2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)
August 28-29, 2018; Shahid Rajaee Teacher Training University - Tehran, Iran

Polynomials over $\mathbb{Z}_{2^n}$ and their applications in symmetric cryptography

S. M. Dehnavi
Kharazmi University
Faculty of Mathematical and Computer Sciences
Tehran, Iran
dehnavism@ipm.ir

M. R. Mirzaee Shamsabad
Shahid Beheshti University
Department of Mathematics
Tehran, Iran
m_mirzaee@sbu.ac.ir

Abstract— **Components which are constructed via the application of basic instructions of modern processors are common in symmetric ciphers targeting software applications; among them are polynomials over $\mathbb{Z}_{2^n}$, which fit n–bit processors. For instance, the AES finalist RC6 uses a quadratic polynomial over $\mathbb{Z}_{2^{32}}$. In this paper, after some mathematical examination, we give the explicit formula for the inverse of RC6-like polynomials over $\mathbb{Z}_{2^n}$ and propose some degree-one polynomials as well as some self-invertible (involutive) quadratic polynomials with better cryptographic properties, instead of them, for the use in modern software-oriented symmetric ciphers. Then, we provide a new nonlinear generator with provable period, which could be used in stream ciphers and pseudo-random number generators.**

Keywords- Polynomial over $\mathbb{Z}_{2^n}$; Self-invertible polynomial; Involution; RC6; Symmetric cryptography; Stream cipher; Pseudo-random number generator;

I. INTRODUCTION

Some designers of symmetric ciphers use components which are constructed by basic instructions of modern processors in the design of software-oriented ciphers. For example, the AES finalist block ciphers MARS [1] and Twofish [2] use multiplication and addition in $\mathbb{Z}_{2^{32}}$, and the eStream project stream ciphers Rabbit [3] and Sosemanuk [4] (selected for software profile) use multiplication in $\mathbb{Z}$ and $\mathbb{Z}_{2^{32}}$. Many lightweight ciphers are also use basic instructions; among them is the ARX-based block cipher SPECK [5].

Since polynomials over $\mathbb{Z}_{2^n}$ could be implemented by only the operations of addition and multiplication mod 2^n, which are built-in instructions of modern n–bit processors, so, low-degree polynomials are efficient over these processors. For instance, the AES finalist block cipher RC6 [6] utilizes a quadratic polynomial over $\mathbb{Z}_{2^{32}}$. One of the drawbacks of this polynomial is that it has a large set of fixed-points. In this paper, after some mathematical study, we present the explicit formula for the inverse of RC6-like polynomials in general and, we propose some degree-one polynomials along with some self-invertible or involutive quadratic polynomials with only two fixed-points, for the use instead of them, in design of modern software-oriented symmetric ciphers. With the aid of the proposed inverse for RC6-like polynomials, the presented degree-one polynomials whose inverses are acquired easily and the proposed self-invertible quadratic polynomials whose inverses are the same as themselves, the designers of symmetric ciphers could use these kinds of polynomials not only in Feistel schemes like the case of RC6, which do not need the inverse of components, but also in SPN structures.

Then, based on the mathematical investigation, we propose a new nonlinear generator with provable period. This nonlinear generator could be used in stream ciphers and pseudo-random number generators.

In Section II, we give preliminary notations and definitions. Section III is dedicated to theoretical aspects of the paper. In Sections IV we present some applications of the mathematical study and, Section V is the conclusion.

II. PRELIMINARY NOTATIONS AND DEFINITIONS

Throughout the paper k, m, n, r, s and t are natural numbers. We denote the ring of integers modulo 2^n by $\mathbb{Z}_{2^n}$, the addition in $\mathbb{Z}_{2^n}$ by $+$, the left shift operation by $\ll$ and the complement of $a \in \mathbb{Z}_{2^n}$ by $\bar{a}$. Note that $2^n - a = \bar{a} + 1$. The greatest t such that 2^t divides $a \in \mathbb{Z}_{2^n}$ is denoted by $\mathbf{p}_2(a)$, the unique inverse of an invertible element a in $\mathbb{Z}_{2^n}$ by $a^{-1} \ mod \ 2^n$, the Hamming weight of $a \in \mathbb{Z}_{2^n}$ by $\mathbf{wt}(a)$ and the n times composition of a bijection f by itself, by $f^{(n)}$. We denote the number of fixed-points of a bijection $f: A \to A$, i.e. the number of $x \in A$ such that $f(x) = x$, by Θ_f.

