There are siblings of χ which are permutations for n even

Björn Kriepke and Gohar Kyureghyan

September 30, 2025

Let $\mathbb{1}$ be the all-one vector and $\odot$ denote the component-wise multiplication of two vectors in $\mathbb{F}_2^n$. We study the vector space Γ_n over $\mathbb{F}_2$ generated by the functions $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n, k \geq 0$, where

$$\gamma_{2k} = S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot (\mathbb{1} + S^{2k-3}) \odot \ldots \odot (\mathbb{1} + S)$$

and $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the cyclic left shift function. The functions in Γ_n are shift-invariant and the well known χ function used in several cryptographic primitives is contained in Γ_n. For even n, we show that the permutations from Γ_n with respect to composition form an Abelian group, which is isomorphic to the unit group of the residue ring $\mathbb{F}_2[X]/(X^n + X^{n/2})$. This isomorphism yields an efficient theoretic and algorithmic method for constructing and studying a rich family of shift-invariant permutations on $\mathbb{F}_2^n$ which are natural generalizations of χ. To demonstrate it, we apply the obtained results to investigate the function $\gamma_0 + \gamma_2 + \gamma_4$ on $\mathbb{F}_2^n$.

1 Introduction

Let $\mathbb{F}_2$ be the field with two elements. The function $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ mapping x to $\chi(x)$ is defined by

$$\chi(x)_i = x_i + x_{i+2}(1 + x_{i+1}),$$

where $\chi(x)_i$ denotes the ith coordinate function of χ for $1 \leq i \leq n$. The computations of indexes are done modulo n. The function χ is used in several important cryptographic primitives, for example SHA-3 [16] and Ascon [4]. Mathematical properties of χ are studied in [7, 14, 13, 19, 20]. The function χ commutes with the left and right shift functions. Such functions are called shift invariant and can be effectively implemented in practice. Shift invariant functions are closely related with cellular automata (CA) [8], they are one-dimensional CA on periodic configurations.

The shift invariant permutation on $\mathbb{F}_2^n$ are of particular interest in cryptological applications. It is well-known that χ is a permutation if and only if n is odd (see for example [3]). However, in many of designs of block ciphers, the block length is even and therefore constructions of permutations with good cryptographic properties required for n even. In [2], a permutation for $n = 2m$ with m even is constructed via concatenation of two χ functions and the addition of a suitable linear function. This method was extended to cover any even n in a recent paper [1]. However, the resulting permutations are not shift-invariant.

In our recent paper [10], it is observed that for an odd n a number of properties of χ can be explained by studying the binary polynomial $1 + X$ modulo $X^{(n+1)/2}$. For example, its order, its cycle structure, the explicit form of its iterates and its inverse function can be effectively derived via this correspondence. We outline briefly the main ideas and results of [10] below.

Let $\mathbb{1}$ denote the vector $(1, \ldots, 1) \in \mathbb{F}_2^n$ and $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the cyclic left shift function, i.e.,

$$S(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1).$$

With the symbol $\odot$ we denote the component-wise multiplication of two vectors $x, y \in \mathbb{F}_2^n$. More precisely, $z = x \odot y$ denotes the vector with the ith component $z_i = x_i \cdot y_i$ for all $1 \leq i \leq n$. Note that S is linear. Furthermore, $S(x \odot y) = S(x) \odot S(y)$. The operation $\odot$ is commutative and distributive with respect to the addition, that is, $x \odot y = y \odot x$ and $x \odot (y + z) = x \odot y + x \odot z$. Define $\gamma_0 = \mathrm{id}$ and $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for $k \geq 1$ by

$$\gamma_{2k} := S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot (\mathbb{1} + S^{2k-3}) \odot \ldots \odot (\mathbb{1} + S).$$

The function γ_{2k} is shift-invariant, since $\gamma_{2k} \circ S = S \circ \gamma_{2k}$. Note that $\chi = \gamma_0 + \gamma_2$.

For n odd, it is shown in [10], that the iterates of the function χ are linear combinations of functions γ_{2k} over $\mathbb{F}_2$. This motivated the study of the linear span Γ_n of the functions γ_{2k} over $\mathbb{F}_2$. If n is odd, then Γ_n has dimension $(n+1)/2$, since $\gamma_{2k} = 0$ for every k with $2k > n$ and the functions $\gamma_0, \gamma_2, \gamma_4, \ldots, \gamma_{n-1}$ are linearly independent over $\mathbb{F}_2$. Since $\gamma_{2k}(0) = \gamma_{2k}(\mathbb{1}) = 0$ for every $k \geq 1$, it follows that every permutation in Γ_n is contained in $G_n = \gamma_0 + \mathrm{span}\{\gamma_2, \ldots, \gamma_{n-1}\}$. Notably, it was shown in [10] that G_n is a monoid with respect to composition, which is isomorphic to

$$\mathcal{M}_n = \left\{ \left[1 + \sum_{i=1}^{t} a_i X^i \right] \right\} \subseteq \mathbb{F}_2[X]/(X^{(n+1)/2}),$$

that is to the unit group of the residue ring $\mathbb{F}_2[X]/(X^{(n+1)/2})$. From the fact that $(\mathcal{M}_n, \cdot)$ is an Abelian group it follows that $(G_n, \circ)$ is also an Abelian group. Hence, G_n consists of permutations which commute. This isomorphism allows to construct, both theoretically and algorithmically, a rich family of shift-invariant permutations. Further, it reduces the study of specific properties of these permutations to that of the corresponding binary polynomials. To the best of our knowledge, the previously known families

of shift-invariant permutations are sporadic, in the sense that they are described by a specific algebraic formula for suitable infinite set of n.

The ideas of [10] are adapted in [15] to construct χ-like permutations which are called $\chi_{n,m}$. If $m = 2$ then $\chi_{n,2}$ coincides with χ. Using similar steps as [10], they show that $\chi_{n,m}$ is contained in an Abelian group which is isomorphic to the unit group of $\mathbb{F}_2[X]/(X^{\lfloor n/m \rfloor+1})$ if m does not divide n.

