Permutation Polynomials and Their Differential Properties over Residue Class Rings

Yuyin Yu[a,b], Mingsheng Wang [a,b,*]

[a] *The State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, PO Box 8718, China*
[b] *Graduate School of Chinese Academy of Sciences, Beijing 100049, China*

Abstract

This paper mainly focuses on permutation polynomials over the residue class ring $\mathbb{Z}_N$, where $N > 3$ is composite. We have proved that for the polynomial $f(x) = a_1x^1 + \cdots + a_kx^k$ with integral coefficients, $f(x) \bmod N$ permutes $\mathbb{Z}_N$ if and only if $f(x) \bmod N$ permutes S_μ for all $\mu \mid N$, where $S_\mu = \{0 < t < N : \gcd(N,t) = \mu\}$ and $S_N = S_0 = \{0\}$. Based on it, we give a lower bound of the differential uniformities for such permutation polynomials, that is, $\delta(f) \geq \frac{N}{\#S_a}$, where a is the biggest nontrivial divisor of N. Especially, $f(x)$ can not be APN permutations over the residue class ring $\mathbb{Z}_N$. It is also proved that $f(x) \bmod N$ and $(f(x) + x) \bmod N$ can not permute $\mathbb{Z}_N$ at the same time when N is even.

Keywords: permutation polynomial, residue class ring, Almost Perfect Nonlinear (APN)
2000 MSC: 11C08, 13F20, 13B25, 94A60

1. Introduction

Permutation functions with low differential uniformity are used in cryptography, especially in the design of S-boxes. An important condition on these function is that they can provide balance and high resistance to differential analysis. The functions with the lowest differential uniformity oppose

*Corresponding author
Email addresses: yuyuyin@163.com (Yuyin Yu), mingsheng_wang@yahoo.com.cn (Mingsheng Wang)

an optimal resistance to differential attack. They are called almost perfect nonlinear (APN).

Mainstream cryptographic algorithms are designed on the finite field $\mathbb{F}_{2^n}$ for some even n, but it is rather difficult to find APN permutations on $\mathbb{F}_{2^n}$ when n is even. Up to now, only on $\mathbb{F}_{2^6}$ has Dillon [6] found an APN permutation. So, many cryptographic algorithms have to choose differential 4-uniform permutations as their S-boxes.

Considering the above situation, it is a natural generalization to study the functions over the residue class rings. As a matter of fact, related results have been employed in cryptography for a long time. For example, the SAFER family of cryptosystem, proposed by Massey [13] used APN functions from $\mathbb{Z}_{256}$ to itself. The block cipher RC6 [20] employed the permutation function $x(2x+1)$ over $\mathbb{Z}_{2^{32}}$, and quickly Rivest [19] gave a general rule to describe the permutation properties over $\mathbb{Z}_{2^n}$ ($n \geq 1$ is an integer). Drakakis [5] also investigated APN permutations over $\mathbb{Z}_n$ ($n \geq 4$ is an integer). Therefore, our main topic in this paper is to study the polynomial functions over the residue class rings, and we give a necessary and sufficient condition to decide when the polynomial functions are permutations. Some cryptography related properties, such as differential uniformity and orthomorphic permutation are also investigated.

In the following part of this section we shall give a short survey about the history of polynomial functions over the residue class rings.

Kempner [11] provided an extensive and detailed account of that subclass of the m^m functions on the ring $\mathbb{Z}_m$ to itself whose members can be expressed as polynomials. Mullen and Stevens [15] studied this subject and gave a simpler and more explicit formula. Carlitz [1], Keller and Olson [10], Singmaster [21] also discussed related questions. All the work focused on polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. Chen [2] generalized the former results and obtained the following theorem.

Theorem 1. *Let f be a polynomial function from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. Then f can be uniquely represented by a polynomial*

$$F = \sum_{k=0}^{\mu-1} a_k x^k \text{ with } 0 \leq a_k < \frac{m}{\gcd(m, k!)},$$

where $\mu = min\{n, \lambda(m)\}$ and $\lambda(m) =$ the least positive integer λ such that $m \mid \lambda!$.

