0, a_1, \cdots, a_{r-1}$ is a **cycle of period** r.

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

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

Then it is easy to show that $f^i(x)$ is a T-function if $f(x)$ is a T-function. Hence if $f(x)$ is a bijective T-function, then so is $f^i(x)$. Also, for any element (or word) α of $\mathbb{Z}_{2^n}$ we can get a sequence of words $\alpha_0 = \alpha, \alpha_1 = f(\alpha), \alpha_2 = f^2(\alpha), \cdots, \alpha_l = f^l(\alpha), \cdots$. 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** r in f if r is the least positive integer such that $f^r(\alpha) = \alpha$. If α has a cycle of period r in f and $\alpha_i = f^i(\alpha)$ for each nonnegative integer i, then α generates a sequence $\alpha = \alpha_0, \alpha_1, \cdots, \alpha_{r-1}, \cdots$ of period r. Also, in this case every word α_i $(0 \leq i \leq r-1)$ has a cycle of period

r. 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 cycled property** (or an **SCP**) if there is a word which has a cycle of period 2^n. Hence if f has an SCP, then every word of $\mathbb{Z}_{2^n}$ has a cycle of period 2^n and so f generates a binary sequence of period $n \cdot 2^n$, which is the longest period in f.

EXAMPLE 1.3. *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 an SCP.*

Invertible functions with an SCP have many cryptographic applications. The main context in which we study them in this paper is pseudorandom generators in stream ciphers. Modern microprocessors can directly operate on up to 64-bit words in a single clock cycle, and thus a univariate mapping can go through at most 2^{64} different states before ending a cycle. In some cryptographic applications this cycle of period 2^{64} may be too short and in addition the cryptanalyst can guess a 64-bit state in a feasible computation. A common way to increase the size of the state and extend the period of a generator is to run in parallel and combine the outputs of several generators with different period. To do this we use combination of some polynomials with an SCP. In this paper we will characterize a secure trinomial on $\mathbb{Z}_{2^n}$, which generates an n-bit word sequence with period $n \cdot 2^n$ and without consecutive elements, where $n \geq 3$. Also, an odd (or even) number means a positive odd (or even) integer.

2. A trinomial with a single cycle property

In this section we characterize trinomials with a single cycle property. Throughout this paper we may assume n is a positive integer greater than 2. Also, we write **an SCP** for a single cycle property.

PROPOSITION 2.1. *Let $f(x) = \sum_{k=0}^{m} a_k x^k$ be a polynomial on $\mathbb{Z}_{2^n}$. Then f is a permutation polynomial if and only if a_1 is odd, $a_2 + a_4 + \cdots$ is even and $a_3 + a_5 + \cdots$ is even.*

Proof. The proof follows from [7]. □

It follows from Proposition 2.1 that Proposition 2.2 is easily proved.

PROPOSITION 2.2. *(1) A linear polynomial $bx + c$ is a permutation on $\mathbb{Z}_{2^n}$ if and only if b is odd.*

(2) A quadratic polynomial $ax^2 + bx + c$ is a permutation on $\mathbb{Z}_{2^n}$ if and only if b is odd and a is nonzero even.

PROPOSITION 2.3. *A trinomial $a_m x^m + a_k x^k + a_i x^i$ in $\mathbb{Z}_{2^n}$ of degree m, where $m > k > i \geq 0$, is a permutation polynomial if and only if it is one of the following forms:*

(1) $a_m x^m + a_k x^k + a_1 x$, *where a_1 is odd and* $\begin{cases} a_m + a_k \text{ is even if } m + k \\ \text{ is even;} \\ a_m \text{ and } a_k \text{ are even if } m \\ \text{ } + k \text{ is odd.} \end{cases}$

(2) $a_m x^m + a_1 x + a_0$, *where a_1 is odd and a_m is even.*

Proof. Since a permutation polynomial has a nonzero term of degree 1 we have two cases: (1) $i = 1$ and (2) $k = 1$. By Proposition 2.1 we get following results:
(1) If $i = 1$, then a_1 is odd and $a_m + a_k$ is even. If $m + k$ is odd, then both a_m and a_k are even. If $m + k$ is even, then both a_m and a_k are either odd or even. That is, $a_m + a_k$ is even.
(2) If $k = 1$, then a_0 is arbitrary, a_1 is odd and a_m is even. □