In this paper we generalize the ideas of [10] to study the linear span Γ_n of the functions γ_{2k} when n is even. We show that Γ_n is an n-dimensional vector space. Similarly to the n odd case, all permutations in Γ_n are contained in $G_n = \gamma_0 + \mathrm{span}\{\gamma_{2i} : i \geq 1\}$. However, in contrast to the n odd case, G_n also contains non-bijective functions if n is even. We show that the subset of bijections in Γ_n is an Abelian group which is isomorphic to the unit group of the ring $\mathbb{F}_2[X]/(X^n + X^{n/2})$. We expect that analogously to the case n odd, the ideas of this paper can be adapted to cover the remaining case $m \mid n$ for the functions studied in [15].

The study of units in $\mathbb{F}_2[X]/(X^n + X^{n/2})$ is closely related to the factorization of the polynomial $X^{n/2} + 1$ over $\mathbb{F}_2$, which is a challenging classical problem in algebra and number theory. This explains why the behavior of permutation from Γ_n is not as consistent as for n odd. For n odd the corresponding residue ring is modulo $X^{(n+1)/2}$, which has the unique irreducible factor X, independently of n. For n even, the factorization of $X^{n/2} + 1$ depends on n and in general is not easy to write down [6]. In spite of this, similarly to the n odd case, the isomorphism of the set of permutations in Γ_n with the unit group of $\mathbb{F}_2[X]/(X^n + X^{n/2})$ yields an effective and powerful method for constructing and studying a rich family of shift-invariant permutations, which are natural generalizations of χ. We demonstrate our methods by applying them to study the map $\kappa = \gamma_0 + \gamma_2 + \gamma_4$ which is the simplest function in G_n which can be a permutation for n even.

2 χ-like shift-invariant permutations for n even

The next example demonstrates that the behavior of the set of functions γ_{2k} on $\mathbb{F}_2^n$ depends strongly on the parity of n.

Example 1. First consider an odd n. We take $n = 7$. Then the first few functions γ_{2k} are given by

$$\begin{aligned}
\gamma_0 &= \mathrm{id} \\
\gamma_2 &= S^2 \odot (\mathbb{1} + S) \\
\gamma_4 &= S^4 \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_6 &= S^6 \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S)
\end{aligned}$$

$$\gamma_8 = S^8 \odot (\mathbb{1} + S^7) \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S).$$

Since $S^8 = S^1$ we get the product $S^1 \odot (\mathbb{1} + S) = 0$ in the last line, implying that $\gamma_8 = 0$. Moreover, all functions $\gamma_0, \ldots, \gamma_6$ have distinct algebraic degree. Recall, that the algebraic degree of a function $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as the maximum over the multivariate degrees of its component functions of $g(x)_i, 1 \leq i \leq n$. In [10] it is shown, that $\gamma_{2k} = 0$ for any $2k \geq n + 1$ and that γ_{2k} has algebraic degree $k + 1$ for $2k < n + 1$.

For n even this is not the case. Let $n = 6$. Then the first functions γ_{2k} are:

$$\begin{aligned}
\gamma_0 &= S^0 = \mathrm{id} \\
\gamma_2 &= S^2 \odot (\mathbb{1} + S) \\
\gamma_4 &= S^4 \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_6 &= S^6 \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_8 &= S^8 \odot (\mathbb{1} + S^7) \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_{10} &= S^{10} \odot (\mathbb{1} + S^9) \odot (\mathbb{1} + S^7) \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_{12} &= S^{12} \odot (\mathbb{1} + S^{11}) \odot (\mathbb{1} + S^9) \odot (\mathbb{1} + S^7) \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_{14} &= S^{14} \odot (\mathbb{1} + S^{13}) \odot (\mathbb{1} + S^{11}) \odot (\mathbb{1} + S^9) \odot (\mathbb{1} + S^7) \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S)
\end{aligned}$$

Using $S^6 = \mathrm{id} = S^0$ and that $y \odot y = y$ for all $y \in \mathbb{F}_2^n$, we get

$$\begin{aligned}
\gamma_6 &= S^0 \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_8 &= S^2 \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_{10} &= S^4 \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \\
\gamma_{12} &= S^0 \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) = \gamma_6 \\
\gamma_{14} &= S^2 \odot (\mathbb{1} + S^5) \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) = \gamma_8
\end{aligned}$$

In contrast to the situation for n odd, we observe that $\gamma_{12} = \gamma_6$ and $\gamma_{14} = \gamma_8$. In particular, the functions eventually repeat instead of vanishing for large k. Furthermore their algebraic degrees are not distinct for $k \geq n/2$.

The above example suggests that for n even and k large, the functions γ_{2k} are equal to ones with smaller k. The next lemma confirms this.

Lemma 1. *Let n be even and $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$. If $k \geq n/2$, then*

$$\gamma_{2k} = S^{2k \bmod n} \odot (\mathbb{1} + S^{n-1}) \odot (\mathbb{1} + S^{n-3}) \odot \ldots \odot (\mathbb{1} + S).$$

In particular,

(a) if $k, k' \geq n/2$ and $2k \equiv 2k' \bmod n$, then $\gamma_{2k} = \gamma_{2k'}$;

(b) if $2k \geq n$ then $\gamma_{2k} = \gamma_{2(\frac{n}{2} + k \bmod \frac{n}{2})}$.

Proof. The statement follows from the observations that on $\mathbb{F}_2^n$ it holds $S^n = \mathrm{id}$ and

$$(\mathbb{1} + S^j) \odot \ldots \odot (\mathbb{1} + S^j) = \mathbb{1} + S^j.$$

□

As a direct consequence of Lemma 1 we get

Lemma 2. *Let n be even. Then $\gamma_{2k} = \gamma_{2k-n}$ on $\mathbb{F}_2^n$ if $k \geq n$.*

Proof. This follows from Lemma 1, since $2k \equiv 2k-n \bmod n$ and $k, (k-n/2) \geq n/2$. □

For even n, Lemma 1 implies that the set of functions $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $k \geq 0$ reduces to that of γ_{2k} with $0 \leq k \leq n-1$. Next we prove that these n functions are linearly independent over $\mathbb{F}_2$.