Let R be a (finite commutative) ring with identity and $r \in R$. If we have $r^m = 0$ for some m, then r is said to be nilpotent. We denote the least t such that $r^t = 0$ by $\mathcal{N}_r$.

A mapping

$$f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n},$$

978-1-5386-7582-3/18/$31.00 ©2018 IEEE

$$f(x) = \sum_{i=0}^{m} a_i x^i \mod 2^n,$$

is called a polynomial over $\mathbb{Z}_{2^n}$. When $m = 1$, we say that f is degree-one and when $m = 2$, we call f quadratic. Suppose that $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is a polynomial such that f is equal to its compositional inverse; in other words:

$$f^{(2)}(x) = x,$$

for any $x \in \mathbb{Z}_{2^n}$. In this case, we say that f is a self-invertible or involutive polynomial.

III. Theoretical Aspects

In this section, we lay a theoretical foundation for the applications which are presented in Section IV. Firstly, we give the explicit formula for the inverse of elements of the form $2^t - 1$ in $\mathbb{Z}_{2^n}$.

Theorem 1. The inverse of $2^t - 1$ modulo 2^n, is of the following form:

$$2^t - 2^{t\left\lfloor \frac{n}{t} \right\rfloor + 1} - 1 + \frac{2^{t+1}(2^{t-1} - 1)\left(2^{t\left(\left\lfloor \frac{n}{t} \right\rfloor - 1\right)} - 1\right)}{2^t - 1}.$$

Proof. Let $n = tk + r$, $0 \le r < t$. Since the inverse of odd numbers in $\mathbb{Z}_{2^n}$ is unique, it suffices to show that the multiplication of $2^t - 1$ by the presented inverse is equal to 1 modulo 2^n:

$$\begin{aligned}(2^t - 1)&\left(2^t - 2^{tk+1} - 1 + \frac{2^{t+1}(2^{t-1} - 1)\left(2^{t(k-1)} - 1\right)}{2^t - 1}\right)\\ &= 2^{2t} - 2^{t(k+1)+1} - 2^t - 2^t + 2^{tk+1} + 1\\ &\quad + 2^{t(k+1)} - 2^{2t} - 2^{kt+1} + 2^{t+1}\\ &= 1 \mod 2^n.\end{aligned}$$

Note that, since $t > r$, so

$$2^{t(k+1)+1} = 2^{t(k+1)} = 0 \mod 2^n. \qquad \blacksquare$$

We know that $\mathbf{wt}(2^t - 1) = t$. In the next theorem, we give the Hamming weight of the inverse of $2^t - 1$, modulo 2^n.

Theorem 2. Let $n = tk + r$, $0 \le r < t$, and

$$s = (2^t - 1)^{-1} \mod 2^n.$$

Then,

$$\mathbf{wt}(s) = \begin{cases} (t-1)(k-1) + t + r - 1 & r \ge 1, \\ (t-1)(k-1) + t & r = 0. \end{cases}$$

Proof. Regarding Theorem 1, s can also be written in the following form:

$$\begin{aligned}s &= 2^t - 2^{kt+1} - 1 + 2(2^{t-1} - 1)\sum_{i=1}^{k-1} 2^{it}\\ &= (2^t - 1) + (2^{t-1} - 1)\sum_{i=1}^{k-1} 2^{it+1} + (2^n - 2^{kt+1}).\end{aligned}$$

Since $\mathbf{wt}(2^t - 1) = t$, $\mathbf{wt}(2^{t-1} - 1) = t - 1$, and regarding the fact that there are no overlaps between blocks of 1 in the binary representation of s, so we have

$$\begin{aligned}\mathbf{wt}&\left((2^t - 1) + (2^{t-1} - 1)\sum_{i=1}^{k-1} 2^{it+1} + (2^n - 2^{kt+1})\right)\\ &= (t-1)(k-1) + t.\end{aligned}$$

Now, we should compute $\mathbf{wt}(2^n - 2^{kt+1})$, which is equal to 0 when $r = 0$ and to $r - 1$, otherwise. $\blacksquare$

Next, we give the explicit formula for the inverse of elements of the form $2^t + 1$ in $\mathbb{Z}_{2^n}$.