A special case of (2) in Proposition 2.3 is (2) in Proposition 2.2. If a trinomial $f(x) = a_m x^m + a_k x^k + a_i x^i$ in $\mathbb{Z}_{2^n}$ of degree m, where $m > k > i \geq 0$ has an SCP, then $f(x)$ has no fixed points. Consequently, $f(x) = a_m x^m + a_1 x + a_0$, where a_0, a_1 is odd and a_m is even.

PROPOSITION 2.4. *Let $f(x)$ be a T-function on $\mathbb{Z}_{2^n}$. Then the period of $f(x)$ is of the form 2^k, where k is a nonnegative integer not greater than n.*

Proof. The proof follows from [2]. □

PROPOSITION 2.5. *A polynomial $f(x)$ has an SCP on $\mathbb{Z}_{2^n}$ (for any $n \geq 3$) if and only if it has an SCP on $\mathbb{Z}_{2^3}$.*

Proof. The proof follows from [3]. □

The proof of following two propositions may be found in [5,6]

PROPOSITION 2.6. *A polynomial $bx + c$ on $\mathbb{Z}_{2^n}$ has an SCP if and only if $b \equiv 1 \bmod 4$ and $c \equiv 1 \bmod 2$.*

PROPOSITION 2.7. *A polynomial $ax^2 + bx + c$ on $\mathbb{Z}_{2^n}$ has an SCP if and only if one of the following is satisfied:*

(1) $a \equiv 2 \bmod 4$, $b \equiv 3 \bmod 4$, *and* $c \equiv 1 \bmod 2$

(2) $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 4$, *and* $c \equiv 1 \bmod 2$

PROPOSITION 2.8. *Let $f(x) = ax^m + bx + c$ be a trinomial on $\mathbb{Z}_{2^n}$. If m is even, then $f(x)$ has an SCP if and only if one of the following is satisfied:*

(1) $a \equiv 2 \bmod 4$, $b \equiv 3 \bmod 4$ *and* $c \equiv 1 \bmod 2$

(2) $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 4$ *and* $c \equiv 1 \bmod 2$

Proof. Since $f(x)$ is a permutation polynomial, by Proposition 2.3 a is even and b is odd. Note that $a\alpha^2 \equiv \begin{cases} a \bmod 8 \text{ if } \alpha \text{ is odd} \\ 0 \bmod 8 \text{ if } \alpha \text{ is even.} \end{cases}$ Hence $a(\alpha^2)^k \equiv a\alpha^2 \bmod 8$ and $f(\alpha) = a\alpha^m + b\alpha + c \equiv a\alpha^2 + b\alpha + c \bmod 8$ for every element α in $\mathbb{Z}_{2^3}$. Hence $f(x) = ax^m + bx + c \equiv ax^2 + bx + c \bmod 8$. Thus by Proposition 2.7 it holds. □

PROPOSITION 2.9. *Let $f(x) = ax^m + bx + c$ be a trinomial on $\mathbb{Z}_{2^n}$. If m is odd, then $f(x)$ has an SCP if and only if $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 4$ and $c \equiv 1 \bmod 2$.*

