Nonliear permutations of a space over a finite field induced by linear transformations of a module over a Galois ring

Alexandr Nechaev and Alexandr Abornev

Let $P = \mathrm{GF}(q),\ \ q = p^r$ be a field with operations $\oplus, \cdot$. Let us consider P as a *p-adic digit set* of a Galois ring $R = \mathrm{GR}(q^2, p^2)$ (with operations $+, \cdot$): $P = \Gamma(R) = \{a \in R : a^q = a\}$. Then every element $a \in R$ has the p-adic decomposition: $a = a_0 + pa_1,\ a_s = \gamma_s(a) \in P,\ s \in \overline{0,1}$. Here $\gamma_s \colon R \to P,$ is *digit function*. Operation $\oplus$ on P satisfies the equality $x \oplus y = \gamma_0(x + y)$.

For a matrix $A = (a(ij)) \in R_{m,m}$ the decomposition $A = A_0 + pA_1,\ \ A_s = (a_s(ij)) \in P_{m,m},\ s \in \overline{0,1}$ is also valid. Any matrix $A \in R_{m,m}$ defines a map $\pi_A : P^{(m)} \to P^{(m)}$ by the condition

$$\forall u^{\downarrow} \in P^{(m)} : \quad \pi_A(u^{\downarrow}) = \gamma_1(Au^{\downarrow}) = (f_1(u^{\downarrow}), \ldots, f_m(u^{\downarrow}))^T. \tag{1}$$

Here coordinate functions $f_1, \ldots, f_m$ are polynomials over P.

For any $m \in \mathbb{N}$ there exist matrices $A \in R_{m,m}$ such that π_A is a permutation. In this case the matrix A is called *digit-permutating* (or *DP-matrix*) and the system of functions (2) is said to be *orthogonal* [1].

In the case $p = 2$ it is known [2] that the system of functions in (1) has a form

$$f_j(u^{\downarrow}) = \sigma_2(a_0(j1)u_1, \ldots, a_0(jm)u_m) \oplus l_j(u^{\downarrow}), \quad j \in \overline{1,m}, \tag{2}$$

where σ_2 is an elementary symmetric function of the order 2 and $l_j(u^{\downarrow})$ is a linear function. For an arbitrary orthogonal system of functions (2) there exists a DP-matrix satisfying (1).

All orthogonal systems of functions of the form (2) containing one and two nonlinear functions are described. It is proved that a quadratic function f_1 can be filled up to an orthogonal system with some system of functions $f_2, ..., f_m$ if and only if it can be filled up with some system of linear functions.

It is proved that for any Galois ring $R = \mathrm{GR}(q^2, p^2)$ every matrix $A \in R_{m,m}$ of the form

$$A = \begin{pmatrix} * & \dots & * & u_1 & pv_1 \\ * & \dots & u_2 & pv_2 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ u_{m-1} & pv_{m-1} & \cdots & 0 & 0 \\ pv_m & 0 & \cdots & 0 & u_m \end{pmatrix}, \qquad (3)$$

where $u_1, , u_m, v_1, , v_m \in R^*$, is a digit-permutating matrix.

Properties of block ciphers of the form $(G\pi_A)^l$, where G is a regular permutation subgroup of the symmetric group $S\left(P^{(m)}\right)$ are studied. In particular it is proved that if $R = \mathbb{Z}_{p^2}$, $p^m - 1$ is a composite number and G is a regular representation of the group $(\mathbb{Z}_{p^m}, +)$, then a subgroup $\langle G\pi_A \rangle$ of the group $S\left(\mathbb{Z}_p^{(m)}\right)$ contains alternating group for all matrices of the form (3) and for the big enough class of other permutations listed above.

Keywords: Galois ring, digit-permutating matrix, orthogonal system of quadratic forms, block cipher.

References

[1] Lidl R., Niederreiter H., Finite Fields, Cambridge University Press, second edition, 1997.

[2] Kuz'min A. S., Nechaev A. A. Linear recurring sequences over Galois rings. (Russian, English) Algebra and Logic 34, No.2, 87-100 (1995).