A Generalized χ_n-Function

Cheng Lyu, Mu Yuan, Dabin Zheng, Siwei Sun, and Shun Li

***Abstract*—The mapping χ_n from $\mathbb{F}_2^n$ to itself defined by $y = \chi_n(x)$ with $y_i = x_i + x_{i+2}(1 + x_{i+1})$, where the indices are computed modulo n, has been widely studied for its applications in lightweight cryptography. However, χ_n is bijective on $\mathbb{F}_2^n$ only when n is odd, restricting its use to odd-dimensional vector spaces over $\mathbb{F}_2$. To address this limitation, we introduce and analyze the generalized mapping $\chi_{n,m}$ defined by $y = \chi_{n,m}(x)$ with $y_i = x_i + x_{i+m}(x_{i+m-1} + 1)(x_{i+m-2} + 1) \cdots (x_{i+1} + 1)$, where m is a fixed integer with $m \nmid n$. To investigate such mappings, we further generalize $\chi_{n,m}$ to $\theta_{m,k}$, where $\theta_{m,k}$ is given by $y_i = x_{i+mk} \prod_{j=1,\ m\nmid j}^{mk-1} (x_{i+j} + 1)$, for $i \in \{0, 1, \ldots, n-1\}$. We prove that these mappings generate an abelian group isomorphic to the group of units in $\mathbb{F}_2[z]/(z^{\lfloor n/m \rfloor + 1})$. This structural insight enables us to construct a broad class of permutations over $\mathbb{F}_2^n$ for any positive integer n, along with their inverses. We rigorously analyze algebraic properties of these mappings, including their iterations, fixed points, and cycle structures. Additionally, we provide a comprehensive database of the cryptographic properties for iterates of $\chi_{n,m}$ for small values of n and m. Finally, we conduct a comparative security and implementation cost analysis among $\chi_{n,m}$, χ_n, χ_n (EUROCRYPT 2025 [3]) and their variants, and prove Conjecture 1 proposed in [3] as a by-product of our study. Our results lead to generalizations of χ_n, providing alternatives to χ_n and χ_n.**

***Index Terms*—Permutation, S-boxes, χ_n**

I. Introduction

In order to find a shift-invariant transformation over $\mathbb{F}_2^n$ that is easy to implement and has good cryptographic properties, Joan Daemen in [9] introduced a mapping $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, $x \mapsto y$ defined by $y_i = x_i + (x_{i+1} + 1)x_{i+2}$, where the indices are computed modulo n. Due to its compactness and favorable cryptographic properties, χ_n has been used in several prominent cryptographic algorithms, including KECCAK-f [4] (part of the NIST standard SHA-3 [22]) and Ascon [11] (the NIST standard for lightweight cryptography [24]).

Recent years have witnessed significant progress in the study of the mapping χ_n, with notable advancements in both cryptanalytic and algebraic domains. From a cryptanalytic perspective, Daemen et al. in [10] and Mella et al. in [17] conducted comprehensive investigations into the differential and linear propagation properties of χ_n, respectively. On the algebraic front, Biryukov et al. in [6] pioneered the analysis of the algebraic degree of the inverse mapping χ_n^{-1} of χ_n, demonstrating its resilience against meet-in-the-middle attacks. This foundational work was further extended by Liu et al. in [15], who derived an explicit algebraic expression for χ_n^{-1}. Schoone and Daemen in [21] explored the order and cycle structure of χ_n, while their subsequent research [20] investigated it as a polynomial mapping, leading to the conjecture that χ_n does not act as a bijection of a vector space over any extension field of $\mathbb{F}_2$. This conjecture was later rigorously proven by Graner et al. in [12], who established that the mapping $\chi_n \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a permutation if and only if $q = 2$ and n is odd. These contributions collectively deepen the understanding of χ_n and its cryptographic implications.

A significant advance in understanding the algebraic structure of χ was achieved very recently by Kriepke and Kyureghyan [13]. They observed that all iterates of χ_n can be expressed as linear combinations of the mappings γ_{2k} for $k \geq 1$, where the i-th coordinate of the output is given by

$$y_i = x_{i+2k}(x_{i+2k-1} + 1)(x_{i+2k-3} + 1) \cdots (x_{i+1} + 1)$$

for $i \in \{0, 1, \cdots, n-1\}$. Based on this observation, the authors conducted a systematic study of the set Γ spanned by these γ_{2k}, with a particular focus on its subset G consisting of elements invertible under composition. They creatively used Hadamard product and shift operators to represent vector Boolean functions, and then established a correspondence between the functional iteration of χ_n and polynomial multiplication in $\mathbb{F}_2[z]/(z^{(n+1)/2})$ when n is odd, which allows the algebraic properties of χ_n to be clearly characterized. This represents a fundamental breakthrough in the research methodology. The significance of their work lies not only in elegantly elucidating the algebraic structure and properties of the χ-function itself, but also in leveraging this clear correspondence with polynomial quotient rings to generate a broader family of permutation classes in a unified and efficient method. Along the line of [13], we investigate a broader family of permutations.

Note that χ_n is a bijection on $\mathbb{F}_2^n$ if and only if n is odd. To address this limitation and extend bijective capabilities to even dimensions, we introduce a generalized mapping class, denoted by $\chi_{n,m}$. This mapping $\chi_{n,m} \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as $y = \chi_{n,m}(x)$, where the i-th coordinate of y is represented as

$$y_i = x_i + x_{i+m}(x_{i+m-1} + 1)(x_{i+m-2} + 1) \cdots (x_{i+1} + 1) \quad (1)$$

for $m \geq 2$ and $i \in \{0, 1, \ldots, n-1\}$. Crucially, $\chi_{n,m}$ acts as a bijection on $\mathbb{F}_2^n$ if and only if $m \nmid n$, thereby enabling its application to both odd and even dimension vector spaces over

C. Lyu, M. Yuan, D. Zheng are with Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University. Dabin Zheng is also with Key Laboratory of Intelligent Sensing System and Security (Hubei University), Ministry of Education, Wuhan, 430062, China. E-mail: chenglyu@139.com; yuanmu847566@outlook.com; dzheng@hubu.edu.cn. S. Sun and S. Li are with School of Cryptology, University of Chinese Academy of Sciences, Beijing 100049, China. S. Sun is also with State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, China. E-mail: sunsiwei@ucas.ac.cn; lishun@ucas.ac.cn. The corresponding author is Dabin Zheng. The research was supported in part by the China National Key Research and Development Program under Grant 2021YFA1000600, and in part by the National Nature Science Foundation of China (NSFC) under Grants 62272148, 12301671, 62532013, 62502494, and in part by the National Cryptologic Science Foundation of China (2025NCSF01012), the Fundamental Research Funds for the Central Universities and the Scientific Research Innovation Capability Support Project for Young Faculty, and in part by China Postdoctoral Science Foundation 2024M763221.