Proof. Since $f(x)$ is a permutation polynomial, by Proposition 2.3 a is even. Note that $a\alpha^2 \equiv \begin{cases} a \bmod 8 \text{ if } \alpha \text{ is odd} \\ 0 \bmod 8 \text{ if } \alpha \text{ is even.} \end{cases}$ Hence $a(\alpha^2)^k \equiv a\alpha^2 \bmod 8$ and $f(\alpha) = a\alpha^m + b\alpha + c \equiv a\alpha^3 + b\alpha + c \bmod 8$ for every element α in $\mathbb{Z}_{2^3}$. Hence $f(x) = ax^m + bx + c \equiv ax^3 + bx + c \bmod 8$. It remains to characterize $ax^3 + bx + c$ with an SCP, where a is even and b is odd. Since $f(x)$ has an SCP, c is odd. Since $f(x)$ has an SCP modulo 8, $f(x)$ has an SCP modulo 4. From the eight cases $2x^3 + x + 1$, $2x^3 + x + 3$, $2x^3 + 3x + 1$, $2x^3 + 3x + 3$, $x + 1$, $x + 3$, $3x + 1$ and $3x + 3$, by an easy calculation we find $2x^3 + 3x + 1$, $2x^3 + 3x + 3$, $x + 1$ and $x + 3$ have an SCP modulo 4. To get trinomials with an SCP modulo 8, it is enough to check the following: $(4s+2)x^3 + (4t+3)x + (4u+1)$, $(4s+2)x^3 + (4t+3)x + (4u+3)$, $4x^3 + (4s+1)x + (4t+1)$ and $4x^3 + (4s+1)x + (4t+3)$, where s, t and u are in $\{0, 1\}$.
If $f(x) = (4s + 2)x^3 + (4t + 3)x + (4u + 1)$, then note the following:

$f(0) = 4u+1$,
$f^2(0) = f(4u+1) = (4s+2)(4u+1)^3 + (4t+3)(4u+1) + (4u+1)$

$$\equiv (4s+2)(4u+1)+(4t+3)(4u+1)+(4u+1)$$
$$\equiv 4(s+t+1)+2 \mod 8$$
$$f^3(0)=f(4(s+t+1)+2)\equiv(4t+3)[4(s+t+1)+2]+(4u+1)$$
$$\equiv 4(s+t+1)+6+(4u+1)$$
$$\equiv 4(s+t+u)+3 \mod 8$$
$$f^4(0)=f(4(s+t+u)+3)\equiv(4s+2)3+(4t+3)(4(s+t+u)+3)+(4u+1)$$
$$\equiv (4s+6)+(4t+9+4s+4t+4u)+(4u+1)$$
$$\equiv 0 \mod 8.$$

Hence $f(x)$ does not have an SCP. Similarly, $f(x)=(4s+2)x^3+(4t+3)x+(4u+3)$ does not have an SCP. If $f(x)=4x^3+(4s+1)x+(2t+1)$, then note the following:

$f(0)=2t+1$,

$f^2(0)=f(2t+1)\equiv 4+(2t+4s+1)+(2t+1)\equiv 4(s+t+1)+2 \bmod 8$,

$f^3(0)=f(4(s+t+1)+2)\equiv(4s+1)[4(s+t+1)+2]+(2t+1)$
$$\equiv 4s+6t+7 \bmod 8,$$

$f^4(0)=f(4s+6t+7)\equiv 4+(4s+1)(4s+6t+7)+2t+1\equiv 4 \bmod 8$.
Hence by Proposition 2.4 $f(x)$ has an SCP on $\mathbb{Z}_{2^3}$. Therefore, by Proposition 2.5 we have proved this proposition. □

3. Secure trinomials

An n-bit word sequence $a_0=a, a_1, \cdots, a_i, \cdots, a_m, \cdots$ is said to have consecutive elements if $a_{i+1}=a_i+1$ or $a_{j+1}=a_j-1$ for some integers i and j. A function f on $\mathbb{Z}_{2^n}$ with an SCP is said to be **pseudo secure** if there is no integer i such that $f^{i+1}(a)=f^i(a)+1$ or there is no integer j such that $f^{j+1}(a)=f^j(a)-1$, where $a_0=a$ and $a_m=f^m(a)$ for any positive integer m. In particular, a function f on $\mathbb{Z}_{2^n}$ with an SCP is said to be **secure** if every n-bit word sequence has no consecutive elements.

PROPOSITION 3.1. *A trinomial $f(x)=ax^m+bx+c$ on $\mathbb{Z}_{2^n}$ has an SCP if and only if it is pseudo secure.*

Proof. Suppose that $f(x)$ is pseudo secure. Then by the definition of pseudo secure $f(x)$ has an SCP.

