J. Appl. Math. & Informatics Vol. **29***(2011), No. 1 - 2, pp. 247 - 255*
Website: http://www.kcam.biz

ON A SECURE BINARY SEQUENCE GENERATED BY A QUADRATIC POLYNOMIAL ON $\mathbb{Z}_{2^n}$ †

MIN SURP RHEE

ABSTRACT. Invertible functions with a single cycle property have many cryptographic applications. The main context in which we study them in this paper is pseudo random generation and stream ciphers. In some cryptographic applications we need a generator which generates binary sequences of period long enough. 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. In this paper we will characterize a secure quadratic polynomial on $\mathbb{Z}_{2^n}$, which generates a binary sequence of period long enough and without consecutive elements.

AMS Mathematics Subject Classification : 94A60
Key words and phrases : T-function, n-bit word, a single cycle property

1. Introduction

Let $B^n = \{(x_{n-1}, x_{n-2}, \cdots, x_1, x_0) | x_i \in B\}$ be the set of all n-tuples of elements in B, where $B = \{0, 1\}$ is a field. Then an element of B is called a **bit** and an element of B^n is called an n **- bit word** or simply a **word**. An element x of B^n can be represented as $([x]_{n-1}, [x]_{n-2}, \cdots, [x]_1, [x]_0)$, where $[x]_{i-1}$ is the i-th component from the right end of x. It is often useful to express an n-bit word x as an element $\sum_{i=0}^{n-1} [x]_i 2^i$ of $\mathbb{Z}_{2^n}$, where $\mathbb{Z}_{2^n}$ is the integer residue ring modulo 2^n. In this expression every n-bit word x of B^n is considered as an element of $\mathbb{Z}_{2^n}$ and the set B^n as the set $\mathbb{Z}_{2^n}$. For example, an element $(0, 0, 1, 1, 1, 0, 0, 1)$ of B^8 is considered as 57 in $\mathbb{Z}_{2^8}$.

Definition 1.1 For any n-bit words $(x_{n-1}, x_{n-2}, \cdots, x_1, x_0)$ and $(y_{n-1}, y_{n-2}, \cdots, y_1, y_0)$ of $\mathbb{Z}_{2^n}$, the following operations are defind:
(1) $x \pm y$ and xy are defined as $x \pm y \mod 2^n$ and $xy \mod 2^n$, respectively.

Received July 22, 2010. Revised October 18, 2010. Accepted October 28, 2010.
†The present research was conducted by the research fund of Dankook University in 2009.

(2) $x \oplus y$ is defined as $z = (z_{n-1}, z_{n-2}, \cdots, z_0)$, where $z_i = x_i \oplus y_i$ is the addition of x_i and y_i in B for all $i = 0, 1, \cdots, n-1$.

(3) $\bar{x}$ is defined as $(z_{n-1}, z_{n-2}, \cdots, z_0)$, where $z_i = 1 \oplus x_i$ for all $i = 0, 1, \cdots, n-1$.

(4) $-x$ is defined as $2^n - x \bmod 2^n$.

A function f from B^n to B^n is said to be a $\mathbf{T-function}$(short for a triangular function) if the k-th bit $[f(x)]_{k-1}$ of an n-bit word $f(x)$ only depends on the first k bits $[x]_0, \cdots, [x]_{k-1}$ of an n-bit word x.

Example 1.1 Let $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ be a function defined by $f(x) = x + 1$. Then $[f(x)]_0$ only depends on $[x]_0$ since $[f(x)]_0 = [x+1]_0 = [x]_0 \oplus [1]_0 = [x]_0 \oplus 1$. Note that $[f(x)]_1 = [x+1]_1 = [x]_1 \oplus \alpha_1([x]_0)$, where $\alpha_1([x]_0) = \begin{cases} 0 & \text{if } [x]_0 = 0 \\ 1 & \text{if } [x]_0 = 1. \end{cases}$ Hence $[f(x)]_1$ only depends on $[x]_1$ and $[x]_0$. Similarly $[f(x)]_2$ only depends on $[x]_2$ and $[x]_1 \oplus \alpha_1([x]_0)$. So we may express as $[f(x)]_2 = [x+1]_2 = [x]_2 \oplus \alpha_2([x]_0, [x]_1)$. Hence $[f(x)]_2$ only depends on $[x]_2, [x]_1$ and $[x]_0$. Continuing this process until getting $[f(x)]_{n-1}$, $[f(x)]_{n-1}$ can be obtained from $[x]_{n-1}, [x]_{n-2}, \cdots, [x]_1, [x]_0$. Therefore $f(x)$ is a T-function.