$\mathbb{F}_2$. We note that some instances of $\chi_{n,m}$ have been studied previously. For example, $\chi_{n,3}$ and $\chi_{n,4}$ are listed in Table A.1 of Daemen's thesis. Liu et al. [14] further investigate the compositional inverses for a class of shift-invariant transformations that includes $\chi_{n,3}$ and $\chi_{n,4}$ as subcases, providing an effective method applicable to the transformation used in `Monolith`. In contrast, our results establish a unified algebraic framework for the whole parametric family $\chi_{n,m}$, addressing not only the compositional inverse but also deriving further algebraic properties such as explicit expressions for their iterates.

Building on the approach in [13], we generalize γ_{2k} in [13] to $\theta_{m,k}$. We will demonstrate that these mappings $\theta_{m,k}$ generate a linear space Θ over $\mathbb{F}_2$, and that the coset $\theta_0 + \Theta$ forms an abelian group under composition, where θ_0 represents the identity mapping. This construction yields a broad class of bijective mappings of $\mathbb{F}_2^n$, including $\chi_{n,m}$. Leveraging this algebraic structure, we derive some results on the cycle structure, algebraic degree, compositional inverse, and fixed points of the compositional iterates of $\chi_{n,m}$. Notably, χ_n emerges as a special case of $\chi_{n,m}$ when $m = 2$, and our findings significantly extend previously known results. Furthermore, while χ_n is an involution on $\mathbb{F}_2^n$ only when $n = 1, 3$, involutory mappings $\chi_{n,m}$ exist even for larger n.

Recently, a variant permutation of χ_n on even-dimensional vector spaces $\mathbb{F}_2^{2k}$ has been introduced by Belkheyar et. al. in [3], named ChiChi or $\chi\!\!\chi_{2k}$, defined as follows:

$$y_i = \begin{cases} x_i + \overline{x}_{i+1}x_{i+2}, & i < k-3 \text{ or } k < i < 2k-2, \\ x_k + \overline{x}_{k-2}x_0, & i = k-3, \\ x_{k-1} + \overline{x}_0 x_1, & i = k-2, \\ \overline{x}_{k-3} + \overline{x}_k\,\overline{x}_{k+1}, & i = k-1, \\ x_{k-2} + \overline{x}_{k+1}x_{k+2}, & i = k, \\ x_{2k-2} + \overline{x}_{2k-1}x_{k-1}, & i = 2k-2, \\ x_{2k-1} + \overline{x}_{k-1}x_k, & i = 2k-1, \end{cases} \tag{2}$$

where $\bar{x}_i := x_i + 1$ for $i \in \{0, 1, \ldots, 2k-1\}$, and k is even. Note that $\chi\!\!\chi_{2k}$ is extended affine (EA) equivalent to the concatenation of χ_{k-1} and χ_{k+1}, denoted by $\chi_{k-1} \parallel \chi_{k+1}$. ChiChi serves as the core primitive in ChiLow, which constitutes a family of tweakable block ciphers along with an associated pseudorandom function (PRF) specifically designed for embedded code encryption.

We conduct a comprehensive comparative analysis of $\chi_{n,m}$, χ_n, $\chi\!\!\chi_n$ regarding cryptographic security and implementation costs for small parameter values. We prove Conjecture 1 in [3] which determines the algebraic degree of $\chi\!\!\chi_n^{-1}$ as a by-product. As a concurrent work, Samuele et al. ([1, Theorem 4]) also independently arrived at a proof of the conjecture(see Remark 2). Our result shows that $\chi_{n,m}$ has a higher algebraic degree than that of χ_n and $\chi\!\!\chi_n$, and the inverse of $\chi_{n,m}$ also has a higher algebraic degree than that of χ_n and $\chi\!\!\chi_n$. Nevertheless, implementation cost analysis reveals comparable hardware requirements among χ_n, $\chi\!\!\chi_n$, and a modified $\chi_{n,3}$-variant. Tables I-IV present detailed comparisons of critical security metrics including differential uniformity, nonlinearity, boomerang uniformity, and differential-linear uniformity of $\chi_{n,3}, \chi_n$, and $\chi\!\!\chi_n$ for $n = 5, 6, 8$. The data demonstrates a nuanced tradeoff: while our proposed functions exhibit superior performance in certain security indicators (e.g., boomerang/differential-linear resistance), they show slight disadvantages in others (notably differential uniformity and nonlinearity). These findings confirm our construction as a viable alternative to χ_n and $\chi\!\!\chi_n$ for odd- and even-dimensional vector spaces, respectively. We anticipate that this expanded design space will enhance flexibility in cryptographic algorithm development, particularly for resource-constrained applications.

The remainder of this paper is organized as follows. Section II introduces the necessary preliminaries and notations. Section III investigates the properties of the mappings $\theta_{m,k}$ and constructs an abelian group $G_{n,m}$ comprising invertible mappings from $\mathbb{F}_2^n$ to itself. Section IV applies these theoretical insights to analyze specific mappings within $G_{n,m}$, including $\chi_{n,m}$. Section V provides a database detailing cryptographic properties of the compositional iterates of $\chi_{n,m}$ and conducts a comparative security and implementation cost analysis for small values of n and m. Section VI concludes this paper.

II. Notations and preliminaries

Let $\mathcal{M}_n$ denote the set of all mappings from $\mathbb{F}_2^n$ to itself, and let $S \in \mathcal{M}_n$ be the cyclic left shift operator over $\mathbb{F}_2^n$, defined as $S(x_0, x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, x_0)$. It is straightforward to verify that S is an invertible linear mapping. For $i \geq 0$, let $S^i = \underbrace{S \circ S \circ \cdots \circ S}_{i}$ denote the i-th iterate of S, with S^0 representing the identity mapping on $\mathbb{F}_2^n$. In order to generate a nonlinear mapping over $\mathbb{F}_2^n$ from the shift operator S, recall the Hadamard product $\odot$ over $\mathbb{F}_2^n$ as follows: $x \odot y := (x_0y_0, x_1y_1, \ldots, x_{n-1}y_{n-1})$, where $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_2^n$. It is easy to see that the Hadamard product $\odot$ is commutative and distributive with respect to addition, i.e., $x \odot y = y \odot x$ and $x \odot (y + z) = x \odot y + x \odot z$ for all $x, y, z \in \mathbb{F}_2^n$. In particular, $x \odot x = x$ and $x \odot (\mathbf{1} + x) = \mathbf{0}$, where $\mathbf{1} = (1, 1, \cdots, 1)$ and $\mathbf{0} = (0, 0, \cdots, 0)$ are the all-one and all-zero vectors in $\mathbb{F}_2^n$, respectively.