Conversely, suppose that $f(x) = ax^m + bx + c$ on $\mathbb{Z}_{2^n}$ has an SCP for an even number m. Then it is one of the following:

(i) $a \equiv 2 \bmod 4,\ b \equiv 3 \bmod 4$ and $c \equiv 1 \bmod 2$.

(ii) $a \equiv 0 \bmod 4,\ b \equiv 1 \bmod 4$ and $c \equiv 1 \bmod 2$.

If $a \equiv 2 \bmod 4$, $b \equiv 3 \bmod 4$ and $c \equiv 1 \bmod 2$, then $a = 4s + 2$, $b = 4t + 3$ and $c = 4u + 1$ or $c = 4u + 3$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. Let $f(x) = (4s+2)x^m + (4t+3)x + 4u + 1$. If $f(x) \equiv x - 1 \bmod 2^n$, then $(4s+2)x^m + (4t+2)x + 4u + 2 \equiv 0 \bmod 2^n$ and $4(sx^m + tx + u) + 2x(x^{m-1} + 1) + 2 \equiv 0 \bmod 2^n$. Since $2x(x^{m-1}+1) \equiv 0 \bmod 4$ for every element x in $\mathbb{Z}_{2^n}$ we have $4(sx^m + tx) + 2x(x^{m-1}+1) + 2 \not\equiv 0 \bmod 2^n$ for every element x in $\mathbb{Z}_{2^n}$. Hence $f(x) \not\equiv x - 1 \bmod 2^n$ for every element x in $\mathbb{Z}_{2^n}$ and so $f(x)$ is pseudo secure. Also, let $f(x) = (4s + 2)x^m + (4t + 3)x + 4u + 3$. Similarly, we can prove $f(x) \not\equiv x + 1 \bmod 2^n$ for every element x in $\mathbb{Z}_{2^n}$. Hence $f(x)$ is pseudo secure.
If $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 4$ and $c \equiv 1 \bmod 2$, then $a = 4s$, $b = 4t + 1$ and $c = 4u + 1$ or $c = 4u + 3$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. By the above argument we can easily show that $f(x)$ is pseudo secure.
Now, suppose that $f(x) = ax^m + bx + c$ on $\mathbb{Z}_{2^n}$ has an SCP for an odd number m. Then $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 4$ and $c \equiv 1 \bmod 2$. By the above argument we can easily show that $f(x)$ is pseudo secure. □

PROPOSITION 3.2. *Let m be an even number and $f(x) = ax^m + bx + c$ a trinomial on $\mathbb{Z}_{2^n}$, where $a \equiv 2 \bmod 4$, $b \equiv 3 \bmod 4$ and $c \equiv 1 \bmod 2$. Then $f(x)$ is not secure.*

Proof. Suppose that $a \equiv 2 \bmod 4$, $b \equiv 3 \bmod 4$ and $c \equiv 1 \bmod 2$. Then $a = 4s + 2$, $b = 4t + 3$ and $c = 4u + 1$ or $4u + 3$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. Let $f(x) = (4s + 2)x^m + (4t + 3)x + 4u + 1$. In this case we show $f(x) \equiv x + 1 \bmod 2^n$ has a solution for any elements s, t, u in $\mathbb{Z}_{2^n}$ to prove that $f(x)$ is not secure. From above congruence we have

$$(4s + 2)x^m + (4t + 2)x + 4u \equiv 0 \bmod 2^n \text{ or}$$

$$4(sx^m + tx + u) + 2x^m + 2x \equiv 0 \bmod 2^n.$$

It suffices to show $g(x) \equiv 2(sx^m + tx + u) + x^m + x + 2k \equiv 0 \bmod 2^{n-1}$ has a solution for any elements s, t and u. If $n = 2$, then it is clear that $g(x)$ has a solution. Assume that $g(x)$ has a solution modulo 2^k, say $x \equiv a \bmod 2^k$. That is,
$g(a) \equiv 2(sa^m + ta + u) + a^m + a \equiv 0 \bmod 2^k$ or $2(sa^m + ta + u) + a^m + a = 2^k q$

for some integer q. Let $x = a + 2^k l$ be a solution of $g(x)$ modulo 2^{k+1}. Then

$$\begin{aligned} g(a+2^k l) &\equiv 2\{s(a+2^k l)^m + t(a+2^k l) + u\} + (a+2^k l)^m + (a+2^k l) \\ &\equiv 2(sa^m + ta + u) + a^m + a + 2^k l \\ &\equiv (q+l)2^k \\ &\equiv 0 \bmod 2^{k+1} \end{aligned}$$