It is well known that every polynomial $f(x)$ on $\mathbb{Z}_{2^n}$ is a T-function[4]. A polynomial on $\mathbb{Z}_{2^n}$ is said to be **a permutation polynomial** if it is a bijective function on $\mathbb{Z}_{2^n}$.

It follows from Definition 1.1 that Proposition 1.2 can be easily proved.

Proposition 1.2 If $f : B^n \to B^n$ and $g : B^n \to B^n$ are T-functions, then the composition $g \circ f : B^n \to B^n$ is a T-function. If $f : B^n \to B^n$ and $g : B^n \to B^n$ are permutation polynomials, then the composition $g \circ f : B^n \to B^n$ is a permutation polynomial.

Let $a_0, a_1, \cdots, a_m, \cdots$ be a sequence of numbers(or a word sequence) 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 $a_0, a_1, \cdots, a_m, \cdots$ is called **a word sequence of period** r. Also in this case we say that $a_i, a_{i+1}, \cdots, a_{i+r-1}$ is **a cycle of length** r for each nonnegative integer i.

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

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

Then we get a word sequence $f^0(x), f(x), \cdots, f^i(x), \cdots, f^m(x), \cdots$ for every element $x \in \mathbb{Z}_{2^n}$.

A word α of $\mathbb{Z}_{2^n}$ has **a cycle of period** r in f if r is the least positive integer such that $f^r(\alpha) = \alpha$. In particular, a word α is said to be a **a fixed word** if α has a cycle of length 1. Also, f is said to have **a single cycle property** 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.

Consider a sequence of words

$$\alpha_0 = f^0(\alpha) = \alpha,\ \alpha_1 = f(\alpha), \cdots, \alpha_i = f^i(\alpha), \cdots, \alpha_m = f^m(\alpha), \cdots$$

where a word α of $\mathbb{Z}_{2^n}$ has a cycle of length r in f. Then the r words

$$\alpha_0 = f^0(\alpha) = \alpha,\ \alpha_1 = f(\alpha), \cdots, \alpha_i = f^i(\alpha), \cdots, \alpha_{r-1} = f^{r-1}(\alpha)$$

are repeated in the sequence $\alpha_0, \alpha_1, \cdots, \alpha_m, \cdots$.

We may consider that a word α of $\mathbb{Z}_{2^n}$ which has a cycle of length r in f generates a binary sequence of period $r \cdot n$. Hence a T-function f that has a single cycle property generates a binary sequence of period $n \cdot 2^n$, which is the longest period(or maximal length cycle) in f.

The following proposition can be easily found in [1].

Proposition 1.3 Let f be an invertible T-function on $\mathbb{Z}_{2^n}$. Then every element of $\mathbb{Z}_{2^n}$ has a cycle of length 2^l in f for some $l \leq n$.

Proposition 1.4 and Proposition 1.5 can be easily obtained from Proposition 1.3 and the definition of a single cycle property.

Proposition 1.4 Let f be a T-function on Z_{2^n}. Then f has a single cycle property if and only if $f^{2^{n-1}}(0) = 2^{n-1} \bmod 2^n$.

Proposition 1.5 If $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ has a single cycle property, then $\mathbb{Z}_{2^n} = \{f^i(x) | i \in \mathbb{Z}_{2^n}\}$ for every element $x \in \mathbb{Z}_{2^n}$. In particular, $\mathbb{Z}_{2^n} = \{f^i(0) | i \in \mathbb{Z}_{2^n}\}$. Consequently, f is an invertible function on $\mathbb{Z}_{2^n}$.