Theorem 3. The inverse of $2^t + 1$ modulo 2^n, is of the following form:

$$1 - 2^{t\left(2\left\lfloor \frac{n}{2t} \right\rfloor + 1\right)} + \frac{2^t\left(2^{2t\left\lfloor \frac{n}{2t} \right\rfloor} - 1\right)}{2^t + 1}.$$

Proof. Let $n = 2tk + r$, $0 \le r < 2t$. Similar to the proof of Theorem 1, we have

$$\begin{aligned}(2^t + 1)&\left(1 - 2^{t(2k+1)} + \frac{2^t(2^{2kt} - 1)}{2^t + 1}\right)\\ &= 2^t + 1 - 2^{2(k+1)t} - 2^{(2k+1)t} + 2^{(2k+1)t} - 2^t\\ &= 1 \mod 2^n.\end{aligned}$$

Again, note that

$$2^{2(k+1)t} = 0 \mod 2^n. \qquad \blacksquare$$

Now, we give the explicit formula for the inverses of 3,5 and 7 mod 2^n, which are used in Section IV, to obtain the explicit formula for the inverse of RC6-like polynomials in general.

Corollary 1. Regarding Theorem 1 and Theorem 3, we have

$$3^{-1} \mod 2^n = 3 - 2^{2\left\lfloor \frac{n}{2} \right\rfloor + 1} + \frac{8}{3}\left(2^{2\left(\left\lfloor \frac{n}{2} \right\rfloor - 1\right)} - 1\right),$$

$$5^{-1} \mod 2^n = 1 - 2^{2\left(2\left\lfloor \frac{n}{4} \right\rfloor + 1\right)} + \frac{4}{5}\left(2^{4\left\lfloor \frac{n}{4} \right\rfloor} - 1\right),$$

$$7^{-1} \mod 2^n = 7 - 2^{3\left\lfloor \frac{n}{3} \right\rfloor + 1} + \frac{48}{7}\left(2^{3\left(\left\lfloor \frac{n}{3} \right\rfloor - 1\right)} - 1\right).$$

Note that, there are $O(n)$ algorithms [7] for computing the inverse of odd elements in $\mathbb{Z}_{2^n}$; but Theorem 1, Theorem 3 and Corollary 1 give $O(1)$ algorithms for computing these inverses in some special cases.

We know that $\mathbf{wt}(2^t + 1) = 2$. In the following theorem, we give the Hamming weight of the inverse of $2^t + 1$, modulo 2^n.

Theorem 4. Let $n = 2tk + r$, $0 \le r < 2t$ and

$$s = (2^t + 1)^{-1} \mod 2^n.$$

Then,

$$\mathbf{wt}(s) = \begin{cases} kt + 1 & 0 \le r \le t, \\ (k-1)t + r + 1 & t < r < 2t. \end{cases}$$

Proof. Regarding Theorem 3, s can also be written in the following form:

$$s = 1 - 2^{(2k+1)t} - (2^t - 1)\sum_{i=0}^{k-1} 2^{(2i+1)t},$$

$$= 1 + 2^n - 2^{(2k+1)t} + (2^t - 1)\sum_{i=0}^{k-1} 2^{(2i+1)t}.$$

Again, since $\mathbf{wt}(2^t - 1) = t$, so,

$$\mathbf{wt}\left(1 + (2^t - 1)\sum_{i=0}^{k-1} 2^{(2i+1)t}\right) = kt + 1.$$

Therefore, we should verify $\mathbf{wt}\left(2^n - 2^{(2k+1)t}\right)$, which is equal to 0 when $0 \le r \le t$ and $r + 1$, otherwise. ■

The next lemma is used in Remark 1. Its proof is straightforward.