Lemma 3. *Let n be even. The functions $\gamma_0, \gamma_2, \gamma_4, \ldots, \gamma_{2n-2}$ of $\mathbb{F}_2^n$ are linearly independent over $\mathbb{F}_2$.*

Proof. Let $x = (x_0, x_1, \ldots, x_{n-1})$. Then the coordinate functions $\gamma_{2k}(x)_0$ are given by

$$\begin{aligned}
\gamma_0(x)_0 &= x_0 \\
\gamma_2(x)_0 &= x_2(1 + x_1) \\
\gamma_4(x)_0 &= x_4(1 + x_3)(1 + x_1) \\
&\vdots \\
\gamma_{n-2}(x)_0 &= x_{n-2}(1 + x_{n-3}) \ldots (1 + x_1) \\
\gamma_n(x)_0 &= x_0(1 + x_{n-1})(1 + x_{n-3}) \ldots (1 + x_1) \\
\gamma_{n+2}(x)_0 &= x_2(1 + x_{n-1})(1 + x_{n-3}) \ldots (1 + x_1) \\
&\vdots \\
\gamma_{2n-2}(x)_0 &= x_{n-2}(1 + x_{n-1})(1 + x_{n-3}) \ldots (1 + x_1).
\end{aligned}$$

Note that the highest degree monomials in these coordinate functions are pairwise different, implying that they are linearly independent over $\mathbb{F}_2$. □

Lemma 4. *Let n be even, $k \geq 0$ and d be the algebraic degree of $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then*

$$d = \begin{cases} k+1 & k \leq n/2 \\ n/2+1 & k \geq n/2. \end{cases}$$

Proof. The statement follows immediately from the proof of Lemma 3, since all coordinate functions of γ_{2k} have the same multivariate degree due to the shift-invariance. □

We consider the set of the linear combinations of the functions $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ over $\mathbb{F}_2$

$$\Gamma_n := \left\{ \sum_{k=0}^{\ell} a_k \gamma_{2k} : \ell \geq 0,\ a_k \in \mathbb{F}_2 \right\} = \left\{ \sum_{k=0}^{n-1} a_k \gamma_{2k} : a_k \in \mathbb{F}_2 \right\}.$$

Note that the latter equality follows from Lemma 1.

Lemma 5. *Let n be even. Then the set Γ_n is an n-dimensional vector space over $\mathbb{F}_2$ and $\{\gamma_0, \gamma_2, \ldots, \gamma_{2n-2}\}$ is a basis of it.*

Proof. Let V be the $\mathbb{F}_2$-vector space of all functions of $\mathbb{F}_2^n$. The set Γ_n is defined as the subspace of V generated by functions γ_{2k}, $k \geq 0$. Lemma 3 shows that $\{\gamma_0, \gamma_2, \ldots, \gamma_{n-1}\}$ is a basis of Γ_n. □

Lemmas 4–7 of [10] show that compositions of the linear combinations of functions γ_{2k} have a strongly structured behavior. However these lemmas hold independently on the parity of n (and in fact also for γ_{2k} considered as functions on $\mathbb{F}_2^{\mathbb{N}}$ or $\mathbb{F}_2^{\mathbb{Z}}$), which makes the study of functions from Γ_n interesting also for n even. Lemma 7 from those results is the key lemma for our considerations here, therefore we state it below. Let G_n to denote the coset of $\gamma_0 = \mathrm{id}$ with respect to the subspace generated by the remaining $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n, k \geq 1$, that is

$$G_n := \gamma_0 + \mathrm{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{2n-2}\}.$$

The next lemma shows that the left composition of functions from G_n with any γ_{2k} is again a linear combination from Γ_n.

Lemma 6 ([10], Lemma 7)**.** *Let $m \geq 2$ be even and $f = \gamma_0 + \sum_{i=1}^{t} a_i \gamma_{2i} \in G_n$. Then*

$$\gamma_m \circ f = \sum_{i=0}^{t} a_i \gamma_{2i+m} \in \Gamma_n.$$

Lemma 6 indicates that the composition of the functions in G_n has strong similarities with the multiplication of polynomials over $\mathbb{F}_2$. Indeed,

$$\gamma_2 \circ (\gamma_0 + \gamma_4 + \gamma_6) = \gamma_2 + \gamma_6 + \gamma_8$$

looks very much like

$$X^2 \cdot (1 + X^4 + X^6) = X^2 + X^6 + X^8.$$

After dividing the exponents of the polynomials by 2, we then obtain correspondence of the form

$$\sum_{i=0}^{t} a_i \gamma_{2i} \mapsto \sum_{i=0}^{t} a_i X^i.$$

Further, by Lemma 2 the equality $\gamma_{2k} = \gamma_{2k-n}$ holds for all k with $k \geq n$, when n is even. This means that in the polynomial setting we need to require $X^k = X^{k-n/2}$, or equivalently $X^k + X^{k-n/2} = 0$ if $k \geq n$. We can achieve this by considering the polynomials modulo $X^n + X^{n/2}$. In other words, we work in the residue ring

$$\mathcal{R}_n = \mathbb{F}_2[X]/(X^n + X^{n/2}),$$

where $(X^n + X^{n/2})$ is the ideal generated by the polynomial $X^n + X^{n/2}$ in $\mathbb{F}_2[X]$.

For a polynomial $f \in \mathbb{F}_2[X]$, let $[f] = f + (X^n + X^{n/2})$ denote the coset of f in $\mathcal{R}_n$. Then the maps $\varphi : \Gamma_n \to \mathcal{R}_n$ and $\psi : \mathcal{R}_n \to \Gamma_n$ are well-defined and inverse each to other, where

$$\varphi\left(\sum_{i=0}^{t} a_i \gamma_{2i}\right) = \left[\sum_{i=0}^{t} a_i X^i\right]$$

and

$$\psi\left(\left[\sum_{i=0}^{t} a_i X^i\right]\right) = \sum_{i=0}^{t} a_i \gamma_{2i}.$$

In particular, φ and ψ are bijections.

Further, we define the set

$$\mathcal{M}_n := \left\{ \left[1 + \sum_{i=1}^{t} a_i X^i\right] : t \geq 1, a_i \in \mathbb{F}_2 \right\} \subseteq \mathcal{R}_n.$$

Note that $\mathcal{M}_n$ is closed under the multiplication of $\mathcal{R}_n$ and $[1] \in \mathcal{M}_n$. Hence $\mathcal{M}_n$ is a monoid with respect to the multiplication. Recall, that a monoid $(M, \star)$ is a set together with an associative operation $\star : M \times M \to M$ such that there exists a neutral element $e \in M$ with respect to $\star$. The invertible elements of M are called units and their set is denoted by M^*. Now we are ready to prove our first main result. It is worth to note that its proof is an analogue of that for n odd from [10].