The following is an example which explains above definitions and propositions.

Example 1.2 Let's consider a function f defined by $f(x) = x(2x+1) \bmod 2^4$. Then f is a bijective T-function. Consider the following :

(i) $f(0) = 0$, $f(4) = 4$, $f(8) = 8$ and $f(12) = 12$,

(ii) $f(2) = 10$ and $f^2(2) = 2$, $f(6) = 14$ and $f^2(6) = 6$.

(iii) $f(1) = 3$, $f^2(1) = 5$, $\cdots$, $f^7(1) = 15$, $f^8(1) = 1$.

Hence we know the following :

(i) 0, 4, 8, 12 are fixed words

(ii) 2, 6, 10, 14 are words which have a cycle of length 2,

(iii) every odd element has a cycle of length 2^3.

Consequently, 1 generates a binary sequence of period $4 \cdot 2^3$ as follows:

0001 0011 0101 0111 1001 1011 1101 1111.

In fact the function f defined by $f(x) = x(2x+1) \bmod 2^n$ is used in RC6, which is one of 5 candidate algorithms that were chosen in the second test of AES(advanced encryption standard). But this function is very unsuitable for PRNG(pseudo random number generator) since each word is either a fixed point or satisfies a special relation. In this sense a function which has a single cycle property is very important for PRNG.

2. Secure binary sequences

Invertible functions with a single cycle property have many cryptographic applications. The main context in which we study them in this paper is pseudorandom generation and 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 entering a cycle. In some cryptographic applications this cycle length 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 a single cycle property. In this paper we will characterize a secure quadratic polynomial on $\mathbb{Z}_{2^n}$, which generates a binary sequence of period long enough and without consecutive elements.

A word sequence $\{a, f(a), f^2(a), \cdots, f^t(a), \cdots\}$ of a function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is said to have **consecutive elements** if $f^{i+1}(x) = f^i(x)+1$ or $f^{i+1}(x) = f^i(x)-1$ for some elements x and i in $\mathbb{Z}_{2^n}$. A function f with a single cycle property on $\mathbb{Z}_{2^n}$ is said to be **pseudo secure** if $f^{i+1}(x) \neq f^i(x)+1$ for all elements x and i in $\mathbb{Z}_{2^n}$ or $f^{i+1}(x) \neq f^i(x)-1$ for all elements x and i in $\mathbb{Z}_{2^n}$.

But some pseudo secure polynomials can not be used in cipher systems. For example, the function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ defined by $f(x) = x+1$ is not good for a generator even it is pseudo secure.

Now we will define a new concept for a function on $\mathbb{Z}_{2^n}$.

Definition 2.1 A function f on $\mathbb{Z}_{2^n}$ is said to be **secure** if it has a single cycle property and every word sequence generated by f has no consecutive elements.

In this chapter we characterize quadratic polynomials on $\mathbb{Z}_{2^n}$ which are secure. The following two propositions are well known by Rivests[4].

Proposition 2.2 Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ be a polynomial on $\mathbb{Z}_{2^n}$. Then f is a permutation polynomial modulo 2 if and only if $(a_1 + a_2 + \cdots + a_m)$ is odd.

Proposition 2.3 Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ be a polynomial on $\mathbb{Z}_{2^n}$. Then f is a permutation polynomial modulo $\mathbb{Z}_{2^n}$, $n > 1$, if and only if a_1 is odd, $(a_2 + a_4 + a_6 + \cdots)$ is even, and $(a_3 + a_5 + a_7 + \cdots)$ is even.

Example 2.1 From Proposition 2.3 every quadratic permutation polynomial modulo 2^n is of the form $ax^2 + bx + c$, where a is even, b is odd and c is an arbitrary constant in $\mathbb{Z}_8$.