Lemma 1: Let R be a (finite commutative) ring with identity and $r \in R$ be nilpotent with $k = \mathcal{N}_r$. Then we have

$$(r-1)^{-1} = -1 - r - r^2 - \ldots - r^{k-1},$$

and

$$(r+1)^{-1} = \begin{cases} 1 - r + r^2 - r^3 + \ldots + r^{k-1} & k \text{ odd}, \\ 1 - r + r^2 - r^3 + \ldots - r^{k-1} & k \text{ even}. \end{cases}$$

Remark 1: In the mentioned four theorems, our approach was guessing the pattern of the inverses. Another (direct) proof of these theorems, which is based on Lemma 1, is as follows: Let $n = tk + r, \ 0 \le r < t$. Then, $k + 1 = \mathcal{N}_{2^t}$ in the ring $\mathbb{Z}_{2^n}$. So, by Lemma 1, modulo 2^n, we have

$$(2^t - 1)^{-1} = -1 - 2^t - 2^{2t} - \ldots - 2^{t(k-1)}$$

$$= 2^n - \left(1 + 2^t + 2^{2t} + \ldots + 2^{t(k-1)}\right)$$

$$= 1 + \overline{(1 + 2^t + 2^{2t} + \ldots + 2^{t(k-1)})}.$$

It is not hard to see that this accords with Theorem 1 and Theorem 2. On the other hand, by Lemma 1, in the case that k is odd, modulo 2^n, we have

$$(2^t + 1)^{-1} = 1 - 2^t + \ldots - 2^{t(k-1)}$$

$$= 2^n - \left(2^t - 1 + 2^{3t} - 2^{2t} + \ldots + 2^{t(k-1)} - 2^{t(k-2)}\right)$$

$$= 1 + \overline{\left(2^t - 1 + 2^{3t} - 2^{2t} + \cdots + 2^{t(k-1)} - 2^{t(k-2)}\right)},$$

and in the case that k is even, modulo 2^n, we have

$$(2^t + 1)^{-1} = 1 - 2^t + \ldots + 2^{t(k-3)} - 2^{t(k-2)} + 2^{t(k-1)}$$

$$= 2^n - \left(2^t - 1 + 2^{3t} - 2^{2t} + \ldots + 2^{t(k-2)} - 2^{t(k-3)} - 2^{t(k-1)}\right)$$

$$= 1 + \overline{(2^t - 1 + 2^{3t} - 2^{2t} + \ldots + 2^{t(k-2)} - 2^{t(k-3)} + 2^n - 2^{t(k-1)})}.$$

One can check that this coincides with Theorem 3 and Theorem 4. Proof of next theorem can be seen in [8].

Theorem 5. Suppose that $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ with

$$f(x) = ax^2 + bx \mod 2^n.$$

Then, the quadratic compositional inverse (one of the two quadratic compositional inverses) of f is the polynomial

$$g: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n},$$

$$g(x) = cx^2 + dx \mod 2^n,$$

where

$$c = -a(b+a)^{-1}(b+2a)^{-1}(b+3a)^{-1} \mod 2^n,$$

$$d = (b+a)^{-1} - c(b+a) \mod 2^n.$$

In Section IV, we use Corollary 1 and Theorem 5 to present the explicit formula for the inverse of RC6-like polynomials, in general.

Now, we present all the degree-one self-invertible polynomials over $\mathbb{Z}_{2^n}$.

Theorem 6. All the $3.2^{n-1} + 2$ degree one self-invertible polynomials over $\mathbb{Z}_{2^n}$ are as follows

a) $f(x) = x + 2^{n-1} \mod 2^n$,

b) $f(x) = (2^{n-1} - 1)x + v \mod 2^n, \ v \text{ even}$,

c) $f(x) = (2^{n-1} + 1)x \mod 2^n$,

d) $f(x) = -x + w \mod 2^n, \ w \in \mathbb{Z}_{2^n}$.