Hence we can choose l so that $g(x)$ has a solution modulo 2^{k+1}. Consequently, by mathematical induction $g(x) \equiv 0 \bmod 2^{n-1}$ has a solution for any n. Also, if $f(x) = (4s+2)x^m + (4t+3)x + (4u+3)$, then by a similar argument $f(x) \equiv x - 1 \mod 2^n$ has a solution for any n. Thus $f(x)$ is not secure. □

PROPOSITION 3.3. *Let $f(x) = ax^m + bx + c$ be a trinomial on $\mathbb{Z}_{2^n}$, where $a \equiv 4$ mod 8, $b \equiv 5$ mod 8 and $c \equiv \pm 1$ mod 8. Then $f(x)$ is not secure.*

Proof. Suppose that $a \equiv 4 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv 1 \bmod 8$. Then $a = 4 + 8s$, $b = 5 + 8t$ and $c = 1 + 8u$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. So $f(x) = (4+8s)x^m + (5+8t)x + 1 + 8u$. In this case we show $f(x) \equiv x + 1 \bmod 2^n$ has a solution for any elements s, t, u in $\mathbb{Z}_{2^n}$. From above congruence we have

$$(4+8s)x^m + (4+8t)x + 8u \equiv 0 \bmod 2^n \text{ or}$$
$$2(sx^m + tx + u) + x^m + x \equiv 0 \bmod 2^{n-2}.$$

If $n = 3$, then $f(x) \equiv x + 1 \bmod 2^n$ has a solution for any elements s, t, u in $\mathbb{Z}_{2^n}$. Assume that $x \equiv a \bmod 2^k$ is a solution of $2(sx^m + tx + u) + x^m + x \equiv 0 \bmod 2^k$ and let $x = a + 2^k l$. Consider $2\{s(a+2^k l)^m + t(a + 2^k l) + u\} + (a+2^k l)^m + (a+2^k l) \pmod{2^{k+1}}$:
Since $2(sa^m + ta + u) + a^m + a \equiv 0 \bmod 2^k$, we get $2(sa^m + ta + 2^k lt + u) + a^m + a + 2^k l \equiv 2^k l + 2(sa^m + ta + u) + a^m + a \pmod{2^{k+1}}$ and $2^k l + 2(sa^m + ta + u) + a^m + a \equiv 0 \pmod{2^{k+1}}$ has a solution for l. Therefore by mathematical induction $f(x) \equiv x + 1 \bmod 2^n$ has a solution for any elements s, t, u in $\mathbb{Z}_{2^n}$.
Suppose that $a \equiv 4 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv -1 \bmod 8$. Then $a = 4 + 8s$, $b = 5 + 8t$ and $c = -1 + 8u$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. So $f(x) = (4+8s)x^m + (5+8t)x - 1 + 8u$. From the congruence $f(x) \equiv x - 1 \bmod 2^n$ we have

$$(4+8s)x^m + (4+8t)x + 8u \equiv 0 \bmod 2^n \text{ or}$$
$$2(sx^m + tx + u) + x^m + x \equiv 0 \bmod 2^{n-2}.$$

By the above argument $f(x) \equiv x - 1 \bmod 2^n$ has a solution for any elements s, t, u in $\mathbb{Z}_{2^n}$.
Therefore $f(x)$ is not secure. □

PROPOSITION 3.4. *Let $f(x) = ax^m + bx + c$ be a trinomial on $\mathbb{Z}_{2^n}$, where $a \equiv 4 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv \pm 3 \bmod 8$. Then $f(x)$ is secure.*