Theorem 1. *Let $n \geq 2$ be even. Then*

(a) G_n is an Abelian monoid with respect to composition. The map $\varphi : G_n \to \mathcal{M}_n$ is a monoid isomorphism. In particular, $G_n \cong \mathcal{M}_n$.

(b) The set G_n^* of invertible (equivalently, bijective) functions from G_n is an Abelian group with respect to composition, which is isomorphic to the unit group $\mathcal{R}_n^* = \mathcal{M}_n^*$ of $\mathcal{R}_n$.

Proof. We first show that G_n is a monoid. Clearly $\mathrm{id} = \gamma_0 \in G_n$, so we only need to show that G_n is closed under composition. Set $\mathcal{C}_n := \mathrm{span}\{\gamma_2, \ldots, \gamma_{2n-2}\}$, and then $G_n = \gamma_0 + \mathcal{C}_n$. By Lemma 6, we have $\gamma_m \circ g \in \mathcal{C}_n$ for all $g \in G_n$. Let now $f, g \in G_n$ with $f = \gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}$. Then

$$f \circ g = \left(\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}\right) \circ g = \underbrace{\gamma_0 \circ g}_{=g} + \left(\sum_{i=1}^{k} a_i \gamma_{2i}\right) \circ g = g + \sum_{i=1}^{k} a_i \underbrace{\gamma_{2i} \circ g}_{\in \mathcal{C}_n} \in \gamma_0 + \mathcal{C}_n = G_n$$

since $g \in \gamma_0 + \mathcal{C}_n$ and $\mathcal{C}_n$ is a subspace.

Next we show that φ is a monoid homomorphism. From the definition it is clear that φ (as a map $\Gamma_n \to \mathcal{R}_n$) is additive. Let $f = \sum_{i=0}^{k} a_i \gamma_{2i}, g = \sum_{j=0}^{m} b_j \gamma_{2j} \in G_n$ with $a_0 = b_0 = 1$. Using Lemma 6 we have

$$\varphi(f \circ g) = \varphi\left(\left(\sum_{i=0}^{k} a_i \gamma_{2i}\right) \circ g\right) = \sum_{i=0}^{k} a_i \varphi(\gamma_{2i} \circ g)$$

$$= \sum_{i=0}^{k} a_i \varphi \left(\sum_{j=0}^{m} b_j \gamma_{2j+2i} \right) = \sum_{i=0}^{k} a_i \left[\sum_{j=0}^{m} b_j X^{j+i} \right]$$
$$= \sum_{i=0}^{k} a_i \left[X^i \right] \left[\sum_{j=0}^{m} b_j X^j \right] = \left[\sum_{i=0}^{k} a_i X^i \right] \left[\sum_{j=0}^{m} b_j X^j \right] = \varphi(f)\varphi(g).$$

Since $\varphi(\gamma_0) = [1]$ is the identity in $\mathcal{M}_n$, we get that φ is a monoid homomorphism between G_n and $\mathcal{M}_n$. As φ is bijective it is then a monoid isomorphism. To complete the proof of part (a), note that $\mathcal{M}_n$ is an Abelian monoid and thus G_n is Abelian too.

Observe that since G_n is a finite monoid with respect to composition, a function $f \in G_n$ is bijective if and only if it is invertible in G_n. That is, the inverse function of a bijection from G_n is contained in G_n too. Since $\varphi(\mathrm{id}) = [1]$, the invertible functions in G_n correspond to those in $\mathcal{M}_n$. It remains to observe that the units in $\mathcal{R}_n$ are contained in $\mathcal{M}_n$. □

Recall that for any $p(X) \in \mathbb{F}_2[X]$, the unit group of the residue ring $S = \mathbb{F}_2[X]/(p(X))$ is given by

$$S^* = \{[g(X)] : g(X) \in \mathbb{F}_2[X] \text{ s.t. } \gcd(g(X), p(X)) = 1\}.$$

In particular, the unit group S^* depends heavily on the factorization of $p(X)$ in $\mathbb{F}_2[X]$. If $[g(X)] \in \mathbb{F}_2[X]/(p(X))$ is a unit, then its inverse $[g(X)]^{-1}$ can be computed using the Extended Euclidean Algorithm in $\mathbb{F}_2[X]$.

The above discussions with Theorem 1 yield our next main result.

Theorem 2. *Let n be even and $f = \gamma_0 + \sum_{i=1}^{n-1} a_i \gamma_{2i} \in G_n$. Then f is a permutation on $\mathbb{F}_2^n$ if and only if $\varphi(f) = \left[1 + \sum_{i=1}^{n-1} a_i X^i\right] \in \mathcal{M}_n$ is a unit in $\mathbb{F}_2[X]/(X^n + X^{n/2})$, or equivalently, if and only if in $\mathbb{F}_2[X]$ it holds*

$$\gcd\left(1 + \sum_{i=1}^{n-1} a_i X^i, 1 + X^{n/2}\right) = \gcd\left(1 + \sum_{i=1}^{n-1} a_i X^i, 1 + X^m\right) = 1,$$

where m is the largest odd divisor of n.

Proof. Let $n = 2^s \cdot m$ with $s \geq 1$ and $m \geq 1$ odd. Then

$$X^n + X^{n/2} = X^{n/2}(X^{n/2} + 1) = X^{n/2}(X^m + 1)^{2^{s-1}}$$

and the statement follows from the discussions preceding the theorem. □

For n odd it was shown in [10] that $G_n = \gamma_0 + \mathrm{span}\{\gamma_2, \ldots, \gamma_{n-1}\}$ is isomorphic to the monoid

$$\mathcal{M}_n = \left\{ \left[1 + \sum_{i=1}^{t} a_i X^i\right] \right\} \subseteq \mathbb{F}_2[X]/(X^{(n+1)/2}),$$

which is the unit group of $\mathbb{F}_2[X]/(X^{(n+1)/2})$. This implies that G_n itself is a group. However, for n even, the unit group of $\mathcal{R}_n = \mathbb{F}_2[X]/(X^n + X^{n/2})$ is a proper subset of $\mathcal{M}_n$, as Theorem 2 shows. As an example, it is well-known and easy to see that $\chi = \gamma_0 + \gamma_2 \in G_n$ is not a permutation on $\mathbb{F}_2^n$ if n is even. Theorem 2 gives an alternative proof for it: It holds that $\varphi(\chi) = [1+X] \in \mathbb{F}_2[X]/(X^n+X^{n/2})$ and $\gcd(1+X, 1+X^{n/2}) = 1 + X \neq 1$, implying that χ is not a permutation. The same argument shows that if a linear combination f of γ_{2k} defines a permutation on $\mathbb{F}_2^n$ for an even n, then f needs to contain an odd number of non-zero terms.