Proof. Consider the equation $f^{(2)}(x) = x \mod 2^n$, or

$$(a^2 - 1)x + b(a+1) = 0 \mod 2^n.$$

Evaluating the equation on the points 0 and 1, we have

$$a^2 = 1 \mod 2^n,$$

$$b(a+1) = 0 \mod 2^n.$$

Now, regarding Theorem 1 in [9], the four cases are acquired. Note that Case ***b*** has 2^{n-1} and Case ***d*** has 2^n functions. ■

The following theorem is from [10]. Note that we only give two of the five cases, for brevity.

Theorem 7. Let $n \ge 6$. Then the following polynomials over $\mathbb{Z}_{2^n}$ are self-invertible:

- $f(x) = -x + 2^r v x^2 \mod 2^n, \ r \ge \frac{n-1}{2}, \ v \text{ odd}$,
- $f(x) = (1 + 2^{n-2}w)x + 2^{n-1}vx^2 \mod 2^n, \ w, v \text{ odd}$.

The next lemma presents the number of fixed points of some special degree-one polynomials over $\mathbb{Z}_{2^n}$.

Lemma 2. Let $c \in \mathbb{Z}_{2^n}$ be odd and

$$f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n},$$

$$f(x) = cx \mod 2^n.$$

Then the number of fixed-points of f is $\Theta_f = 2^{\mathbf{p}_2(c-1)}$.

Proof. Let $s = \mathbf{p}_2(c-1)$. We must count the number of $x \in \mathbb{Z}_{2^n}$ such that

$$(c-1)x = 0 \mod 2^n.$$

For $x \in \mathbb{Z}_{2^n}$, suppose that $\mathbf{p}_2(x) = t$. Then $cx = 0 \mod 2^n$ iff $t \geq n - \mathbf{p}_2(c-1)$; and since the number $x \in \mathbb{Z}_{2^n}$ with $\mathbf{p}_2(x) = r$ is 2^{n-r}, so we have

$$\Theta_f - 1 = \sum_{i=n-s}^{n-1} 2^{n-i} = \sum_{i=0}^{s-1} 2^i = 2^s - 1,$$

and since 0 is also a fixed-point of f, so the lemma is proved. ■

Corollary ۲. The number of fixed-points of the mappings $x \mapsto (2^t+1)x \mod 2^n$ and $x \mapsto (2^t-1)x \mod 2^n$, from $\mathbb{Z}_{2^n}$ to itself is 2^t and 2, respectively.

The next lemma is used in Section IV, to construct a new nonlinear generator.

Lemma 3. Let

$$f(x) = (2^t+1)x + 1 \mod 2^n, \quad \frac{n}{2} < t < n.$$

Then,

$$f^{(m)}(x) = (m2^t+1)x + m + 2^{t-1}(m^2-m), \quad m \geq 1.$$

Proof. Firstly, suppose that

$$f(x) = ax + b \mod 2^n.$$

One can check that

$$f^{(m)}(x) = a^m x + b\left(\frac{a^m - 1}{a-1}\right) \mod 2^n.$$

Now, since

$$(2^t+1)^m = \sum_{i=0}^{m} \binom{m}{i} 2^{it} = 1 + m2^t + \frac{m(m-1)}{2}2^{2t} + \cdots + 2^{mt};$$

$$\frac{m(m-1)}{2}2^{2t} + \cdots + 2^{mt} = 0 \mod 2^n;$$

and

$$\frac{\binom{m}{3}2^{3t} + \cdots + 2^{mt}}{2^t} = 0 \mod 2^n,$$

so we have

$$f^{(m)}(x) = (m2^t+1)x + m + 2^{t-1}(m^2-m) \mod 2^n. \quad ■$$

IV. Applications

In this section, based upon the theoretical investigations of the previous section, we present the explicit formula for inverse of RC6-like polynomials in general and propose some degree-one as well as some self-invertible quadratic polynomials for usage in symmetric cryptography. Then, we present a new nonlinear generator with provable period, that could be used in stream ciphers and pseudo-random number generators.