Proof. Suppose that $a \equiv 4 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv 3 \bmod 8$. Then $a = 4 + 8s$, $b = 5 + 8t$ and $c = 3 + 8u$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. So $f(x) = (4 + 8s)x^m + (5 + 8t)x + 3 + 8u$. If $f(x) \equiv x + 1 \bmod 2^n$, then $(4 + 8s)x^m + (4 + 8t)x + 2 + 8u \equiv 0 \bmod 2^n$. Hence we have $4[(1 + 2s)x^m + (1 + 2t)x + 2u] + 2 \not\equiv 0 \bmod 2^n$, a contradiction. So $f(x) \equiv x + 1 \bmod 2^n$ has no solutions for any elements s, t, u in $\mathbb{Z}_{2^n}$. Also, if $f(x) \equiv x - 1 \bmod 2^n$, then $(4+8s)x^m+(4+8t)x+4+8u \equiv 0 \bmod 2^n$ and $8(sx^m + tx + u) + 4(x^m + x) + 4 \equiv 0 \bmod 2^n$. Since $x^m + x \equiv 0 \bmod 2$, we have $f(x) \not\equiv 0 \bmod 2^n$, a contradiction. So $f(x) \equiv x - 1 \bmod 2^n$ has no solutions for any elements s, t, u in $\mathbb{Z}_{2^n}$. Hence $f(x)$ is secure. Similarly we can prove that $f(x)$ is secure for the case $a \equiv 4 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv -3 \bmod 8$. □

EXAMPLE 3.5. *Consider polynomials $f_1(x) = 4x^2+5x+3$ and $f_2(x) = 4x^3 + 5x + 3$ over $\mathbb{Z}_{2^3}$. Then $a = 0$, $a_1 = f_i(0) = 3$, $a_2 = 6$, $a_3 = 1$, $a_4 = 4$, $a_5 = 7$, $a_6 = 2$, $a_7 = 5$, where $i = 1, 2$. Hence $f_1(x)$ and $f_2(x)$ generate the same secure sequence modulo 2^3. Consider sequences modulo 2^4 generated by $f_i(x)$, where $i = 1, 2$. Then $f_1(x)$ generates $a = 0$, $a_1 = f_1(0) = 3$, $a_2 = 6$, $a_3 = 1$, $a_4 = 12$, $a_5 = 15$, $a_6 = 2$, $a_7 = 13$, $a_8 = 8, \cdots$ and $f_2(x)$ generates $a = 0$, $a_1 = f_2(0) = 3$, $a_2 = 14$, $a_3 = 9$, $a_4 = 4$, $a_5 = 7$, $a_6 = 2$, $a_7 = 13$, $a_8 = 8, \cdots$. Hence $f_1(x)$ and $f_2(x)$ generate different secure sequences modulo 2^n for every integer $n \geq 4$.*

PROPOSITION 3.6. *Let $f(x) = ax^m + bx + c$ be a trinomial on $\mathbb{Z}_{2^n}$, where $a \equiv 0 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv \pm 1 \bmod 8$. Then $f(x)$ is not secure.*

Proof. Suppose that $a \equiv 0 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv 1 \bmod 8$. Then $a = 8s$, $b = 5 + 8t$ and $c = 1 + 8u$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. So $f(x) = 8sx^m + (5 + 8t)x + 1 + 8u$. If $f(x) \equiv x + 1 \bmod 2^n$, then $8sx^m + (4 + 8t)x + 8u \equiv 0 \bmod 2^n$ or $8(sx^m + tx + u) + 4x \equiv 0 \bmod 2^n$, which has a solution for any elements s, t, u in $\mathbb{Z}_{2^n}$. So $f(x)$ is not secure. Similarly, we can prove that $f(x)$ is not secure for the case $a \equiv 0$

mod 8, $b \equiv 5 \bmod 8$ and $c \equiv -1 \bmod 8$ by showing that $f(x) \equiv x - 1 \bmod 2^n$ has a solution for any elements s, t, u in $\mathbb{Z}_{2^n}$. □