Proposition 2.4 Let $f(x) = ax^2 + bx + c$ be a polynomial on $\mathbb{Z}_{2^n}$. Then $f(x)$ has a single cycle property if and only if one of the following is satisfied :

$$(i)\ \ a \equiv 2 \bmod 4,\ b \equiv 3 \bmod 4, \text{ and } c \equiv 1 \bmod 2$$
$$(ii)\ \ a \equiv 0 \bmod 4,\ b \equiv 1 \bmod 4, \text{ and } c \equiv 1 \bmod 2$$

Proof. The proof follows from [3]. □

Example 2.2 From Proposition 2.4 every quadratic permutation polynomial modulo 2^2 which has a single cycle property is of the form $2x^2 + 3x + c$ where c is either 1 or 3 in $\mathbb{Z}_4$.

Theorem 2.5 Let $f(x) = ax^2 + bx + c$ be a polynomial on $\mathbb{Z}_{2^n}$, $n > 1$. Suppose that one of following two conditions holds :

$$(i)\ \ a \equiv 2 \bmod 4,\ b \equiv 3 \bmod 4, \text{ and } c \equiv 1 \bmod 4$$
$$(ii)\ \ a \equiv 0 \bmod 4,\ b \equiv 1 \bmod 4, \text{ and } c \equiv 3 \bmod 4$$

Then $f(x) \not\equiv x + 1 \bmod 2^n$ for every $x \in \mathbb{Z}_{2^n}$ and so $f(x)$ is pseudo secure.

Proof. It follows from Proposition 2.4 that $f(x)$ has a single cycle property. If $a \equiv 2 \bmod 4$, $b \equiv 3 \bmod 4$ and $c \equiv 3 \bmod 4$, then $a = 4m + 2$, $b = 4s + 3$ and $c = 4l + 3$ for some integers m, s and l. Consider a congruence $f(x) \equiv x + 1 \bmod 2^n$. From this congruence we get

$$(4m + 2)x^2 + (4s + 2)x + 4l + 2 \equiv 0 \bmod 2^n$$

Note that $(4m + 2)x^2 + (4s + 2)x \equiv 4(mx^2 + sx) + 2x(x + 1) \equiv 0 \bmod 4$. Hence we get $(4m+2)x^2 + (4s+2)x + 4l + 2 \equiv 2 \bmod 4$. Thus for every positive integer $n \geq 2$, $(4m + 2)x^2 + (4s + 2)x + 4l + 2 \equiv 0 \bmod 2^n$ has no solutions. That is, $f(x) \not\equiv x + 1 \bmod 2^n$ for every $x \in \mathbb{Z}_{2^n}$.

If $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 4$ and $c \equiv 3 \bmod 4$, then $a = 4m$, $b = 4s + 1$ and $c = 4l + 3$ for some integers m, s and l. Similarly $f(x) \equiv x + 1 \bmod 2^n$ implies $4mx^2 + 4sx + 4l + 2 \equiv 0 \bmod 2^n$, which has no solutions for every positive integer $n \geq 2$. Hence $f(x) \not\equiv x + 1 \bmod 2^n$ for every $x \in \mathbb{Z}_{2^n}$. Therefore this theorem holds.

□

Example 2.3 From Theorem 2.5 all quadratic permutation polynomials modulo 2^n which are pseudo secure are

$$4mx^2 + (4l + 1)x + 4k + 3 \text{ and } (4s + 2)x^2 + (4t + 3)x + 4u + 3$$

where $m \neq 0, l, k, s, t$ and u are elements of $\mathbb{Z}_{2^n}$. In fact, let $f(x) \equiv 6x^2 + 3x + 7 \mod 2^9$. Then $f(x)$ has a cycle of period 2^9 and $f(x) \not\equiv x + 1 \mod 2^9$ for every $x \in \mathbb{Z}_{2^9}$. Hence $f(x)$ is pseudo secure. In this case there is only one value $a \in \mathbb{Z}_{2^9}$ such that $f(a) = a - 1$. That is, $f^{73}(1) = f(9) = 8$. Hence $f(x)$ is not secure.