Furthermore, we formally extend the Hadamard product to the set $\mathcal{M}_n$ as follows:

$$\begin{aligned} &\mathcal{M}_n \times \mathcal{M}_n \to \mathcal{M}_n \\ &(f, g) \mapsto f \odot g, \text{ where } (f \odot g)(x) = f(x) \odot g(x) \end{aligned}$$

for $x \in \mathbb{F}_2^n$. More precisely, let the i-th coordinate functions of f and g be f_i and g_i respectively, then the i-th coordinate functions of $f \odot g$ is represented as

$$(f \odot g)_i(x) = f_i(x) \cdot g_i(x)$$

for $i \in \{0, 1, \ldots, n-1\}$. The set $\mathcal{M}_n$ is equipped with three fundamental operations: addition ($+$), composition ($\circ$), and Hadamard product ($\odot$) of mappings over $\mathbb{F}_2^n$. For any $f, g, h \in \mathcal{M}_n$, it is straightforward to verify that $f \odot (f + \mathbf{1}) = \mathbf{0}$. Moreover, these operations satisfy the following algebraic properties:

The composition $\circ$ is right distributive with respect to $+$ and $\odot$, i.e.,

$$(f + g) \circ h = f \circ h + g \circ h, \;\; (f \odot g) \circ h = (f \circ h) \odot (g \circ h).$$

The Hadamard product $\odot$ is commutative, associative and distributive with respect to addition, i.e.,

$$f \odot g = g \odot f,\ (f \odot g) \odot h = f \odot (g \odot h),$$
$$f \odot (g + h) = f \odot g + f \odot h.$$

Note that the left shift operator S is distributive with respect to $+$ and $\odot$, i.e.,

$$(f \odot g) \circ S = (f \circ S) \odot (g \circ S),$$
$$S \circ (f \odot g) = (S \circ f) \odot (S \circ g),$$
$$(f + g) \circ S = (f \circ S) + (g \circ S),$$
$$S \circ (f + g) = (S \circ f) + (S \circ g).$$

To analyze the mapping $\chi_{n,m}$ introduced in (1), we define a key mapping $\theta_{m,k} \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ as follows:

$$\theta_{m,k}(x_0, x_1, \ldots, x_{n-1}) = (y_0, y_1, \ldots, y_{n-1}), \tag{3}$$

where m and k are nonnegative integers with $m \nmid n$, and the i-th coordinate of the output is given by

$$y_i = x_{i+mk} \prod_{j=1,\ m\nmid j}^{mk-1} (x_{i+j} + 1)\,,\ \text{for } i \in \{0, 1, \ldots, n-1\}.$$

This mapping can be compactly expressed using the shift operator S and the Hadamard product as

$$\theta_{m,k} = S^{mk} \bigodot_{j=1,\ m\nmid j}^{mk-1} (S^j + \mathbf{1}),$$

where $\mathbf{1} = (1, 1, \ldots, 1) \in \mathbb{F}_2^n$. Note that the function $\theta_{2,k}$ is a generalization of γ_{2k} in [13]. This formulation illustrates the interplay between the shift operator and the Hadamard product in constructing nonlinear mappings over $\mathbb{F}_2^n$.

III. Algebraic structure of the set associated with $\theta_{m,k}$

In this section, we investigate the vector space generated by $\theta_{m,k}$ over $\mathbb{F}_2$ for $k \in \left[\left\lfloor \frac{n}{m} \right\rfloor\right]$, as well as the associated abelian group, where m is a fixed positive integer satisfying $m \nmid n$. To this end, we first establish some fundamental properties of $\theta_{m,k}$.

Lemma 3.1: If $mk > n$, then $\theta_{m,k} = \mathbf{0}$, i.e., $\theta_{m,k}(x) = \mathbf{0}$ for any $x \in \mathbb{F}_2^n$.

Proof: Assume $mk > n$. By the periodicity of the shift operator S, we have $S^{mk} = S^{mk-n}$. Since $m \nmid n$, it follows that $m \nmid (mk - n)$. Consequently, the expression for $\theta_{m,k}$ includes a term of the form $(S^{mk-n} + \mathbf{1})$. Utilizing the properties of the shift operator S and the Hadamard product, we derive that

$$\begin{aligned}\theta_{m,k} &= S^{mk} \bigodot_{i=1,\ m\nmid i}^{mk-1} (S^i + \mathbf{1}) \\ &= S^{mk-n} \odot (S^{mk-n} + \mathbf{1}) \bigodot_{\substack{i=1 \\ m\nmid i \text{ and } i\neq mk-n}}^{mk-1} (S^i + \mathbf{1}) \\ &= \mathbf{0}.\end{aligned}$$

The last equality follows from the fact that

$$S^{mk-n} \odot (S^{mk-n} + \mathbf{1}) = \mathbf{0}.$$

■

Lemma 3.1 immediately leads to the following corollary.

Corollary 3.2: Let $\ell = \left\lfloor \frac{n}{m} \right\rfloor$. Then $k = \ell + 1$ is the smallest integer for which $\theta_{m,k} = \mathbf{0}$.

It is important to note that for $1 \le i \le \ell$, the mappings $\theta_{m,i}$ are constructed as the Hadamard product of certain linear mappings, resulting in nonlinear mappings over $\mathbb{F}_2^n$. Recall that the algebraic degree of a mapping from $\mathbb{F}_2^n$ to itself is defined as the maximum multivariate degree of its component functions.

Lemma 3.3: Let $\theta_{m,0} = \theta_0$ denote the identity mapping from $\mathbb{F}_2^n$ to itself, and $\ell = \left\lfloor \frac{n}{m} \right\rfloor$. Then $\deg(\theta_{m,k}(x)) = (m-1)k + 1$ for $0 \le k \le \ell$. In particular, the mappings $\theta_{m,0}, \theta_{m,1}, \cdots, \theta_{m,\ell}$ are linearly independent over $\mathbb{F}_2$, and thus $\Theta_{n,m} \colon = \left\{ \sum_{k=0}^{\ell} a_k \theta_{m,k} \colon a_k \in \mathbb{F}_2 \right\}$ forms a vector space over $\mathbb{F}_2$ of dimension $\ell + 1$.