PROPOSITION 3.7. *Let $f(x) = ax^m + bx + c$ be a trinomial on $\mathbb{Z}_{2^n}$, where $a \equiv 0$ mod 8, $b \equiv 5$ mod 8 and $c \equiv \pm 3$ mod 8. Then $f(x)$ is not secure.*

Proof. Suppose that $a \equiv 0 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv 3 \bmod 8$. Then $a = 8s$, $b = 5 + 8t$ and $c = 3 + 8u$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. So $f(x) = 8sx^m + (5 + 8t)x + 3 + 8u$. If $f(x) \equiv x - 1 \bmod 2^n$, then $8sx^m + (4 + 8t)x + 4 + 8u \equiv 0 \bmod 2^n$ or $8(sx^m + tx + u) + 4(x + 1) \equiv 0 \bmod 2^n$, which has a solution for any elements s, t, u in $\mathbb{Z}_{2^n}$. Hence $f(x)$ is not secure. Similarly, we can prove that $f(x)$ is not secure for the case when $a \equiv 0 \bmod 8$, $b \equiv 5 \bmod 8$ and $c \equiv -3 \bmod 8$. □

PROPOSITION 3.8. *Let $f(x) = ax^m + bx + c$ be a trinomial on $\mathbb{Z}_{2^n}$, where $a \equiv 0$ mod 8, $b \equiv 1$ mod 8 and $c \equiv \pm 3$ mod 8. Then $f(x)$ is secure.*

Proof. Suppose that $a \equiv 0 \bmod 8$, $b \equiv 1 \bmod 8$ and $c \equiv 3 \bmod 8$. Then $a = 8s$, $b = 1 + 8t$ and $c = 3 + 8u$ for some elements s, t, u in $\mathbb{Z}_{2^n}$. So $f(x) = 8sx^m + (1 + 8t)x + 3 + 8u$. If $f(x) \equiv x + 1 \bmod 2^n$, then $8sx^m + 8tx + 2 + 8u \equiv 0 \bmod 2^n$ or $8(sx^m + tx + u) + 2 \equiv 0 \bmod 2^n$, which has no solution for any elements s, t, u in $\mathbb{Z}_{2^n}$. Hence $f(x) \equiv x + 1 \bmod 2^n$ has no solutions. If $f(x) \equiv x - 1 \bmod 2^n$, then $8sx^m + 8tx + 4 + 8u \equiv 0 \bmod 2^n$ or $8(sx^m + tx + u) + 4 \equiv 0 \bmod 2^n$, which has no solution for any elements s, t, u in $\mathbb{Z}_{2^n}$. Hence $f(x) \equiv x - 1 \bmod 2^n$ has no solutions. Thus $f(x)$ is secure. Similarly, we can prove that $f(x)$ is secure for the case $a \equiv 0 \bmod 8$, $b \equiv 1 \bmod 8$ and $c \equiv -3 \bmod 8$. □

EXAMPLE 3.9. *Consider polynomials $f_3(x) = 8x^2 + x + 3$ and $f_4(x) = 8x^3 + x + 3$ over $\mathbb{Z}_{2^4}$. Note that $f_1(x)$ generates $a = 0$, $a_1 = f_1(0) = 3$, $a_2 = 14$, $a_3 = 1$, $a_4 = 12$, $a_5 = 15$, $a_6 = 10$, $a_7 = 13$, $a_8 = 8$, $\cdots$ and $f_2(x)$ generates $a = 0$, $a_1 = f_2(0) = 3$, $a_2 = 14$, $a_3 = 1$, $a_4 = 4$, $a_5 = 7$, $a_6 = 2$, $a_7 = 13$, $a_8 = 8$, $\cdots$. In fact, $f_3(x) \equiv f_4(x)$ mod 2^4 since $8x(x - 1) \equiv 0$ mod 2^4. So $f_3(x)$ and $f_4(x)$ generate the same secure sequence modulo 2^4. But $f_3(x)$ and $f_4(x)$ generate different secure sequences modulo 2^n for every integer $n \geq 5$.*

From above six propositions we have Theorem 3.10.