Consider the general form of RC6 quadratic polynomial:

$$f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n},$$

$$f(x) = x(2x+1) \mod 2^n.$$

By Theorem 5, the (compositional) inverse of f is

$$g: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n},$$

$$g(x) = cx^2 + dx \mod 2^n,$$

with

$$c = -2.3^{-1}5^{-1}7^{-1} \mod 2^n,$$

$$d = 3^{-1} - 3c \mod 2^n.$$

Note that the closed formula for 3^{-1}, 5^{-1} and 7^{-1} is given in Corollary 1.

Example 1. Let

$$f: \mathbb{Z}_{2^4} \to \mathbb{Z}_{2^4},$$

$$f(x) = x(2x+1) \mod 2^4.$$

Then, by the above discussion, the compositional inverse of f is

$$g: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n},$$

$$g(x) = 14x^2 + x \mod 2^n.$$

In the next example, we consider the very quadratic polynomial of the block cipher RC6 and compute its compositional inverse.

Example 2. Consider

$$f: \mathbb{Z}_{2^{32}} \to \mathbb{Z}_{2^{32}},$$

$$f(x) = x(2x+1) \mod 2^{32}.$$

By Corollary 1, we have

$$3^{-1} \mod 2^{32} = 3 - 2^{32+1} + \frac{8}{3}(2^{30}-1) = 2863311531,$$

$$5^{-1} \mod 2^n = 1 - 2^{34} + \frac{4}{5}(2^{32}-1) = 3435973837,$$

$$7^{-1} \mod 2^n = 7 - 2^{31} + \frac{48}{7}(2^{27}-1) = 3067833783.$$

Now, notations as above, we have

$$c = -2.3^{-1}5^{-1}7^{-1} \mod 2^{32} = 1308942414,$$

and

$$d = 3^{-1} - 3c \mod 2^{32} = 3231451585.$$

So, the inverse of the quadratic polynomial of RC6 is

$$g: \mathbb{Z}_{2^{32}} \to \mathbb{Z}_{2^{32}},$$

$$g(x) = 1308942414x^2 + 3231451585x \mod 2^{32}.$$

We consider three properties for comparing polynomials, from the cryptographic viewpoint:

1) The number of fixed-points.
2) The implementation cost of polynomials and their inverses.
3) Whether they are involutions, or not.

It is well-known that the number of fixed-points of RC6-like polynomials is

$$2^{n-\left\lceil\frac{n-1}{2}\right\rceil},$$

which is a drawback, from the cryptographic viewpoint, and obviously, these polynomials are not involutions. On the other hand, in modern processors, RC6-like polynomials are efficient. Note that, the inverses of these polynomials, which are given in the present paper, are also efficient in modern processors; so, we could use these polynomials not only in Feistel schemes, where we do not need the inverse of mappings, but also in SPN structures.

The degree-one polynomials

- $f(x) = 3x \mod 2^n$,
- $f(x) = 7x \mod 2^n$,

have two fixed-points, by Corollary 2, and clearly are not involutive. The explicit formula for inverse of these degree-one polynomials, could be acquired based on Corollary 1. Not that, we have

$$(2^t + 1)x = (x \ll t) + x,$$
$$(2^t - 1)x = (x \ll t) - x.$$

Therefore, the implementation cost of these kinds of polynomials is very low, even in low-end processors, in which the multiplication operation has a high cost. By Theorem 2 and Theorem 4, in the mentioned low-cost processors, the implementation cost of the inverse of these polynomials is high; but, all in all, in most of modern processors, the implementation cost of these degree-one polynomials and their inverses is very low.

Self-invertible polynomials of the form $f(x) = -x + 2^r x^2$ in Theorem 7 (put $v = 1$) have only two fixed-points [9] and are involutions; so, the implementation cost of these polynomials and their inverses is equal, and since we have

$$f(x) = -x + (x^2 \ll r) \mod 2^n,$$

so, these involutive polynomials have a suitable implementation cost in modern processors.

Remark 2: We propose the degree-one polynomials

$$f(x) = 3x = x + (x \ll 1) \mod 2^n,$$
$$f(x) = 7x = x + (x \ll 1) + (x \ll 2) \mod 2^n,$$

or the involutive quadratic polynomials

$$f(x) = -x + (x^2 \ll r) \mod 2^n,$$

instead of RC6-like polynomials, for the use in modern processors, because of the fact that they have only two fixed-points and the implementation cost of them (and their inverses) is low.