Proof: For $k \ge 1$, the entries of $\theta_{m,k}(x)$ are defined by

$$y_i = x_{i+mk} \prod_{j=1,\ m\nmid j}^{mk-1} (x_{i+j} + 1)\,.$$

Since all variables x_i appearing in the product are distinct, it follows that $\deg(\theta_{m,k}(x)) = (m-1)k + 1$. Consequently, the mappings $\theta_{m,1}, \theta_{m,2}, \cdots, \theta_{m,\ell}$ are linearly independent over $\mathbb{F}_2$. ■

From Lemma 3.3 we know that $\theta_0, \theta_{m,1}, \cdots, \theta_{m,\ell}$ are linearly independent over $\mathbb{F}_2$. To construct a group comprising invertible mappings on $\mathbb{F}_2^n$, we define a set

$$G_{n,m} = \left\{ \theta_0 + \sum_{k=1}^{\ell} a_k \theta_{m,k} \colon a_k \in \mathbb{F}_2 \right\} \subseteq \Theta_{n,m}, \tag{4}$$

where m is a fixed number with $m \nmid n$ and $\ell = \left\lfloor \frac{n}{m} \right\rfloor$. Next we will show that the set $G_{n,m}$ forms a monoid under composition. Recall that a *monoid* $(\mathcal{G}, *)$ is a set $\mathcal{G}$ equipped with an associative binary operation $*$ and a neutral element with respect to $*$. A monoid in which every element has an inverse element is called a *group*. To establish this result, we require the following key lemma.

Lemma 3.4: Let m, t be integers with $m \mid t$, and let $[m]$ denote the set $\{1, 2, \ldots, m-1\}$ and $f = \sum_{i=0}^{k} a_i \theta_{m,i}$, $g = \theta_0 + \sum_{j=1}^{s} b_j \theta_{m,j}$, where $a_i, b_j \in \mathbb{F}_2$. Then,

$$(S^t \circ f) \bigodot_{v\in[m]} (S^{t-v} \circ g + \mathbf{1}) = S^{t-m} \circ \left(\sum_{i=0}^{k} a_i \theta_{m,(i+1)} \right). \tag{5}$$

Proof: Let $g_0 = \sum_{j=1}^{s} b_j \theta_{m,j}$. We begin by expanding

the left-hand side of (5):

$$\begin{aligned}
&(S^t\circ f)\bigodot_{v\in[m]}\left(S^{t-v}\circ g+\mathbf{1}\right)\\
&=(S^t\circ f)\bigodot_{v\in[m]}\left(S^{t-v}\circ\theta_0+\mathbf{1}+S^{t-v}\circ g_0\right)\\
&=(S^t\circ f)\Bigg(\bigodot_{v\in[m]}(S^{t-v}\circ\theta_0+\mathbf{1})+\\
&\sum_{\emptyset\neq V\subseteq[m]}\bigodot_{u\in V}(S^{t-u}\circ g_0)\bigodot_{w\in[m]\setminus V}(S^{t-w}\circ\theta_0+\mathbf{1})\Bigg)\\
&=(S^t\circ f)\bigodot_{v\in[m]}\left(S^{t-v}+\mathbf{1}\right)+\\
&\sum_{\emptyset\neq V\subseteq[m]}\Bigg(\bigodot_{u\in V}(S^t\circ f)\odot(S^{t-u}\circ g_0)\\
&\qquad\bigodot_{w\in[m]\setminus V}\left(S^{t-w}\circ\theta_0+\mathbf{1}\right)\Bigg).
\end{aligned}\tag{6}$$

Next, we will show that for any $v\in[m]$,

$$\begin{aligned}
&(S^t\circ f)\odot(S^{t-v}\circ g_0)\\
=&\sum_{i=0}^{k}a_i(S^t\circ\theta_{m,i})\odot\sum_{j=1}^{s}b_j(S^{t-v}\circ\theta_{m,j})\\
=&\mathbf{0}.
\end{aligned}$$

To see this, observe that:

$$S^{t-v}\circ\theta_{m,j}=S^{mj+t-v}\bigodot_{\substack{u=1\\ m\nmid u}}^{mj-1}\left(S^{t-v+u}+\mathbf{1}\right).$$

and

$$\begin{aligned}
S^t\circ\theta_{m,i}&=S^t\circ\left(S^{mi}\bigodot_{\substack{u=1\\ m\nmid u}}^{mi-1}(S^u+\mathbf{1})\right)\\
&=S^{mi+t}\bigodot_{\substack{u=1\\ m\nmid u}}^{mi-1}(S^{t+u}+\mathbf{1}).
\end{aligned}$$

Since $v\in[m]$, we have $mj+t-v\geq t+1$ and $mi+t\geq t-v+1$. If $mj-v<mi$, then $t+1\leq mj+t-v<mi+t$. Since $mj-v\not\equiv 0\pmod m$, the term $(S^{mj+t-v}+\mathbf{1})$ must appear in the expression of $S^t\circ\theta_{m,i}$. Since $S^{mj+t-v}\odot(S^{mj+t-v}+\mathbf{1})=\mathbf{0}$, we conclude that $(S^t\circ\theta_{m,i})\odot(S^{t-v}\circ\theta_{m,j})=\mathbf{0}$. Similarly, if $mj-v>mi$, the same result holds. Thus, $(S^t\circ f)\odot(S^{t-v}\circ g_0)=\mathbf{0}$ for all $v\in[m]$. Consequently, by the properties of the operations introduced in Section II, (6) can be reduced to

$$\begin{aligned}
&(S^t\circ f)\bigodot_{v\in[m]}\left(S^{t-v}\circ g+\mathbf{1}\right)=(S^t\circ f)\bigodot_{v\in[m]}\left(S^{t-v}+\mathbf{1}\right)\\
=&\sum_{i=0}^{k}a_i\left(S^t\circ\theta_{m,i}\right)\bigodot_{v\in[m]}\left(S^{t-v}+\mathbf{1}\right)\\
=&\sum_{i=0}^{k}a_iS^t\circ\left(S^{mi}\bigodot_{\substack{j=1\\ m\nmid j}}^{mi-1}(S^j+\mathbf{1})\right)\bigodot_{v\in[m]}\left(S^{t-m}\circ\left(S^{m-v}+\mathbf{1}\right)\right)\\
=&\sum_{i=0}^{k}a_iS^{t-m}\circ\left(S^{mi+m}\bigodot_{\substack{j=1\\ m\nmid j}}^{mi-1}(S^{m+j}+\mathbf{1})\right)\\
&\qquad\bigodot_{v\in[m]}\left(S^{t-m}\circ\left(S^{m-v}+\mathbf{1}\right)\right)\\
=&\sum_{i=0}^{k}a_iS^{t-m}\circ\left(S^{mi+m}\bigodot_{\substack{j=m+1\\ m\nmid j}}^{m(i+1)-1}(S^j+\mathbf{1})\bigodot_{v\in[m]}(S^v+\mathbf{1})\right)\\
=&\sum_{i=0}^{k}a_iS^{t-m}\circ\left(S^{mi+m}\bigodot_{\substack{j=1\\ m\nmid j}}^{m(i+1)-1}(S^j+\mathbf{1})\right)\\
=&\sum_{i=0}^{k}a_iS^{t-m}\circ\theta_{m,(i+1)}.
\end{aligned}$$

■

Based on this lemma, we can show that the set $G_{n,m}$ introduced in (4) forms a monoid under the composition of mappings from $\mathbb{F}_2^n$ to itself.