It is worth to note that when n is a power of 2, then the converse of this fact is true as well, as stated in the next result.

Corollary 1. *Let n be a power of 2. Then $f \in G_n$ is a permutation on $\mathbb{F}_2^n$ if and only if f contains an odd number of non-zero terms.*

Proof. Let $n = 2^s$ and $\varphi(f) = [F(X)] \in \mathcal{M}_n$. By Theorem 2, f is a permutation if and only if $\gcd(F(X), 1 + X) = 1$ if and only if $F(1) = 1$. The latter condition is equivalent to F, and hence f, having an odd number of non-zero terms. □

The above results show that the bijectivity of functions from G_n depends on the factorization of $1+X^m$ over $\mathbb{F}_2$ which is a classical research topic in the field and number theory. For a comprehensive survey and recent developments on the factorization of $1 + X^m$ over finite fields we refer to [6].

We would like to conclude this section by noting that the Chinese Remainder Theorem can be used to study the residue ring $\mathbb{F}_2[X]/(X^n + X^{n/2})$. Indeed, if $n = 2^s m$, m is odd, then $1 + X^m = (1 + X)q(X)$ with $q(X) \in \mathbb{F}_2[X]$ and $q(1) \neq 0$. Then by the Chinese Remainder Theorem,

$$\mathbb{F}_2[X]/(X^n + X^{n/2}) \cong \mathbb{F}_2[X]/(X^{n/2}) \times \mathbb{F}_2[X]/((1 + X)^{2^s}) \times \mathbb{F}_2[X]/(q(X)^{2^s}).$$

In particular the unit group of $\mathbb{F}_2[X]/(X^n + X^{n/2})$ is a product of the unit groups of the rings on the right-hand side, which are easier to study.

3 A closer look on the permutations from G_n

Any shift-invariant function can be considered as a map $\mathbb{F}_2^n \to \mathbb{F}_2^n$ for every $n \geq 1$, since it is uniquely defined by its first coordinate function. In Section 2 we considered functions defined by linear combinations of $\gamma_{2k}, k \geq 0$ when n is fixed. In this section we study the functions defined by a fixed linear combination of γ_{2k} on $\mathbb{F}_2^n$ where n runs over $\mathbb{N}$. For this purpose it is convenient to introduce the set $G = \gamma_0 + \mathrm{span}\{\gamma_2, \gamma_4, \ldots\}$ which is independent of n.

Following [17], for a given shift-invariant f we consider the set

$$\mathrm{inv}(f) = \{n \in \mathbb{N} : f \text{ is a permutation on } \mathbb{F}_2^n\}.$$

The next statement is well-known, c.f. [3, Proposition 6.1] and the discussion afterwards. We give a short alternative proof.

Lemma 7. *Let n, d be positive integers with $d \mid n$ and let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a shift-invariant permutation. Then $f : \mathbb{F}_2^d \to \mathbb{F}_2^d$ is also a permutation.*

Proof. Consider the set

$$H = \{(x, x, \ldots, x) : x \in \mathbb{F}_2^d\} \subseteq \mathbb{F}_2^n.$$

As f is a permutation on $\mathbb{F}_2^n$, then $|f(H)| = |H| = 2^d$. On the other hand,

$$f(H) = \{(f(x), f(x), \ldots, f(x)) : x \in \mathbb{F}_2^d\}$$

by shift-invariance and hence $|f(H)| = \left|\{f(x) : x \in \mathbb{F}_2^d\}\right|$. The claim follows. □

Lemma 7 implies that $\mathrm{inv}(f)$ is closed under taking divisors. Equivalently, $\mathbb{N} \setminus \mathrm{inv}(f)$ is closed under taking multiples, which implies that there is a generating set $\xi(f) \subseteq \mathbb{N} \setminus \mathrm{inv}(f)$ of elements, so that $n \in \mathbb{N} \setminus \mathrm{inv}(f)$ if and only if n is a multiple of an element in $\xi(f)$. The set $\xi(f)$ has first been introduced in [3]. As an example, $\xi(\chi) = \{2\}$, because χ is invertible if and only if n is odd. There are very few functions f for which $\mathrm{inv}(f)$ and $\xi(f)$ are known. Even the question of whether they are finite is in general difficult to answer. Using our results on the correspondence between permutations in G_n and units in the residue ring $\mathbb{F}_2[X]/(X^{(n+1)/2})$, respectively $\mathbb{F}_2[X]/(X^n + X^{n/2})$ depending on parity of n, we determine $\mathrm{inv}(f)$ and $\xi(f)$ for every $f \in G$.

For a polynomial $F(X) \in \mathbb{F}_2[X]$ with $F(0) = 1$, the smallest natural number ℓ such that $F(X)$ divides $X^\ell + 1$ is called the order of $F(X)$. We denote it by $\mathrm{ord}(F)$. If $F(X) \in \mathbb{F}_2[X]$ is irreducible of degree $d \geq 2$, then $\mathrm{ord}(F)$ is a divisor of $2^d - 1$. Hence $\mathrm{ord}(F)$ is odd. Moreover, $F(X)$ divides $X^m + 1$ if and only if $\mathrm{ord}(F)$ divides m. For more information on the order of a polynomial, see for example [12].