Remark 3: We believe that the self-invertible polynomials presented in Theorem 7:

$$f(x) = (1 + 2^{n-2}w)x + 2^{n-1}vx^2 \mod 2^n, \qquad w, v \text{ odd}.$$

are not good candidates for the use in cryptography, because they have a large set of fixed-points [9]. Also, we think that the degree-one self-invertible polynomials should be used wittingly. For example, the polynomial

$$f(x) = x + 2^{n-1} \mod 2^n,$$

is a (bitwise) linear mapping and only flips the most significant bit of the input. On the other hand, since

$$(2^{n-1} - 1)x + v = \big(x \ll (n-1)\big) + v - x,$$

and

$$(2^{n-1} + 1)x = \big(x \ll (n-1)\big) + x,$$

so, there is no effective multiplication (or good mixing, similar to case of *3x* and *7x*) in any of these degree-on self-invertible polynomials. It seems that the quadratic self-invertible polynomials are better candidates for the use in symmetric ciphers.

In the sequel, we present a nonlinear generator, based upon Lemma 3. Suppose that $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is a single-cycle T-function [11], and for an initial value

$$s_0 = (s_{0,n-1},.., s_{0,0}),$$

let

$$s_i = f^{(i)}(s_0) = (s_{i,n-1},.., s_{i,0}), \qquad 0 < i < 2^n.$$

It is well-known that the period of $\{s_i\}_{i\geq 0}$ is 2^n and for a fixed $0 \leq j < n$, the period of $\{s_{i,j}\}_{i\geq 0}$ is 2^{j+1}. For example, the period of the output slice corresponding to the least significant bit is 2. So, the cryptographic properties of the lower bits of the generated sequence by means of this single-cycle T-function is not good.

We know that maximal-length LFSRs [12] have good statistical properties, but are linear. Consider a maximal-length LFSR. We denote its action on the *n*–bit value X by $L(X)$. For an initial value

$$s_0 = (s_{0,n-1},.., s_{0,0}),$$

let

$$s_i = L^{(i)}(s_0) = (s_{i,n-1},.., s_{i,0}), \qquad 0 < i < 2^n - 1.$$

It is well-known that the period of $\{s_i\}_{i\geq 0}$ is $2^n - 1$ and for a fixed $0 \leq j < n$, the period of $\{s_{i,j}\}_{i\geq 0}$ is also $2^n - 1$.

Here, with the aid of Lemma 3 and based on the above discussion, we propose a nonlinear generator based on T-functions and maximal-length binary LFSRs. The pseudo-code of the proposed generator is given in Algorithm 1.

Algorithm 1

Input:

A non-zero n-bit initial state $I \neq (0, \dots, 0)$;

a maximal-length LFSR (whose action on the input X we denote by $L(X)$);

and $\frac{n}{2} < t < n$.

Output:

A sequence of n-bit words with period $2^n - 1$.

Begin

$S = I$

For $i = 1$ to $2^n - 1$

Output $S + \left((S^2 - S) \ll (t-1)\right) \bmod 2^n$

$S = L(S)$

End (For)

End (Algorithm)

Now, we show that the period of the output sequence of Algorithm 1 is $2^n - 1$: Consider a single-cycle T-function $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ and a maximal-length LFSR whose action on input X we denote by $L(X)$. Fix a nonzero element $I \in \mathbb{Z}_{2^n}$. Also, fix an arbitrary element $C \in \mathbb{Z}_{2^n}$ and let

$$s_i = f^{\left(L^{(i)}(I)\right)}(C), \quad 0 < i < 2^n - 1.$$

Since we have

$$\left\{I, L(I), L^{(2)}(I), \dots, L^{(2^n-2)}(I)\right\} = \mathbb{Z}_{2^n} \backslash \{0\},$$

and

$$\left\{f^{(L(I))}(C), f^{\left(L^{(2)}(I)\right)}(C), \dots, f^{\left(L^{(2^n-2)}(I)\right)}(C)\right\} = \mathbb{Z}_{2^n} \backslash \{C\},$$