Theorem 3.5: Let $f,g\in G_{n,m}$, then $f\circ g\in G_{n,m}$. In particular, $(G_{n,m},\circ)$ is a monoid.

Proof: Let $f=\theta_0+\sum_{i=1}^{\ell}a_i\theta_{m,i}$ and $g=\theta_0+\sum_{j=1}^{\ell}b_j\theta_{m,j}$ and $\ell=\lfloor\frac{n}{m}\rfloor$. Then we have

$$\begin{aligned}
f\circ g&=\left(\theta_0+\sum_{i=1}^{\ell}a_i\theta_{m,i}\right)\circ g=g+\left(\sum_{i=1}^{\ell}a_i\theta_{m,i}\right)\circ g\\
&=\theta_0+\sum_{j=1}^{\ell}b_j\theta_{m,j}+\sum_{i=1}^{\ell}a_i\left(\theta_{m,i}\circ g\right).
\end{aligned}\tag{7}$$

Let $g_k:=\sum_{j=0}^{\ell}b_j\theta_{m,(j+k)}$ with $b_0=1$. We have

$$
\begin{aligned}
&(S^{m(i-k)} \circ g_k) \bigodot_{\substack{v=1 \\ m\nmid v}}^{m(i-k)-1} (S^v \circ g + \mathbf{1}) \\
=&(S^{m(i-k)} \circ g_k) \bigodot_{\substack{v_1=1 \\ m\nmid v_1}}^{m-1} (S^{m(i-k)-v_1} \circ g + \mathbf{1}) \\
&\qquad \bigodot_{\substack{v_2=1 \\ m\nmid v}}^{m(i-k-1)-1} (S^{v_2} \circ g + \mathbf{1}) \\
=&\left(S^{m(i-k-1)} \circ \sum_{j=0}^{\ell} b_j \theta_{m,(j+k+1)} \right) \bigodot_{\substack{v_2=1 \\ m\nmid v}}^{m(i-k-1)-1} (S^{v_2} \circ g + \mathbf{1}) \\
=&\left(S^{m(i-k-1)} \circ g_{k+1} \right) \bigodot_{\substack{v=1 \\ m\nmid v}}^{m(i-k-1)-1} (S^v \circ g + \mathbf{1}),
\end{aligned} \tag{8}
$$

where the second equal sign is obtained by Lemma 3.4. By applying (8) repeatedly, we have

$$
\begin{aligned}
\theta_{m,i} \circ g &= \left(S^{mi} \bigodot_{\substack{v=1 \\ m\nmid v}}^{mi-1} (S^v + \mathbf{1}) \right) \circ g \\
&= \left(S^{mi} \circ g \right) \bigodot_{\substack{v=1 \\ m\nmid v}}^{mi-1} (S^v \circ g + \mathbf{1}) \\
&= \left(S^{m(i-1)} \circ g_1 \right) \bigodot_{\substack{v=1 \\ m\nmid v}}^{m(i-1)-1} (S^v \circ g + \mathbf{1}) \\
&= \left(S^{m(i-2)} \circ g_2 \right) \bigodot_{\substack{v=1 \\ m\nmid v}}^{m(i-2)-1} (S^v \circ g + \mathbf{1}) \\
&= \cdots = g_i = \sum_{j=0}^{\ell} b_j \theta_{m,(i+j)}.
\end{aligned} \tag{9}
$$

Then (7) becomes

$$
\begin{aligned}
f \circ g =& \theta_0 + \sum_{j=1}^{\ell} b_j \theta_{m,j} + \sum_{i=1}^{\ell} a_i \left(\theta_{m,i} \circ g \right) \\
=& \theta_0 + \sum_{j=1}^{\ell} b_j \theta_{m,j} + \sum_{i=1}^{\ell} a_i \sum_{j=0}^{\ell} b_j \theta_{m,(i+j)}.
\end{aligned}
$$

This shows that $f \circ g \in G_{n,m}$. It is easy to see that the neutral element of $G_{n,m}$ under the composition is θ_0. Therefore, $(G_{n,m}, \circ)$ is a monoid. ∎

In the following, we will prove that $(G_{n,m}, \circ)$ is an abelian group by demonstrating that $(G_{n,m}, \circ)$ is isomorphic to an abelian group. Consequently, $G_{n,m}$ defines a broad class of permutations of $\mathbb{F}_2^n$.

Let $\ell = \left\lfloor \frac{n}{m} \right\rfloor$. Consider the factor ring $R_\ell = \mathbb{F}_2[z]/(z^{\ell+1})$ and its unit group $R_\ell^* = (\mathbb{F}_2[z]/(z^{\ell+1}))^*$. Define the coset of f as $[f] = f + (z^{\ell+1})$, where $(z^{\ell+1})$ is the ideal generated by $z^{\ell+1}$ in $\mathbb{F}_2[z]$. Since $\mathbb{F}_2[z]$ is an Euclidean domain, we have $[f] \in R_\ell^*$ if and only if $\gcd(f(z), z^{\ell+1}) = 1$, which is equivalent to the constant term of f being 1. Moreover, polynomials in R_ℓ with a constant term of 1 constitute exactly half of R_ℓ. Thus, the following lemma is immediate.

Lemma 3.6: [13, Lemma 9] Let $f(z) \in \mathbb{F}_2[z]$, then $[f]$ is a unit of R_ℓ if and only if the constant term of f is 1. Furthermore, the unit group R_ℓ^* has 2^ℓ elements.

To show that $G_{n,m}$ is an abelian group, we define a mapping $\varphi \colon \Theta_{n,m} \to R_\ell$ as follows:

$$
\varphi\left(\sum_{i=0}^{\ell} a_i \theta_{m,i} \right) = \sum_{i=0}^{\ell} a_i z^i.
$$

It is a straighrforward verification that the mapping φ is well-defined. The following lemma demonstrates that φ is a monoid homomorphism.

Lemma 3.7: Let $f, g \in G_{n,m}$. Then $\varphi(f \circ g) = \varphi(f) \cdot \varphi(g)$. Consequently, the restriction of φ to G is a monoid homomorphism.