Theorem 3. *Let $f \in G$ with $\varphi(f) = [F(X)]$ and $F = g_1^{e_1} \cdots g_t^{e_t} \in \mathbb{F}_2[X], e_i \geq 1$ be its factorization into irreducible factors. Then*

$$\xi(f) = \{2 \,\mathrm{ord}(g_i) : i \in \{1, \ldots, t\}\}.$$

In particular, $\xi(f)$ is finite and $\mathrm{inv}(f)$ is infinite.

Proof. If n is odd, then f is a permutation by Theorem 3 in [10].

If $n = 2^s m$ is even with m odd and $s \geq 1$, then by Theorem 2 f is a permutation if and only if $\gcd(F(X), X^m + 1) = 1$. This is equivalent to $\gcd(g_i(X), X^m + 1) = 1$ for all $i = 1, \ldots, t$. As g_i is irreducible, this is equivalent to g_i not being a divisor of $X^m + 1$ which is equivalent to $\mathrm{ord}(g_i) \nmid m$. Hence, f is a permutation for an even n if and only if n is not a multiple of $\mathrm{ord}(g_i)$ for every $i = 1, \ldots, t$. □

Remark 1. Theorem 3 and its proof imply that for any set $T = \{2t_1, 2t_2, \ldots, 2t_u\}$ with odd $t_i, 1 \leq i \leq u$, there exists a shift-invariant function f such that $\xi(f) = T$. Indeed, for a given odd t_i there is an irreducible polynomial $g_i \in \mathbb{F}_2[X]$ with $\mathrm{ord}(g_i) = t_i$. Such a polynomial exists: $t_i \mid 2^{m_i} - 1$ for some $m_i \geq 1$, ensuring the existence of an element $\alpha_i \in \mathbb{F}_{2^{m_i}}$ with $\mathrm{ord}(\alpha_i) = t_i$ and thus the minimal polynomial of α has the required properties for g_i. For $F = g_1 \cdots g_u$ and $f = \psi([F])$, it holds $\xi(f) = T$.

The following result is a direct consequence of Theorem 3. It could be useful in applications, since it allows to avoid an explicit computation of the order of the involved irreducible factors.

Corollary 2. *For $F \in \mathbb{F}_2[X]$ let $F = g_1^{e_1} \cdots g_t^{e_t}, e_i \geq 1$, be its factorization into irreducible factors and set $d_i = \deg(g_i)$. Define $f = \psi([F])$. Then*

$$\xi(f) \subseteq \{2\ell : \ell \mid 2^{d_i} - 1 \text{ for some } 1 \leq i \leq t\}.$$

Another immediate consequence of Theorem 2 is that for $f \in G$, with the exception of some special type of multiples, the converse of Lemma 7 holds too. More precisely, with the notation of Theorem 3, if $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a permutation, then $f : \mathbb{F}_2^{nv} \to \mathbb{F}_2^{nv}$ is a permutation as well for any $v \geq 1$ for which nv is not divisible by $2\,\mathrm{ord}(g_i)$ for every $1 \leq i \leq t$. In particular, when v is a power of 2 we get:

Corollary 3. *Let $n = 2^s \cdot m$ with $s \geq 2$ and $m \geq 1$ odd. Then $f \in G$ is a permutation on $\mathbb{F}_2^n$ if and only if it is a permutation on $\mathbb{F}_2^{2m}$.*

An interesting feature of permutations from G is that they permit additive manipulations (as we describe below). This is a rather rare behavior for a family of permutations. Even for linear functions, it is difficult to assure that additive manipulations lead to bijections. Another family of permutations, which tolerates special additive changes is the one constructed via change of coordinate functions with a linear structure [9, 5, 11, 18].

A function $f \in \Gamma$ is a permutation on $\mathbb{F}_2^n$ if and only if the polynomial $F \in \mathbb{F}_2[X]$, corresponding to it via $\varphi(f) = [F]$ in $\mathcal{M}_n$, is co-prime with $X(X^m + 1)$. The sum of F with any multiple of $X(X^m + 1)$ remains clearly co-prime with $X(X^m + 1)$. This simple observation allows to generate from a given permutation f on $\mathbb{F}_2^n$ numerous further permutation on $\mathbb{F}_2^{2^s n}$ for any $s \geq 0$. We demonstrate this with an example.

Example 2. The function $\tau = \gamma_0 + \gamma_2 + \gamma_6$ has algebraic degree 4 and is bijective on $\mathbb{F}_2^{22}$, since $\varphi(\tau) = 1 + X + X^3$ is irreducible and by Corollary 2 the set $\xi(\tau) = \{2 \cdot (2^3 - 1) = 14\}$ (that is, τ is a permutation on $\mathbb{F}_2^n$ for every n not divisible by 14). In particular, $\varphi(\tau) = 1 + X + X^3$ is co-prime with $1 + X^{11}$. Corollary 3 yields that τ is a permutation on $\mathbb{F}_2^n$ for every $n = 2^s \cdot 11$ with $s \geq 1$. Next we generate further permutations on $\mathbb{F}_2^{2^s \cdot 11}$ using τ, equivalently using the polynomial $1 + X + X^3$. Note, that the polynomial

$$H(X) = 1 + X + X^3 + G(X)X(X^{11} + 1)$$

is co-prime with $X^{11} + 1$ for any $G \in \mathbb{F}_2[X]$. Hence the function $\tau' = \psi([H])$ associated to it is a permutation on $\mathbb{F}_2^{2^s \cdot 11}$ for every $s \geq 1$. With the concrete choice $G(X) = 1$ and thus $H(X) = 1 + X + X^3 + X(X^{11} + 1)$ we get that $\psi(1 + X^3 + X^{12}) = \gamma_0 + \gamma_6 + \gamma_{24} = \tau'$ is a permutation on $\mathbb{F}_2^{2^s \cdot 11}$ for every $s \geq 2$. The function τ' differs from τ and it has algebraic degree 12 if $s = 1$ and 13 otherwise by Lemma 4.

4 The properties of $\kappa = \gamma_0 + \gamma_2 + \gamma_4$ in G_n

To conclude this paper, we apply the results of the previous sections to study the permutations corresponding to $1 + X + X^2 \in \mathbb{F}_2[X]$. This polynomial is the simplest one which for an even n may define a unit in $\mathcal{M}_n$, while $1 + X$ is so for an odd n. Recall that $1 + X$ corresponds to χ. We denote $\psi([1 + X + X^2]) = \gamma_0 + \gamma_2 + \gamma_4$ by κ.