THEOREM 3.10. *Let $f(x) = ax^m + bx + c$ be a trinomial on $\mathbb{Z}_{2^n}$. Then:*

(1) *If* $a \equiv 4 \ mod\ 8$, $b \equiv 5 \ mod\ 8$ *and* $c \equiv \pm 1 \ mod\ 8$, *then* $f(x)$ *is not secure.*
(2) *If* $a \equiv 4 \ mod\ 8$, $b \equiv 5 \ mod\ 8$ *and* $c \equiv \pm 3 \ mod\ 8$, *then* $f(x)$ *is secure.*
(3) *If* $a \equiv 0 \ mod\ 8$, $b \equiv 1 \ mod\ 8$ *and* $c \equiv \pm 3 \ mod\ 8$, *then* $f(x)$ *is secure.*
(4) *If* $a \equiv 0 \ mod\ 8$, $b \equiv 5 \ mod\ 8$ *and* $c \equiv \pm 1 \ mod\ 8$, *then* $f(x)$ *is not secure.*
(5) *If* $a \equiv 0 \ mod\ 8$, $b \equiv 5 \ mod\ 8$ *and* $c \equiv \pm 3 \ mod\ 8$, *then* $f(x)$ *is not secure.*

REMARK 3.11. As we explained, a trinomial $f(x) = ax^m + bx + c$ on $\mathbb{Z}_{2^n}$ has an SCP if and only if it is one of the following:

(1) If m is even, then (i) $a \equiv 2 \bmod 4$, $b \equiv 3 \bmod 4$ and $c \equiv 1 \bmod 2$.

(ii) $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 4$ and $c \equiv 1 \bmod 2$.

(2) If m is odd, then $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 4$ and $c \equiv 1 \bmod 2$.

If m is even and $a \equiv 2 \bmod 4$, $b \equiv 3 \bmod 4$ and $c \equiv 1 \bmod 2$, then by Proposition 3.2 $f(x)$ is not secure. In Theorem 3.10 we have characterized $f(x)$ with above 5 cases among 8 cases. So there are 3 cases left for $f(x)$ as below:

(1) If $a \equiv 4 \bmod 8$, $b \equiv 1 \bmod 8$ and $c \equiv \pm 3 \bmod 8$.
(2) If $a \equiv 4 \bmod 8$, $b \equiv 1 \bmod 8$ and $c \equiv \pm 1 \bmod 8$.
(3) If $a \equiv 0 \bmod 8$, $b \equiv 1 \bmod 8$ and $c \equiv \pm 1 \bmod 8$.

But those cases $f(x)$ may be or may not secure. We conclude Remark 3.11 with two trinomials for (2) $a \equiv 4 \bmod 8$, $b \equiv 1 \bmod 8$ and $c \equiv \pm 1 \bmod 8$. With an easy calculation $f(x) = 4x^3 + x + 9$ is secure but $g(x) = 4x^3 + x + 1$ is not secure.

References

[1] A. Kilmov, *Applications of T-functions in cryptography,* Ph.D. Thesis, Weizmann Institute Science, 2005.
[2] A. Kilmov and A. Shamir, *A new class of invertible mappings,* CHES 2002, LNCS **2523** (2003), 470-483.
[3] A. Kilmov and A. Shamir, *Cryptographic applications of T-functions,* SAC 2003, LNCS **3006** (2004), 248-261.
[4] A. Kilmov and A. Shamir, *New cryptographic primitives based on multiword T-functions,* FSE 2004, LNCS **3017** (2004), 1-15.
[5] M. S. Rhee, *On a characterization of T-function with one cycle property,* J. of the Chungcheong Math. Soc. **21** (2008), no. 2, 259-268.

[6] M. S. Rhee, *On a secure binary sequences generated by a quadratic polynomial on* $\mathbb{Z}_{2^n}$, J. of the Applied Math. and Informatics **29** (2011), no. 1-2, 247-255.
[7] R. L. Rivest, *Permutation polynomials modulo* 2^w, Finite fields and their applications **7** (2001), 287-292.

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