Proof: Let $f = \sum_{i=0}^{\ell} a_i \theta_{m,i}$ and $g = \sum_{i=0}^{\ell} b_i \theta_{m,i}$ be elements of $G_{n,m}$, where $a_0 = b_0 = 1$. By (9) we have

$$
\begin{aligned}
\varphi(\theta_{m,k} \circ g) &= \varphi\left(\sum_{i=0}^{\ell} b_i \theta_{m,(i+k)} \right) \\
&= \sum_{i=0}^{\ell} b_i z^{i+k} = z^k \cdot \sum_{i=0}^{\ell} b_i z^i = \varphi(\theta_{m,k}) \cdot \varphi(g).
\end{aligned}
$$

It is straightforward to show that φ is an additive homomorphism, so we have

$$
\begin{aligned}
\varphi(f \circ g) =& \varphi\left(\sum_{i=0}^{\ell} a_i \theta_{m,i} \circ g \right) = \sum_{i=0}^{\ell} a_i \varphi(\theta_{m,i} \circ g) \\
=& \sum_{i=0}^{\ell} a_i \varphi(\theta_{m,i}) \cdot \varphi(g) = \varphi(f) \cdot \varphi(g).
\end{aligned}
$$

It is clear that θ_0 is the neutral element of $G_{n,m}$ and $\varphi(\theta_0) = 1$ is the neutral element of R_ℓ^*. ∎

Based on Lemma 3.4, Theorem 3.5, and equation (9), specifically the relation $\psi_i \circ (\psi_0 + \sum_j a_j \psi_j) = \sum_j a_j \psi_{j+i}$ for $\psi_i = \theta_{m,i}$, which is structurally analogous to the framework in [13] with $\psi_i = \gamma_{2i}$, we obtain an isomorphism from the set $\{\psi_0 + \sum_j a_j \psi_j\}$ to the unit group of $\mathbb{F}_2[z]/(z^d)$. The algebraic structure of G can then be derived from this unit group, and all subsequent properties follow directly from the isomorphism.

Theorem 3.8: Let m, n be integers with $m \nmid n$. Then the set $G_{n,m}$ is an abelian group under the mapping composition, and it is isomorphic to R_ℓ^*.

Proof: By Lemma 3.7, the restriction of φ to $G_{n,m}$ is a monoid homomorphism. For any $f = [1 + \sum_{i=1}^{\ell} a_i z^i] \in R_\ell^*$, we have $f = \varphi(\theta_0 + \sum_{i=1}^{\ell} a_i \theta_{m,i})$, where $\theta_0 + \sum_{i=1}^{\ell} a_i \theta_{m,i} \in G_{n,m}$. Thus, φ is surjective from $G_{n,m}$ to R_ℓ^*. Moreover, since $|G_{n,m}| = |R_\ell^*| = 2^\ell$, φ is also bijective from $G_{n,m}$ to R_ℓ^*.

Therefore, $G_{n,m}$ is isomorphic to R_ℓ^*, and since R_ℓ^* is an abelian group, $G_{n,m}$ is also an abelian group. ∎

Remark 3.9: Every mapping $f \in G_{n,m}$ is a permutation of $\mathbb{F}_2^n$. To determine the compositional inverse of f, it suffices to compute the inverse of $\varphi(f)$ in R_ℓ, which is relatively straightforward.

Proposition 3.10: Let $f = \theta_0 + \sum_{i=1}^{\ell} a_i\theta_{m,i} \in G_{n,m}$. Then its compositional inverse is

$$f^{-1} = \theta_0 + \sum_{j=1}^{\ell} b_j\theta_{m,j},$$

where $b_1 = a_1$, $b_j = a_j + \sum_{\substack{u+v=j \\ u,v\in\{1,2,\ldots,j-1\}}} a_u b_v$ for $j \in \{2,3,\ldots,\ell\}$. Furthermore, f is an involution if and only if $a_i = 0$ for any $i \in \{1,2,\ldots,\lfloor \ell/2 \rfloor\}$, i.e., the lowest degree of the non-constant terms of f is at least $\lfloor \ell/2 \rfloor + 1$.

Proof: By Theorem 3.8, it suffices to find the multiplicative inverse of $\varphi(f) = \left[1 + \sum_{i=1}^{\ell} a_i z^i\right]$. Assume $\varphi(f^{-1}) = \left[1 + \sum_{j=1}^{\ell} b_j z^j\right]$. Then,

$$\begin{aligned} 1 =& \varphi(f)\cdot\varphi(f^{-1}) = \left[(1+\sum_{i=1}^{\ell} a_i z^i)(1+\sum_{j=1}^{\ell} b_j z^j)\right] \\ \equiv& \left[1 + \sum_{i=1}^{\ell} a_i z^i + \sum_{j=1}^{\ell} b_j z^j + \sum_{t=2}^{\ell} c_t z^t\right], \end{aligned} \tag{10}$$

where

$$c_t = \sum_{\substack{u+v=t \\ u,v\in\{1,2,\ldots,\ell-1\}}} a_u b_v.$$

Let $c_1 = 0$. Then the above congruence holds if and only if $a_t + b_t + c_t = 0$ for all $t \in \{1,2,\ldots,\ell\}$. Consequently, we have

$$\begin{cases} b_1 = a_1, \\ b_t = a_t + \sum_{\substack{u+v=t \\ u,v\in\{1,2,\ldots,t-1\}}} a_u b_v, \quad \text{if } 2 \le t \le \ell. \end{cases}$$

When $\ell = 1$, since $a_1 = b_1$, it follows that f is an involution. For $\ell \ge 2$, f is an involution if and only if

$$0 = \sum_{\substack{u+v=h \\ u,v\in\{1,2,\ldots,h-1\}}} a_u a_v = \begin{cases} a_{h/2}, & \text{if } 2 \mid h \\ 0, & \text{if } 2 \nmid h, \end{cases}$$

for all $h \in \{1,2,\ldots,\ell\}$. This condition holds if and only if $a_i = 0$ for all $i \in \{1,2,\ldots,\lfloor \ell/2 \rfloor\}$. ∎

IV. The properties of the mappings $\chi_{n,m}$ and its iterates

In this section, we examine the mapping $\chi_{n,m}$ defined in (1) and its iterates. Using the isomorphic correspondence established previously, the study of iterations of these functions over vector spaces can be translated into a problem concerning multiplication in a polynomial ring. Within this framework, many of our results correspond directly to those in Section 4 of [13]. In particular, we derive an explicit expression for the inverse of $\chi_{n,m}$ and characterize the algebraic structure of its iterates. This characterization offers deeper insights into the fixed points and cycle structure of the mapping $\chi_{n,m}$.

Lemma 4.1: Let $\ell = \lfloor \frac{n}{m} \rfloor$ and $f = \left[1 + z^j + \sum_{i=j+1}^{\ell} a_i z^i\right] \in R_\ell{}^*$, where z^j is the non-constant term with the lowest degree in f. Then, the order of f in R_ℓ^* is $2^{\lceil \log_2 \frac{\ell+1}{j} \rceil}$, i.e., $\mathrm{ord}(f) = 2^{\lceil \log_2 \frac{\ell+1}{j} \rceil}$.