So, the period of $\{s_i\}_{i \geq 0}$ is $2^n - 1$. Although, we could not prove a least period for $\{s_{i,j}\}_{i \geq 0}$ for a fixed $0 \leq j < n$, but, intuitively and experimentally, it can be seen that the period of the mentioned bit-slices of the output of Algorithm 1 is high. On the other hand, knowing the output of Algorithm 1, there is no simple way to acquire the previous state of the proposed generator. Compare this, to the case of LFSRs or T-functions; in both cases, there are efficient algorithms to obtain the previous state of the generator. Note that in Algorithm 1, we have chosen the T-function presented in Lemma 3 and put $C = 0$.

V. CONCLUSION

In this paper, firstly we investigate polynomials over $\mathbb{Z}_{2^n}$ mathematically and based upon this study, we present the explicit formula for the inverse of RC6-like quadratic polynomials over $\mathbb{Z}_{2^n}$. Also, we propose some degree-one along with some self-invertible quadratic polynomials with better cryptographic properties for the use as a replacement of them in modern symmetric ciphers targeting software-oriented applications. Then, we provide a new nonlinear generator with provable least period for usage in stream ciphers or pseudo-random number generators.

We believe that the proposed components of this paper could be used in designing software-oriented symmetric ciphers. The use of these components in block ciphers, stream ciphers, hash functions, pseudo-random number generators and authenticated encryption schemes could be a good line of research in continuation of the studies of this paper.

REFERENCES

[1] E. C. Burwick, D. Coppersmith, E. D'Avingnon, R. Gennaro, Sh. Halevi, Ch. Julta, S. M. Matyas. Jr, L. O'Connor, M. Peyravian, D. Safford, and N. Zunnic, "MARS a Candidate Cipher for AES ," Proceeding of 1st Advanced Encryption Standard Candidate Conference, Venture, California, Aug. 20-22 1998.

[2] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C.Hall, and N. Ferguson, "Twofish: A 128-Bit Block cipher," 1998, Available via http://www.counterpane.com/twofish.html.

[3] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius, "Rabbit: A New High-Performance Stream Cipher", FSE'03, LNCS 2887, pp. 307-329, Springer-Verlag, 2003.

[4] C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert, "Sosemanuk, a Fast Software-Oriented Stream Cipher", submitted to Ecrypt, 2005.

[5] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "SIMON and SPECK: Block Ciphers for the Internet of Things." IACR Cryptology ePrint Archive 2015: 585 (2015)

[6] R. L. Rivest, M. J. B. Robshaw, and R. Sidney, "The RC6 Block Cipher," Proceeding of 1st Advanced Encryption Standard Candidate Conference, Venture, California, Aug. 20-22 1998.

[7] A. J. Menezes, P. C. van Oorschot, and S.A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997

[8] J. Ryu, and O. Y. Takeshita, "On Quadratic Inverses for Quadratic Permutation Polynomials over Integer Rings", CoRR abs/cs/0511060 (2005)

[9] S. M. Dehnavi, M. R. M. Shamsabad, A. M. Rishakani, "Complete solving the quadratic equation mod 2^n", arXiv:1711.03621, available at https://arxiv.org/abs/1711.03621

[10] J. Diaz-Vargas, C. J. Rubio-Barrios, J. A. Sozaya-Chan, and H. Tapia-Recillas, "Self-Invertible Quadratic (Cubic) Permutation Polynomials over $\mathbb{Z}_{2^n}$ ($\mathbb{Z}_{p^n}$, $p > 7$), Int. J. Algebra, Vol. 6, 2012, no. 17, 863-874.

[11] A. Klimov, "Applications Of T-functions In Cryptography," Weizman Institute of Science, Ph.D Thesis, Department of Applied Mathematics and Computer Science, March 2005.

[12] M. Goresky, A, Klapper, "Algebraic Shift Register Sequences", *Cambridge University Press*, 2012