In this paper, we only consider the situation when $n = m$. From Theorem 1 we can deduce that only a very small part of functions over $\mathbb{Z}_n$ can be denoted by polynomials.

Rivest [19] made a survey about the permutation polynomials modulo 2^w and obtained the following results.

Theorem 2. *The polynomial $P(x) = a_0 + a_1x + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo $2^w (w \geq 2)$ 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.*

We shall investigate a generalized case in this paper. It is organized as follows. In Sec. 2, we will introduce some preliminaries needed in the following. Let $N > 3$ be composite, and $f(x) = a_1x^1 + \cdots + a_kx^k$ be an polynomial with integral coefficients. In Sec. 3.1, we will give a necessary and sufficient condition to decide when the function $f(x)$ modulo N is a permutation over $\mathbb{Z}_N$. This result is different from the known ones. In Sec. 3.2, the orthomorphic permutation will be studied, and it is proved that there are no orthomorphic permutation polynomials over the residue class ring $\mathbb{Z}_N$ when $N > 3$ is even. In Sec. 3.3, the differential properties of the polynomial functions over the residue class rings will be investigated, and the lower bound is given in Theorem 6, which shows that an overwhelming majority polynomial functions modulo N have very bad differential properties. In Sec. 4, we will introduce other forms of APN permutations over the residue class rings. In addition, we also give an open problem in this section.

2. Preliminaries

In this section, we will introduce some basic concepts needed in this paper. Define $\mathbb{Z}_N = \{0, 1, 2, \cdots, N-1\}$. Let's recall the following definition related to the resistance to differential cryptanalysis [17].

Definition 1. Let $F(x)$ be a polynomial with integral coefficients. For any $a, b \in \mathbb{Z}_N$, we denote

$$\Delta_F(a, b) = \{x \in \mathbb{Z}_N : (F((x + a) \bmod N) - F(x)) \bmod N = b\}.$$

$$\delta_F(a, b) = \#\Delta_F(a, b),$$

where $\#E$ is the cardinality of the set E. Then, we have

$$\delta(F) = max_{a \neq 0,\, b \in \mathbb{Z}_N} \delta_F(a, b).$$

We can say that F is differential $\delta(F)$-uniform over $\mathbb{Z}_N$, and the function for which $\delta(F) = 2$ is almost perfect nonlinear (APN) over $\mathbb{Z}_N$.

Remark 1. The main topic of this paper is to study the issue when $F(x)$ is a permutation polynomial over $\mathbb{Z}_N$. Suppose $F(x)$ is a permutation polynomial, then $(F((x+a) \bmod N) - F(x)) \bmod N \neq 0$ when $a \neq 0$, and thus there must exist some $b \in \mathbb{Z}_N$ such that $(F((x+a) \bmod N) - F(x)) \bmod N = b$ has more than two solutions, which implies that $\delta_F(a,b) \geq 2$. It might be $\delta_F = 1$ when $F(x)$ is neither a polynomial nor a permutation, but we don't consider it in this paper.

The following notations are also used in this paper.

Definition 2. (1) N is composite and $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where p_i are different primes (Suppose $p_1 < p_2 < \cdots < p_n$) and $\alpha_i \geq 1$ for all $1 \leq i \leq n$. Let $M = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.
(2) $d \mid N$ means d is a divisor of N. $d \parallel N$ means: ① $d \mid N$ and $d < N$; ② if $d \mid c$ and $c \mid N$, then $c = d$ or N.
(3) Define $L_0 = \{0\}$, $L_1 = \{d_1 : d_1 \parallel N\}$, $L_i = \{d_i :$ There exists some $d_{i-1} \in L_{i-1}$ such that $d_i \parallel d_{i-1}\}$ $(1 < i \leq M)$. Note that $L_i = \{p_1^{\alpha_1'} p_2^{\alpha_2'} \cdots p_n^{\alpha_n'} : \alpha_1' + \alpha_2' + \cdots \alpha_n' = M - i$ and $\alpha_j' \geq 0$ for all $0 < j \leq n\}$.
(4) $S_\mu = \{0 < t < N : \gcd(N,t) = \mu\}$, especially, we define $S_N = S_0 = \{0\}$.
(5) We use $f_N(x)$ to denote $f(x) \bmod N$ in the following.