Proof: Since $|R_\ell^*| = 2^\ell$, the order of f is a power of 2, denoted by 2^r, by Lagrange's Theorem. We then have

$$\begin{cases} 1 = f^{2^r} = \left[1 + z^j + \sum_{i=j+1}^{\ell} a_i z^i\right]^{2^r} = \left[1 + z^{2^r j} + \sum_{i=j+1}^{\ell} a_i z^{2^r i}\right] \\ 1 \ne f^{2^{r-1}} = \left[1 + z^{2^{r-1} j} + \sum_{i=j+1}^{\ell} a_i z^{2^{r-1} i}\right]. \end{cases} \tag{11}$$

Note that (11) holds if and only if $2^r j \ge \ell + 1 > 2^{r-1} j$. Therefore, we have $2^{r-1} < \frac{\ell+1}{j} \le 2^r$, which imples that $\mathrm{ord}(f) = 2^{\lceil \log_2 \frac{\ell+1}{j} \rceil}$. ∎

Due to their simple expression, the binomial cases are of particular interest. Using Proposition 3.10, we derive the explicit expression for the inverse of the binomial $\theta_0 + \theta_{m,k} \in G_{n,m}$.

Theorem 4.2: Let $k \ge 1$, $\ell = \left\lfloor \frac{n}{m} \right\rfloor$ and $s = \left\lfloor \frac{\ell}{k} \right\rfloor$. Let $f = \theta_0 + \theta_{m,k} \in G_{n,m}$. Then $\mathrm{ord}(f) = 2^{\lceil \log_2 (\frac{\ell+1}{k}) \rceil}$, and the compositional inverse of f is

$$f^{-1} = \theta_0 + \theta_{m,k} + \theta_{m,2k} + \cdots + \theta_{m,sk}.$$

Moreover, $\deg(f) = (m-1)k + 1$ and $\deg(f^{-1}) = (m-1)sk + 1$.

Proof: Let $a_k = 1$ and $a_i = 0$ for $i \ne k$. By Proposition 3.10, we have $b_t = 0$ for $t < k$ and $b_k = a_k = 1$. In the following, we assume $\ell \ge t > k$. Let $t' < k$ with $t \equiv t' \pmod{k}$. If $k \nmid t$, then $b_t = a_t + a_k b_{t-k} = b_{t-k} = b_{t'} = 0$. If $k \mid t$, then $b_t = a_t + a_k b_{t-k} = b_{t-k} = b_k = 1$. Therefore, $b_t = 1$ if and only if t is a multiple of k and does not exceed ℓ. The $\deg(f)$ and $\deg(f^{-1})$ follow from Lemma 3.3, the order of f is obtained by Lemma 4.1. ∎

Remark 4.3: By examining the state diagram of χ_n, Schoone and Daemen in [21] proved that $\mathrm{ord}(\chi_n) = 2^{\lceil \log_2 \frac{n+1}{2} \rceil}$ when n is odd. This is a special case of Theorem 4.2 for $m = 2$, $k = 1$ and n being odd. So, Theorem 4.2 generalizes Corollary 9 of [21].

Let $k = 1$ in Theorem 4.2, and we have $\chi_{n,m} = \theta_0 + \theta_{m,1}$. As previously stated, $\chi_{n,m}$ permutes $\mathbb{F}_2^n$ if $m \nmid n$. However, if $m \mid n$, then we have

$$\chi_{n,m}(1, \mathbf{0}_{m-1}, 1, \mathbf{0}_{m-1}, \cdots, 1, \mathbf{0}_{m-1}) = \mathbf{0} = \chi_{n,m}(\mathbf{0}),$$

where $\mathbf{0}_i$ denotes the zero vector with i bits. Thus, $\chi_{n,m}$ is not a permutation. This leads us to the necessary and sufficient condition for $\chi_{n,m}$ being a permutation, along with its compositional inverse.

Corollary 4.4: Follow the notation defined above. The mapping $\chi_{n,m}$ in (1) is a permutation of $\mathbb{F}_2^n$ if and only if $m \nmid n$. In particular, if $m \nmid n$, then the inverse of $\chi_{n,m}$ is

$$\chi_{n,m}^{-1} = \theta_0 + \theta_{m,1} + \theta_{m,2} + \cdots + \theta_{m,\ell},$$

or equivalently,

$$y_i = x_i + \sum_{k=1}^{\ell} x_{i+mk} \prod_{\substack{j=1 \\ m\nmid j}}^{mk-1} (x_{i+j}+1) \tag{12}$$

for the i-th coordinate of the output, where $\ell = \left\lfloor \frac{n}{m} \right\rfloor$. Moreover, $\deg(\chi_{n,m}^{-1}) = (m-1)\ell + 1$.

Remark 4.5: By considering an affine variety associated with χ_n, Liu et al. in [15] provided the specific expression for χ_n^{-1} as

$$y_i = x_i + \sum_{k=1}^{\ell} x_{i-2k+1} \prod_{j=k}^{\ell} (x_{i-2j}+1) \tag{13}$$

for the i-th coordinate of the output, where n is odd and $\ell = (n-1)/2$. In fact, the equality (12) is consistent with (13) for $m = 2$. When $m = 2$, (12) becomes

$$\begin{aligned} y_i &= x_i + \sum_{k=1}^{\ell} x_{i+2k} \prod_{j=0}^{k-1} (x_{i+2j+1}+1) \\ &= x_i + \sum_{k'=1}^{\ell} x_{i+2(\ell-k'+1)} \prod_{j'=\ell-k+1}^{\ell} \left(x_{i+2(\ell-j')+1}+1\right) \\ &= x_i + \sum_{k'=1}^{\ell} x_{i-2k'+1} \prod_{j'=k'}^{\ell} (x_{i-2j'}+1), \end{aligned}$$

where the second equality is obtained by substitution $k' = \ell - k + 1, j' = \ell - j$, and the third equality holds since $2\ell + 1 = n$. Therefore, Corollary 4.4 generalizes Theorem 1 in [15].

Next, we investigate the fixed points of the iterate $\chi_{n,m}^k$ of $\chi_{n,m}$ for some positive integer k, which characterize some cryptographic properties. To this end, we need to determine the explicit expression of the iterate $\chi_{n,m}^k$. Let $j, k \in \mathbb{N}$ be written in base 2 as $j = j_0 + 2j_1 + 2^2 j_2 + \cdots + 2^{s-1} j_{s-1}$, and $k = k_0 + 2k_1 + 2^2 k_2 + \cdots + 2^{s-1} k_{s-1}$, where $j_i, k_i \in \mathbb{F}_2$ for any $i \in [s]$. Denote $j \preceq k$ if $j_i \le k_i$ for any $i \in [s]$.