Theorem 2.6 Let $f(x) = ax^2 + bx + c$ be a polynomial on $\mathbb{Z}_{2^n}$, $n > 1$. Suppose that one of following two conditions holds :

$$(i) \;\; a \equiv 2 \mod 4, \; b \equiv 3 \mod 4, \text{ and } c \equiv 1 \mod 4$$
$$(ii) \;\; a \equiv 0 \mod 4, \; b \equiv 1 \mod 4, \text{ and } c \equiv 1 \mod 4$$

Then $f(x) \not\equiv x - 1 \mod 2^n$ for every $x \in \mathbb{Z}_{2^n}$ and so $f(x)$ is pseudo secure.

Proof. It follows from Proposition 2.4 that $f(x)$ has a single cycle property. If $a \equiv 2 \mod 4$, $b \equiv 3 \mod 4$ and $c \equiv 3 \mod 4$, then $a = 4m + 2$, $b = 4s + 3$ and $c = 4l + 1$ for some integers m, s and l. Consider a congruence $f(x) \equiv x - 1 \mod 2^n$. From this congruence we get

$$(4m + 2)x^2 + (4s + 2)x + 4l + 2 \equiv 0 \mod 2^n$$

Note that $(4m+2)x^2 + (4s+2)x \equiv 4(mx^2 + sx) + 2x(x+1) \equiv 0 \mod 4$. Hence we get $(4m+2)x^2 + (4s+2)x + 4l + 2 \equiv 2 \mod 4$. But for every positive integer $n \geq 2$, $(4m + 2)x^2 + (4s + 2)x + 4l + 2 \equiv 0 \mod 2^n$ has no solutions. That is, $f(x) \not\equiv x - 1 \mod 2^n$ for every $x \in \mathbb{Z}_{2^n}$.
If $a \equiv 0 \mod 4$, $b \equiv 1 \mod 4$ and $c \equiv 1 \mod 4$, then $a = 4m$, $b = 4s + 1$ and $c = 4l + 1$ for some integers m, s and l. Similarly $f(x) \equiv x - 1 \mod 2^n$ implies $4mx^2 + 4sx + 4l + 2 \equiv 0 \mod 2^n$, which has no solutions for every positive integer $n \geq 2$. Hence $f(x) \not\equiv x - 1 \mod 2^n$ for every $x \in \mathbb{Z}_{2^n}$.
Therefore this theorem holds.

□

Example 2.4 From Theorem 2.6 all quadratic permutation polynomials modulo 2^n which are pseudo secure are

$$4mx^2 + (4l + 1)x + 4k + 1 \text{ and } (4s + 2)x^2 + (4t + 3)x + 4u + 1$$

where $m \neq 0, l, k, s, t$ and u are elements of $\mathbb{Z}_{2^n}$. In fact, let $f(x) \equiv 6x^2 + 3x + 5 \mod 2^9$. Then $f(x)$ has a cycle of period 2^9 and $f(x) \not\equiv x - 1 \mod 2^9$ for every $x \in \mathbb{Z}_{2^9}$. Hence $f(x)$ is pseudo secure. In this case there is only one value $a \in \mathbb{Z}_{2^9}$ such that $f(a) = a + 1$. That is, $f^{15}(1) = f(163) = 164$. Hence $f(x)$ is not secure.

Theorem 2.7 Every quadratic polynomial on $\mathbb{Z}_{2^n}$ has a single cycle property modulo 2^n if and only if it is pseudo secure.

Proof. Suppose that every quadratic polynomial on $\mathbb{Z}_{2^n}$ has a single cycle property modulo 2^n. Then it follows from Proposition 2.4 that one of the following is satisfied :

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

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

Hence by Theorem 2.5 and Theorem 2.6 it is pseudo secure.
The converse of this theorem clearly follows from the definition of a pseudo secure function.

□

Example 2.5 Let $f(x) \equiv 8x^2 + 9x + 3 \bmod 2^9$. From Theorem 2.5 $f(x)$ has a cycle of period 2^9 and $f(x) \not\equiv x + 1 \bmod 2^9$ for every $x \in \mathbb{Z}_{2^n}$. The table of values $f^i(1)$ for $i \in \mathbb{Z}_{2^9}$ is in Table 1. Hence $f(x)$ is pseudo secure. Let's consider $8x^2 + 9x + 3 \equiv x - 1 \bmod 2^9$. Then $8x^2 + 8x + 4 \equiv 0 \bmod 2^9$, which has no solution. That is, $f(x) \not\equiv x - 1 \bmod 2^9$ for every $x \in \mathbb{Z}_{2^9}$. Therefore $f(x)$ is secure on $x \in \mathbb{Z}_{2^n}$ and so $f(x)$ is secure on $x \in \mathbb{Z}_{2^n}$ for every integer $n(\geq 4)$.