Given the above notations, it is easy to get the following lemma.

Lemma 1. *(1)* $\mathbb{Z}_N = \bigcup_{\mu \mid N} S_\mu$. *If* $\mu \neq \nu$, *then* $S_\mu \cap S_\nu = \emptyset$, *that is, the sets* $S_\mu (\mu \mid N)$ *partition* $\mathbb{Z}_N$.
(2) The sets $L_j\, (0 \leq j \leq M)$ *partition the set of the divisors of* N *(We identify* 0 *with* N*).*
(3) $L_M = \{1\}$.

Since the above results can be easily deduced, we omit the proof here.

3. Permutation Polynomials over $\mathbb{Z}_N$

For convenience and clarity, all the notations used in this section have the same meanings as in Definition 2.

3.1. Basic Properties

In this subsection, we will give a necessary and sufficient condition to decide when the polynomial functions are permutations over the residue class rings.

Theorem 3. *Let $f(x) = a_1x^1 + \cdots + a_kx^k$ be a polynomial with integral coefficients, and N is composite. Then $f_N(x)$ permutes $\mathbb{Z}_N$ if and only if $f_N(x)$ permutes S_μ for all $\mu \mid N$.*

PROOF. $\Leftarrow$ According to Lemma 1, the sets $S_\mu\,(\mu \mid N)$ partition $\mathbb{Z}_N$, so if $f_N(x)$ permutes S_μ for all $\mu \mid N$, it is easy to conclude that $f_N(x)$ permutes $\mathbb{Z}_N$.
$\Rightarrow$ Suppose $f_N(x)$ permutes $\mathbb{Z}_N$, then we need to prove that $f_N(x)$ permutes S_μ for all $\mu \mid N$. Using inductive method, we divide the proving process into three steps:

Step 1: When $\mu \in L_0$, we have $f(\mu) = f(0) = 0$. Thus $f_N(x)$ permutes $S_\mu = S_0$, that is, $f_N(x)$ permutes S_μ when $\mu \in L_0$. This step is the premise of our inductive method.

Step 2: Suppose $f_N(x)$ permutes S_μ when $\mu \in L_j$ and $0 \le j < i\,(0 < i \le M)$.

Step 3: We continue to consider the case when $\mu \in L_i$. If we can prove that $f_N(x)$ permutes S_μ when $\mu \in L_i$, then the whole theorem follows.

Choosing $\gamma \in S_\mu$, that is, $\gcd(\gamma, N) = \mu$, together with the premise $f(0) = 0$ we can get $\mu \mid \gcd(f(\gamma), N)$, which implies $\mu \mid \gcd(f_N(\gamma), N)$. Suppose $\gcd(f_N(\gamma), N) = \mu t$, i.e. $f_N(\gamma) \in S_{\mu t}$. If $t \neq 1$, then there must exist some $0 \le d < i$ such that $\mu t \in L_d$. According to Step 2, we can know that $f_N(x)$ permutes $S_{\mu t}$. Then if $f_N(\gamma) \in S_{\mu t}$, there must be some $\nu \in S_{\mu t}$ such that $f_N(x) = \nu$ has at least two different solutions, and this result is a contradiction with the premise that $f_N(x)$ permutes $\mathbb{Z}_N$.

From the above discussion, we can conclude that $t = 1$, and thus $f_N(\gamma) \in S_\mu$, which implies that $f_N(x)$ permutes S_μ when $\mu \in L_i$. □

In the following, we will give an example to illustrate this theorem.