Lemma 8. *Let $n \geq 1$. The function $\kappa = \gamma_0 + \gamma_2 + \gamma_4$ is a permutation on $\mathbb{F}_2^n$ if and only if n is not a multiple of 6.*

Proof. We apply Theorem 3. We have $F(X) = 1 + X + X^2$ which is irreducible with order $\mathrm{ord}(F) = 3$, since $(1 + X)(1 + X + X^2) = 1 + X^3$. Hence $\xi(\kappa) = \{6\}$. □

A typical way to describe shift-invariant functions is by using the so-called complementing landscape (CL), see for instance [21]. For example, χ is given by the CL $\chi = *01$. To explain what that means, let $y = \chi(x)$. Then the bit x_i gets flipped by χ if and only if x_i is followed by the pattern 01, i.e. $(x_{i+1}, x_{i+2}) = (0, 1)$. It can be quickly seen that this is equivalent to the previously mentioned formula $y_i = x_i + (1 + x_{i+1})x_{i+2}$.

Next we determine the CL for $\kappa = \gamma_0 + \gamma_2 + \gamma_4$. Let $y = \kappa(x)$. Then

$$y_i = x_i + (1 + x_{i+1})x_{i+2} + (1 + x_{i+1})(1 + x_{i+3})x_{i+4}.$$

Therefore, the bit x_i gets flipped by κ if and only if $(x_{i+1}, x_{i+2}, x_{i+3}, x_{i+4})$ satisfies

$$(1 + x_{i+1})x_{i+2} + (1 + x_{i+1})(1 + x_{i+3})x_{i+4} = 1.$$

The first term equals 1 if and only if $(x_{i+1}, x_{i+2}) = (0, 1)$ while the second term equals 1 if and only if $(x_{i+1}, x_{i+2}, x_{i+3}, x_{i+4}) = (0, -, 0, 1)$, where the $-$ means that x_{i+2} is arbitrary. If the first term is 1, then the other term must be 0, so if $(x_{i+1}, x_{i+2}) = (0, 1)$, then either $x_{i+3} = 1$ or $x_{i+4} = 0$. If the second term is 1 then the first term must be 0, so if $(x_{i+1}, x_{i+2}, x_{i+3}, x_{i+4}) = (0, -, 0, 1)$ then $x_{i+2} = 0$. This leads to the CL of κ

$$*011 \vee *01{-}0 \vee *0001.$$

This CL does appear in Table A.2 of Joan Daemen's thesis [3]. In [3] it is shown that κ is a permutation if n is odd and stated that it is invertible if and only if n is not a multiple of 6. The latter statement follows also from Lemma 8.

Next we apply the correspondence between permutations in G_n and the units in $\mathcal{M}_n$ to determine the inverse function of κ. For that we describe the inverse of $[1 + X + X^2]$ in $\mathbb{F}_2[X]/(m(X))$, where

$$m(X) = \begin{cases} X^{(n+1)/2} & \text{if } n \text{ is odd} \\ X^n + X^{n/2} & \text{if } n \text{ is even.} \end{cases}$$

Recall that for any $k \geq 1$ it holds

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

We denote by $P_0(x) = 0$ and for $k \geq 1$ by $P_{3k}(X)$ the polynomial

$$P_{3k}(X) := \frac{1+X^{3k}}{1+X+X^2}.$$

Note, that

$$P_{3k}(X) = (1+X)(1+X^3+\ldots+X^{3(k-1)}) = \sum_{i=0}^{3(k-1)+1} a_i X^i,$$

where $a_i = 0$ if and only if $i = 2 \bmod 3$. Observe that $P_{3k}(X)$ has degree $3k-2$.

The next lemma determines the inverse of $[1+X+X^2]$ for n odd. In particular it shows that for $n = 5$ we have $\kappa^{-1} = \chi$.

Lemma 9. *Let $n \geq 1$ be odd and k be minimal such that $3k \geq (n+1)/2$, that is*

$$k = \begin{cases} \frac{n+5}{6} & \text{if } n = 1 \bmod 6 \\ \frac{n+3}{6} & \text{if } n = 3 \bmod 6 \\ \frac{n+1}{6} & \text{if } n = 5 \bmod 6. \end{cases}$$

The inverse of $[1+X+X^2]$ in $\mathbb{F}_2[X]/(X^{(n+1)/2})$ is

$$[1+X+X^2]^{-1} = [P_{3k}(X)] = \begin{cases} [P_{3k}(X)] & \text{if } n = 3,5 \bmod 6 \\ [P_{3k}(X) - X^{3k-2}] & \text{if } n = 1 \bmod 6. \end{cases}$$

Proof. Note that

$$\left[1+X+X^2\right]\left[P_{3k}(X)\right] = \left[X^{3k}+1\right] = [1],$$

since $3k \geq (n+1)/2$. It remains to observe that the degree of P_{3k} is less than $(n+1)/2$ if $n = 3,5 \bmod 6$. If $n = 1 \bmod 6$, then $\deg P_{3k}(X) = 3k-2 = 3 \cdot \frac{n+5}{6} - 2 = \frac{n+1}{2}$, so that the highest degree term in $[P_{3k}(X)]$ vanishes modulo $X^{(n+1)/2}$. □

The inverse of $[1+X+X^2]$ for n even is as follows:

Lemma 10. *Let $n \geq 2$ be even and not a multiple of 6. The inverse of $[1+X+X^2] \in \mathbb{F}_2[X]/(X^n + X^{n/2})$ is*

$$[1+X+X^2]^{-1} = \begin{cases} [1+XP_{3k}(X)+X^2P_{6k}(X)] & \text{if } n = 6k+2 \\ [1+X^2P_{3k}(X)+XP_{6k+3}(X)] & \text{if } n = 6k+4. \end{cases}$$

n	coefficients of $[1+X+X^2]^{-1}$
8	1101011
10	110111011
14	1101101011011
16	110110111011011

Table 1: Coefficients of $[1+X+X^2]^{-1}$ for n even. As an example, for $n=8$ the inverse is given by $[1+X+0X^2+X^3+0X^4+X^5+X^6]$.