Until now we give 3 concrete examples which is pseudo secure. These examples generate binary sequences of period 9×2^9. In particular the last example is secure. That is, for any given large number n the function $f(x) \equiv 8x^2 + 9x + 3 \bmod 2^n$ is secure and it generates a binary sequence of period $n \times 2^n$. Similarly we can construct many secure quadratic polynomial modulo 2^n if n is large enough. In fact, we have following theorem.

Theorem 2.8 Let $f(x) \equiv ax^2 + bx + c$ be a quadratic polynomial on $\mathbb{Z}_{2^n}$, where $n \geq 4$. Suppose that $a \equiv 4t \bmod 2^3$, $b \equiv 4t + 1 \bmod 2^3$ and $c \equiv 4t \pm 1 \bmod 2^3$, where $t = 0$ or $t = 1$. Then $f(x)$ is secure on $\mathbb{Z}_{2^n}$.

Proof. If $a \equiv 4t \bmod 2^3$, $b \equiv 4t+1 \bmod 2^3$ and $c \equiv 5 \bmod 2^3$, then $a = 4t+8m$, $b = 4t+8s+1$ and $c = 8l+5$ for some integers m, s and l. First, $a \equiv 0 \bmod 2^2$, $b \equiv 1 \bmod 2^2$ and $c \equiv 1 \bmod 2^2$. Hence by Theorem 2.6 $f(x) \not\equiv x - 1 \bmod 2^n$ for every $x \in \mathbb{Z}_{2^n}$. Next, note $4x(x+1)t \equiv 0 \bmod 8$ for every $x \in \mathbb{Z}_{2^n}$. Hence $(4t+8m)x^2 + (4t+8s+1)x + 8l + 5 \equiv x + 1 \bmod 2^n$ has no solutions since $(4t+8m)x^2 + (4t+8s)x + 8l + 4 \equiv 8(mx^2 + sx + l) + 4x(x+1)t + 4 \equiv 0 \bmod 2^n$ has no solutions. Hence $f(x) \not\equiv x + 1 \bmod 2^n$ for every $x \in \mathbb{Z}_{2^n}$. Thus $f(x)$ is secure on $\mathbb{Z}_{2^n}$.
If $a \equiv 4t \bmod 2^3$, $b \equiv 4t + 1 \bmod 2^3$ and $c \equiv 3 \bmod 2^3$, then $a = 4t + 8m$, $b = 4t+8s+1$ and $c = 8l+3$ for some integers m, s and l. First, $a \equiv 0 \bmod 2^2$, $b \equiv 1 \bmod 2^2$ and $c \equiv 3 \bmod 2^2$. Hence by Theorem 2.5 $f(x) \not\equiv x + 1 \bmod 2^n$ for every $x \in \mathbb{Z}_{2^n}$. Next, note $4x(x+1)t \equiv 0 \bmod 8$ for every $x \in \mathbb{Z}_{2^n}$. Hence $(4t+8m)x^2 + (4t+8s+1)x + 8l + 3 \equiv x - 1 \bmod 2^n$ has no solutions since $(4t+8m)x^2 + (4t+8s)x + 8l + 4 \equiv 8(mx^2 + sx + l) + 4x(x+1)t + 4 \equiv 0 \bmod 2^n$ has no solutions. Hence $f(x) \not\equiv x - 1 \bmod 2^n$ for every $x \in \mathbb{Z}_{2^n}$. Thus $f(x)$ is secure on $\mathbb{Z}_{2^n}$.

□

In this paper, we have shown Theorem 2.8 which can find secure quadratic polynomials on $\mathbb{Z}_{2^n}$. So by using such polynomials, we can get secure binary sequences which can be used in stream cipher.