Example 1. *Let $N = 2^2 3^2$ (See Fig. 1), then $M = 2 + 2 = 4$, $L_0 = \{0\}$, $L_1 = \{2^{\alpha_1'}3^{\alpha_2'} : \alpha_1' + \alpha_2' = M - 1 = 3\} = \{2^2 3^1, 2^1 3^2\} = \{12, 18\}$, $L_2 = \{2^2, 2^1 3^1, 3^2\} = \{4, 6, 9\}$, $L_3 = \{2, 3\}$, $L_4 = \{1\}$. $S_0 = \{0\}$, $S_{12} = \{0 < t < 36 : \gcd(36, t) = 12\} = \{12, 24\}$, $S_{18} = \{0 < t < 36 : \gcd(36, t) = 18\} =$*

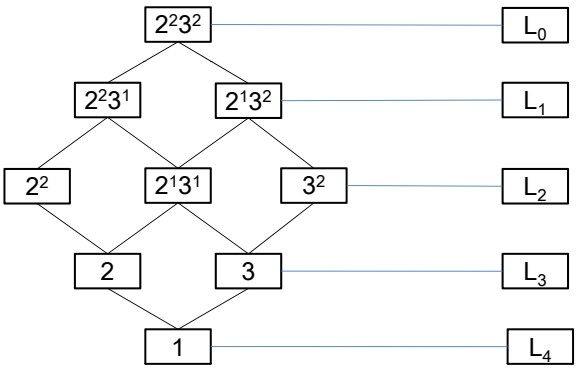

Figure 1: When $N = 36$

$\{18\}$, *similarly we can define* S_4, S_6, S_9, S_2, S_3, *and* S_1, *omitting them here. Let* $f(x) = a_1x^1 + \cdots + a_kx^k$ *be an polynomial with integral coefficients. We want to prove that* $f_{36}(x)$ *permutes* $\mathbb{Z}_{36}$ *if and only if* $f_{36}(x)$ *permutes* S_μ *for all* $\mu \mid 36$. *Since the sufficient condition is trivial, we only show how to prove the necessary condition here. Suppose* $f_{36}(x)$ *permutes* $\mathbb{Z}_{36}$. *Firstly,* $f(0) = 0$, *which implies that* $f_{36}(x)$ *permutes* S_μ *when* $\mu \in L_0$, *and we continue to consider the case when* $\mu \in L_1$. *Without loss of generality, let* $\mu = 12$. *Choosing* $\gamma \in S_{12}$, *then* $12 \mid f(\gamma)$, *which implies that* $12 \mid \gcd(f_{36}(\gamma), 36)$, *then we can conclude that* $f_{36}(\gamma) \in S_{12} \cup S_0$. *But* $f_{36}(\gamma)$ *can not be in* S_0, *otherwise it will contradict with the fact that* $f_{36}(x)$ *permutes* $\mathbb{Z}_{36}$, *so we have* $f_{36}(\gamma) \in S_{12}$, *which implies that* $f_{36}(x)$ *permutes* S_{12}. *Similarly we can prove that* $f_{36}(x)$ *permutes* S_{18}. *From the above discussion, we conclude that* $f_{36}(x)$ *permutes* S_μ *when* $\mu \in S_1$. *Using inductive method we can prove the whole theorem.*

Theorem 3 seems to be a very strict restriction on permutation polynomials over the residue class rings, but when we notice Theorem 1 we can deduce that there are only precious few functions over the residue class rings can be denoted by polynomials. Together with the former results we can have a more clear understanding about the polynomial functions over the residue class rings.

There are other results about the permutation polynomials over the residue class rings.

Theorem 4. *[22] For any $N = \prod_{i=1}^{m} p_i^{n_i}$, where p_i are distinct prime numbers, $P(x)$ is a permutation polynomial modulo N if and only if $P(x)$ is also a permutation polynomial modulo $p_i^{n_i}$ for all $1 \leq i \leq m$.*

As for the case $N = p^n$, there exists the following results.