Proof. We consider only $n=6k+2$ for some $k\in\mathbb{N}$, since the other case is analogous. We have

$$\begin{aligned}1+X^n+X^{n/2} &= 1+X+X^2+X^{6k+2}+X^2+X^{3k+1}+X\\ &= 1+X+X^2+X^2(X^{6k}+1)+X(X^{3k}+1)\\ &= 1+X+X^2+X^2(1+X+X^2)P_{6k}(X)+X(1+X+X^2)P_{3k}(X)\\ &= (1+X+X^2)(1+X^2P_{6k}(X)+XP_{3k}(X))\end{aligned}$$

from which the claim follows. □

If n is even, the sequence of the coefficients a_i of $[1+X+X^2]^{-1}=[\sum_{i=0}^{k}a_iX^i]$ has an interesting pattern as can be seen from Table 1. The coefficients yield a palindrome starting with a repeating pattern of 110, ending with a repeating pattern of 011 and meeting in the middle with either 01110 or 010, depending on $n=1,2 \mod 3$.

We summarize our observations on κ the following theorem.

Theorem 4. *Let $n\geq 4$. The map $\kappa=\gamma_0+\gamma_2+\gamma_4$ is a permutation on $\mathbb{F}_2^n$ if and only if n is not a multiple of 6. The inverse κ^{-1} is given by $\psi([1+X+X^2]^{-1})$ described in Lemmas 9 and 10. The algebraic degree of κ is 3 and the algebraic degree d of κ^{-1} is*

$$d=\begin{cases}n/2+1 & \text{if } n=0,2,4 \bmod 6\\ (n+1)/2 & \text{if } n=1,3 \bmod 6\\ (n-1)/2 & \text{if } n=5 \bmod 6\end{cases}$$

Proof. The statement follows from Lemmas 8 to 10. The algebraic degree of γ_{2k} is given in Lemma 4 for n even and in [10, Lemma 2] for n odd. □

Our numerical results show that the cryptographic properties of κ are comparable with those of χ. In particular, our computations for small values of n yield the following open question.

Open Problem 1. For any $n\geq 5$ the differential uniformity of κ on $\mathbb{F}_2^n$ is $2^{n-2}-2^{n-5}$.

The differential uniformity of χ on $\mathbb{F}_2^n$ is 2^{n-2} which has been known for a long time [3]. However, to the best of our knowledge, all published proofs of this fact are recent, see [19, 7].

References

[1] Andreoli, S., Leander, G., Piccione, E., Stennes, L.: Generalizations of chichi: Families of low-latency permutations in any even dimension. IACR Transactions on Symmetric Cryptology **2025**(3), 800–826 (2025)

[2] Belkheyar, Y., Derbez, P., Ghosh, S., Leander, G., Mella, S., Perrin, L., Rasoolzadeh, S., Stennes, L., Sun, S., Assche, G.V., Vizár, D.: Chilow and chichi: New constructions for code encryption. Springer-Verlag (2025)

[3] Daemen, J.: Cipher and hash function design strategies based on linear and differential cryptanalysis. Ph.D. thesis, Doctoral Dissertation, March 1995, KU Leuven (1995)

[4] Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon v1. 2: Lightweight authenticated encryption and hashing. Journal of Cryptology **34**, 1–42 (2021). https://doi.org/10.1007/s00145-021-09398-9

[5] Evoyan, M.G., Kyuregyan, G.M., Kyuregyan, M.K.: On k-switching of mappings on finite fields. Mathematical Problems of Computer Science **39**, 5–12 (2013)

[6] Graner, A.M.: Irreducible polynomials over finite fields for coding and cryptography. Ph.D. thesis, Dissertation, Rostock, Universität Rostock, 2024 (2024)

[7] Graner, A.M., Kriepke, B., Krompholz, L., Kyureghyan, G.: On the bijectivity of the map χ. Cryptography and Communications pp. 1–9 (2025)

[8] Kari, J.: Theory of cellular automata: A survey. Theoretical computer science **334**(1-3), 3–33 (2005)

[9] Kim, K., Namgoong, J., Yie, I.: Groups of permutations generated by function–linear translator pairs. Finite Fields and Their Applications **45**, 170–182 (2017)

[10] Kriepke, B., Kyureghyan, G.: Algebraic structure of the iterates of χ. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology – CRYPTO 2024. pp. 412–424. Springer Nature Switzerland, Cham (2024)

[11] Kyureghyan, G.M.: Constructing permutations of finite fields via linear translators. Journal of Combinatorial Theory, Series A **118**(3), 1052–1061 (2011)

[12] Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press (1997)

[13] Liu, F., Dixit, V., Sarkar, S., Meier, W., Isobe, T.: Finding the inverse of some shift invariant transformations. Cryptology ePrint Archive (2025)

[14] Liu, F., Sarkar, S., Meier, W., Isobe, T.: The inverse of χ and its applications to rasta-like ciphers. Journal of Cryptology **35**(4), 28 (2022). https://doi.org/10.1007/s00145-022-09439-x

[15] Lyu, C., Yuan, M., Zheng, D., Sun, S., Li, S.: A generalized χ_n-function. arXiv preprint arXiv:2509.20880 (2025)

[16] NIST: SHA-3 standard: Permutation-based hash and extendable-output functions. Tech. Rep. Federal Information Processing Standard (FIPS) 202, U.S. Department of Commerce (Aug 2015). https://doi.org/10.6028/NIST.FIPS.202

[17] Omland, T., Stanica, P.: Permutation rotation-symmetric s-boxes, liftings and affine equivalence (2022), `https://arxiv.org/abs/2203.00778`

[18] Qin, X., Qian, G., Hong, S.: New results on permutation polynomials over finite fields. International Journal of Number Theory **11**(02), 437–449 (2015)

[19] Schoone, J., Daemen, J.: Algebraic properties of the maps χ n. Designs, Codes and Cryptography **92**(8), 2341–2365 (2024). https://doi.org/10.1007/s10623-024-01395-w

[20] Schoone, J., Daemen, J.: The state diagram of χ. Designs, Codes and Cryptography **92**(5), 1393–1421 (2024). https://doi.org/10.1007/s10623-023-01349-8

[21] Toffoli, T., Margolus, N.H.: Invertible cellular automata: a review. Physica D: Nonlinear Phenomena **45**(1-3), 229–253 (1990)