References

1. A. Klimov and A. Shamir, *A New Class of Invertible Mappings*, Workshop on Cryptographic hardware and Embedded Systems (CHES), 2002.
2. R. A. Mollin, An Introduction to Cryptography, 2007.
3. M.S. Rhee, *On a characterization of T-functions with one cycle property*, J. of the Chungcheong M. S., Vol 21, No. 2, 259-268, 2008.
4. R. L. Rivest, *Permutation polynomials modulo* 2^ω, Finite Fields and Their Applications, 7, 287-292, 2001.
5. C. Romero and R. Kumanduri, Number theory with computer applications, 1998
6. R. P. Singh and S. Maity, *Permutation Polynomials modulo* $p2^n$,
7. D. R. Stinson, CRYPTOGRAPHY : Theory and Practice, 2002.
8. W. Trappe and L. C. Washington, Introduction to Cryptography with Coding Theory, 2002.

Min Surp Rhee received his BS from Seoul National University and Ph.D at University of Alabama(at Tuscaloosa, USA). He has been a professor at Dankook University since 1980. His research interests focus on Order Theory, Applied Algebras and Cryptography.

Department of Applied Mathematics, Dankook University, Cheonan-si, Choongnam, 330-714, Korea

e-mail: msrhee@dankook.ac.kr

TABLE 1. The values of $f^i(1)$, where $f(x) = 8x^2 + 9x + 3 \bmod 2^9$.

1	384	463	446	413	316	491	122	313	504	7	54	213	436
20	387	338	465	208	415	270	365	140	443	458	265	328	471
311	486	5	356	339	162	417	32	367	94	317	476	395	282
378	57	248	263	310	469	180	291	498	369	368	319	430	269
109	396	187	202	9	72	215	134	421	4	243	322	321	192
288	111	350	61	220	139	26	473	408	167	470	373	340	195
35	242	113	112	60	174	13	44	91	362	425	232	119	294
390	165	260	499	66	65	448	15	510	477	380	43	186	377
217	152	423	214	117	84	451	402	17	272	479	334	429	204
300	347	106	169	488	375	38	69	420	403	226	481	96	431
271	254	221	124	299	442	121	312	327	374	21	244	355	50
146	273	16	223	78	173	460	251	266	73	136	279	198	485
325	164	147	482	225	352	175	414	125	284	203	90	25	472
56	71	118	277	500	99	306	177	176	127	238	77	108	155
507	10	329	392	23	454	229	324	51	130	129	0	79	62
158	381	28	459	346	281	216	487	278	181	148	3	466	81
433	432	383	494	333	364	411	170	233	40	439	102	133	484
68	307	386	385	256	335	318	285	188	363	506	185	376	391
231	22	437	404	259	210	337	80	287	142	237	12	315	330
426	489	296	183	358	389	228	211	34	289	416	239	478	189
29	444	107	250	441	120	135	182	341	52	163	370	241	240
336	31	398	493	268	59	74	393	456	87	6	293	388	115
467	290	33	160	495	222	445	92	11	410	345	280	39	342
438	85	308	419	114	497	496	447	46	397	428	475	234	297
137	200	343	262	37	132	371	450	449	320	399	382	349	252
348	267	154	89	24	295	86	501	468	323	274	401	144	351
191	302	141	172	219	490	41	360	247	422	453	292	275	98
194	193	64	143	126	93	508	171	314	505	184	199	246	405
245	212	67	18	145	400	95	462	45	332	123	138	457	8
104	503	166	197	36	19	354	97	224	47	286	509	156	75
427	58	249	440	455	502	149	372	483	178	49	48	511	110
206	301	76	379	394	201	264	407	326	101	196	435	2	1
353	480	303	30	253	412	331	218	153	88	359	150	53	
116	227	434	305	304	255	366	205	236	283	42	105	424	
151	70	357	452	179	258	257	128	207	190	157	60	235	
474	409	344	103	406	309	276	131	82	209	464	159	14	
461	492	27	298	361	168	55	230	261	100	83	418	161	