Theorem 5. *[22] $P(x)$ is a permutation polynomial over the residue class ring $\mathbb{Z}_{p^n} (n > 1)$ if and only if $P(x)$ is a permutation polynomial over $\mathbb{Z}_p$ and $P'(x) \bmod p \neq 0$ for all integers $x \in \mathbb{Z}_{p^n}$.*

This result can be concluded from Theorem 123 in [8]. Using this conclusion, Rivest's Theorem [19] can be easily deduced.

3.2. Orthomorphic Permutations

Theorem 3 reveals some new properties of permutation polynomials over the residue class rings. In addition, from this theorem we can deduce some other useful results.

In some cryptosystems, the orthomorphic permutation is a necessary part, such as SMS4 [3] and LOISS [7]. The function $f(x)$ defined on the finite field $\mathbb{F}_{2^n}$ is called an orthomorphic permutation if both $f(x)$ and $f(x) + x$ are permutations on $\mathbb{F}_{2^n}$. Orthomorphic permutation was proposed by lv [12] and Mittenthal [14] independently in their research work. It is a subclass of complete mapping [18], and useful in cryptography. So when we consider the functions over residue class rings, it is worth studying similar properties.

Corollary 1. *Let $f(x)$ and $g(x)$ be permutation polynomials over $\mathbb{Z}_N$. $N > 3$ is an even integer. Then $(f(x) + g(x))$ can not permute $\mathbb{Z}_N$. Especially, $f(x)$ will never be an orthomorphic permutation over $\mathbb{Z}_N$.*

Proof. According to Theorem 3, we know that if both $f(x)$ and $g(x)$ permute $\mathbb{Z}_N$, then we can conclude that both $f(x)$ and $g(x)$ permute $S_1 = \{0 < t < N : \gcd(N, t) = 1\}$, and then $2 \mid (f(x) + g(x))$. So $(f(x) + g(x))$ will not permute S_1, thus it can not permutes $\mathbb{Z}_N$. The last statement is oblivious if $g(x) = x$. □

Remark 2. In Corollary 1, "$a + b$" means "$(a + b) \bmod N$".

3.3. Differential Properties

Differential cryptanalysis [4] is a powerful tool to attack the cryptosystems, while low differential uniform functions can provide good resistance against it. Especially, APN functions can provide the optimal resistance against differential cryptanalysis in the finite field of characteristic 2. But it is rather difficult to find APN permutations in practice. Hou [9] proved that there are no APN permutations on $\mathbb{F}_{2^4}$, while Dillon [6] found an APN permutation on $\mathbb{F}_{2^6}$, but it is still an open problem whether APN permutations exist on $\mathbb{F}_{2^n}$ with n even and greater than 6. Therefore, it is a potential choice to study the case over the residue class rings, and it maybe be better to design the cryptosystems over them. As a matter of fact, there seems to be many APN permutation functions over the residue class rings [5], but when the functions can be represented by polynomials, their differential properties will become even worse.

Theorem 6. *Let $f(x)$ be the same as in Theorem 3. $N > 3$ is composite. $a \in \mathbb{Z}_N$ is the biggest nontrivial divisor of N, then*
(1) $\delta(f) \geq \frac{N}{\#S_a+1}$. Especially, $f(x)$ can never be APN functions over $\mathbb{Z}_N$ when $N > 4$.
(2) If we add the premise that $f_N(x)$ permutes $\mathbb{Z}_N$, then $\delta(f) \geq \frac{N}{\#S_a}$. Especially, $f(x)$ can never be APN permutations over $\mathbb{Z}_N$.

Proof. (1) Consider the function $D(x) = f(x+a) - f(x)$, then it is easy to see that $a \mid D(x)$, so there must be $a \mid \gcd(D(x), N)$, which implies that $a \mid \gcd(D_N(x), N)$ (Note that $D_N(x) = D(x) \bmod N$). In addition, we have $a \in L_1$, so we can deduce that $D_N(x) \in (S_a \cup S_0)$. When x varies over $\mathbb{Z}_N$, the function $D_N(x)$ will produce N values. Based on Pigeonhole Principle, there must exist some $b \in (S_a \cup S_0)$ such that $D_N(x) = b$ has at less $\frac{N}{\#S_a+1}$ solutions, which means that $\delta(f) \geq \frac{N}{\#S_a+1}$. Easy to check that $\frac{N}{\#S_a+1} > 2$ when $N > 4$. When $N = 4$, $f(x) = x^2 \bmod 4$ is an APN function, so the lowerbound is tight.
(2) The proof is similar as in (1), the only difference is that when $f_N(x)$ permutes $\mathbb{Z}_N$, $D_N(x) \neq 0$, which implies that $D_N(x) \notin S_0$, and then $D_N(x) \in S_a$. Thus we can get $\delta(f) \geq \frac{N}{\#S_a}$. Since N is composite, easy to check that $\frac{N}{\#S_a} > 2$. □

Corollary 2. *Let $f(x)$ be the same as in Theorem 3. $N > 3$ is an even integer, then $\delta(f) \geq \frac{N}{2}$. If $f_N(x)$ permutes $\mathbb{Z}_N$, then $\delta(f) = N$.*

PROOF. Note $2 \mid N$, then the biggest nontrivial divisor of N is $\frac{N}{2}$. Easy to see that $\#S_{\frac{N}{2}} = \#\{\frac{N}{2}\} = 1$. Thus, according to Theorem 6 we can conclude that $\delta(f) \geq \frac{N}{\#S_{\frac{N}{2}}+1} = \frac{N}{2}$. If $f_N(x)$ permutes $\mathbb{Z}_N$, then $\delta(f) \geq \frac{N}{\#S_{\frac{N}{2}}} = N$. $\square$

In block cipher RC6 [20], the designers use a polynomial function $f(x) = x(2x+1)$ defined over $\mathbb{Z}_{2^{32}}$. Based on Rivest's theorem [19], it is easy to conclude that $f(x)$ is a permutation polynomial over $\mathbb{Z}_{2^{32}}$. However, from Corollary 2 we can see that $\delta(f) = 2^{32}$, and there are no better choices since all permutation polynomials defined over $\mathbb{Z}_{2^{32}}$ have the same differential uniformity 2^{32}. So $f(x)$ performs badly against differential attacks, and the designers have to use other method to provide differential safety.

4. Beyond Polynomial Forms

According to what we have got above, it is easy to see that the polynomial functions defined over the residue class rings have very good mathematical structures, especially when they are permutations. Therefore, an overwhelming majority polynomial functions can not provide direct differential safety for a crptosystem. If these functions are used in some cryptographic algorithms, the designers must use other method to guarantee safety, but this does not mean that all functions over the residue class rings have bad differential properties. As a matter of fact, if we do not restrict the functions to be polynomial forms, many APN permutations can be found over the residue class rings. Drakakis [5] studied APN permutations over them and got the following results.

Theorem 7. *Suppose $\mathbb{F}_p$ is a finite field with p elements, $p > 2$ is a prime number, g is a primitive element over $\mathbb{F}_p$, define a function $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$, that is, $f(i) = (g^i \bmod p) - 1$, then $f(x)$ is an APN permutation over the ring $\mathbb{Z}_{p-1}$.*

By this means, many APN permutations have been builded in practice. The Russian standard GOST has used $\mathbb{Z}_{16}$ already. The SAFER family of cryptosystems, proposed by Massey [13], uses APN functions from $\mathbb{Z}_{256}$ to itself. This is a special case for Drakakis's construction when $p = 257$.

In addition, Drakakis made a computer search about the APN permutations over $\mathbb{Z}_n$ for some integer n, and we list some of his results in Table 1.

Table 1: APN permutations over $\mathbb{Z}_n$

n	3	4	5	6	7	8	9
APNs	0	16	100	252	588	2816	1458
n	10	11	12	13	14	15	16
APNs	47800	136730	380736	1614288	4083072	13305600	54771712

In Table 1, row "n" denotes the value of n, and row "APNs" denotes the number of APN permutations over the corresponding residue class ring $\mathbb{Z}_n$.

Based on the above results, it is observed that although the polynomial functions over the residue class rings do not have good differential properties, there are still other choices, but how to find them? We give an open problem here.

Problem 1. *Find more APN permutations over $\mathbb{Z}_n$ for the general integer n? Give proper forms to denote the APN permutations over $\mathbb{Z}_n$?*

References

[1] L. Carlitz, Functions and polynomials (mod p^n), Acta Arith. IX (1964) 67-78.

[2] Z. Chen, On polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$, Discrete Mathematics 137 (1995) 137-145.

[3] Chinese State Bureau of Cryptography Administration, Cryptographic algorithms SMS4 used in wireless LAN products, http://www.oscca.gov.cn/Doc/6/News_1106.htm.

[4] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, 4(1) (1991) 3-72.

[5] K. Drakakis, R. Gow, G. McGuire, APN Permutations on $\mathbb{Z}_n$ and Costas Arrays, Discrete Applied Mathematics, 157(15) (2009) 3320-3326.

[6] J. F. Dillon, APN polynomials: an update, The 9th International Conference on Finite Fields and Applications, Dublin, Ireland, July 2009.

[7] D.G. Feng, X.T. Feng, W.T. Zhang, X.B.Fan, C.K. Wu, Loiss: A Byte-Oriented Stream Cipher, http://eprint.iacr.org/2010/489.

[8] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Clarendon, Oxford, 5th ed., 1979.

[9] X.D. Hou, Affinity of permutations of $\mathbb{F}_2^n$, Discrete Applied Mathematics 154(2) (2006) 313-325.

[10] G. Keller, F.R. Olson, Counting polynomial functions (mod p^n), Duke Math. J. 35 (1968) 835-838.

[11] A.J. Kempner, Polynomials and their residue systems, Amer. Math. Soc. Trans. 22 (1921) 240-288.

[12] S.W Lv, X.B Fan, Z.S Wang, J.L Xu and J. Zhang, Complete mappings and their appliactions, University of Sciences and Technology of China Press, 2008.

[13] J.L. Massey, SAFER K-64: A byte-oriented block-ciphering algorithm, Fast Software Encryption, 1993, pp. 1-17.

[14] L. Mittenthal, Block substitutions using orthomorphic mappings, Advances in Applied Mathematics, 16(1) (1995) 59-71.

[15] G. Mullen, H. Stevens, Polynomial functions (mod m), Acta Math. Hungar. 44 (Nos. 3 and 4) (1984) 237-241.

[16] R. Lidl, H. Niederreiter, Finite fields. Cambridge, U.K.: Cambridge Univ. Press, 1983.

[17] K. Nyberg, Differentially uniform mappings for cryptography. Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science 765, 1994, pp. 55-64.

[18] L.J. Paige, Complete mappings of finite groups, Pacific J. Math. Volume 1 Number 1 (1951) 111-116.

[19] R. Rivest, Permutation polynomials modulo 2^w, Finite Fields and their Applications 7 (2001) 287-292.

[20] R. Rivest, M. Robshaw, R. Sidney, Y. Yin, The RC6$^{\mathrm{TM}}$ Block Cipher, Specification version 1.1 1998.

[21] D. Singmaster, On polynomial functions (mod m), J. Number Theory 6 (1974) 345-352.

[22] J. Sun, O. Y. Takeshita, Interleavers for turbo codes using permutation polynomials over integer rings, IEEE Trans. Inform. Theory, 51(1) (2005) 101-119.