Theorem 4.6: Let $k \ge 1$ and $\ell = \left\lfloor \frac{n}{m} \right\rfloor$, where $m \nmid n$. Then

$$\chi_{n,m}^k = \sum_{j=0}^{\min\{k,\ell\}} a_j \theta_{m,j},$$

where $a_j = 1$ if and only if $j \preceq k$.

Proof: It is known that $G_{n,m}$ is isomorphic to R_ℓ^* by the mapping φ. We obtain $\chi_{n,m}^k$ by investigating the inverse of $\varphi(\chi_{n,m}^k)$. Since $\varphi(\chi_{n,m}^k) = (1+z)^k \in R_\ell^*$, we need to expand the polynomial $(1+z)^k$ to find its preimage under φ.

By Lucas's theorem,

$$\begin{aligned} \binom{k}{j} &= \binom{k_0 + 2k_1 + 2^2 k_2 + \cdots + 2^{s-1} k_{s-1}}{j_0 + 2j_1 + 2^2 j_2 + \cdots + 2^{s-1} j_{s-1}} \\ &\equiv \binom{k_0}{j_0} \cdot \binom{k_1}{j_1} \cdot \cdots \cdot \binom{k_{s-1}}{j_{s-1}} \pmod 2. \end{aligned}$$

Thus, $\binom{k}{j} \equiv 1 \bmod 2$ if and only if $j \preceq k$. Therefore,

$$(1+z)^k = \sum_{j=0}^{k} \binom{k}{j} z^j = \sum_{j=0}^{k} a_j z^j \equiv \sum_{j=0}^{\min\{k,\ell\}} a_j z^j \mod z^{\ell+1},$$

where $a_j = 1$ if and only if $j \preceq k$. Consequently, the preimage of $(1+z)^k$ under φ is $\sum_{j=0}^{\min\{k,\ell\}} a_j \theta_{m,j}$. This completes proof. ∎

A vector $x \in \mathbb{F}_2^n$ is called a *fixed point* of $\chi_{n,m}^k$ if $\chi_{n,m}^k(x) = x$.

Theorem 4.7: Let $\ell = \lfloor \frac{n}{m} \rfloor$. The length of any cycle of mapping $\chi_{n,m}$ is $k = 2^j$ for some $j \in \{0, 1, 2, \ldots, r\}$, where $r = \lceil \log_2(\ell+1) \rceil$. Furthermore, $x \in \mathbb{F}_2^n$ is a fixed point of $\chi_{n,m}^{2^j}$ if and only if x does not contain a substring of the form $(\mathbf{0}_{m-1}, *, \mathbf{0}_{m-1}, *, \cdots, \mathbf{0}_{m-1}, 1)$ of length $2^j m$, where $* \in \mathbb{F}_2$ is any bit value and $\mathbf{0}_{m-1}$ denotes $m-1$ consecutive bits of 0.

Proof: By Theorem 4.2, we know that $\mathrm{ord}(\chi_{n,m}) = 2^r$, which is the least common multiple of the lengths of all cycles in $\chi_{n,m}$. Thus, the length of any cycle in $\chi_{n,m}$ must be a power of 2. By Theorem 4.6 we have $\chi_{n,m}^{2^j} = \theta_0 + \theta_{m,2^j}$. Consequently, x is a fixed point of $\chi_{n,m}^{2^j}$ if and only if $\theta_{m,2^j}(x) = \mathbf{0}$. Note that the i-th component of $\theta_{m,2^j}(x)$ is equal to 1 if and only if $(x_{i+1}, \cdots, x_{i+2^j m}) = (\mathbf{0}_{m-1}, *, \mathbf{0}_{m-1}, *, \cdots, \mathbf{0}_{m-1}, 1)$. This completes proof. ∎

Remark 4.8: A fixed point $x \in \mathbb{F}_2^n$ of $\chi_{n,m}^j$ lies in a cycle of length dividing j in the cycle decomposition of the mapping $\chi_{n,m}$. Moreover, if x is not a fixed point of $\chi_{n,m}^{j'}$ for any $j' < j$, then the length of the cycle containing x is exactly j.

Theorem 4.9: Let $x \in \mathbb{F}_2^n$ be a vector containing at least one substring $(\mathbf{0}_{m-1}, 1)$. Then the length of the cycle containing x is $2^{s(x)+1}$, where

$$\begin{aligned} s(x) = \max\{k : \exists i \in \{1, \ldots, n\} \text{ with } &(x_{i+1}, \ldots, x_{i+2^k m}) \\ &= (\mathbf{0}_{m-1}, *, \ldots, \mathbf{0}_{m-1}, 1)\}. \end{aligned}$$

Moreover, every vector $y \in \mathbb{F}_2^n$ that contains no substring $(\mathbf{0}_{m-1}, 1)$ is a fixed point of $\chi_{n,m}$. Consequently, the maximal cycle length of $\chi_{n,m}$ is $2^{\lfloor \log_2 \ell \rfloor + 1}$, where $\ell = \lfloor n/m \rfloor$.

Proof: For a vector $x \in \mathbb{F}_2^n$ containing at least one substring $(\mathbf{0}_{m-1}, 1)$, the quantity $s(x)$ is well-defined. By the definition of $s = s(x)$, there exists an index $i \in \{1, \ldots, n\}$ such that $(x_{i+1}, \ldots, x_{i+2^s m}) = (\mathbf{0}_{m-1}, *, \ldots, \mathbf{0}_{m-1}, 1)$. According to Theorem 4.7, this implies that x is not a fixed point of $\chi_{n,m}^{2^j}$ for any $j \le s$. On the other hand, the maximality of s guarantees that x does not contain a substring of the form $(\mathbf{0}_{m-1}, *, \ldots, \mathbf{0}_{m-1}, 1)$ of length $2^{s+1} m$. Hence, by Theorem 4.7 again, x is a fixed point of $\chi_{n,m}^{2^{s+1}}$. Therefore, the cycle containing x has length exactly 2^{s+1}.

If a vector $y \in \mathbb{F}_2^n$ contains no substring $(\mathbf{0}_{m-1}, 1)$, then Theorem 4.7 directly shows that y is a fixed point of $\chi_{n,m}$. Finally, the expression $2^{\lfloor \log_2 \ell \rfloor + 1}$ with $\ell = \lfloor n/m \rfloor$ follows by evaluating the maximum possible value of $s(x)$ over all $x \in \mathbb{F}_2^n$. ∎

Recall that $\chi_{n,m} = \theta_0 + \theta_{m,1}$, and by Theorem 4.6, $\chi_{n,m}^2 = \theta_0 + \theta_{m,2}$. Thus, $\chi_{n,m}$ is an involution if and only if $\chi_{n,m}^2(x) = x$ for any $x \in \mathbb{F}_2^n$, i.e., $\theta_{m,2} = \mathbf{0}$. By Lemma 3.10, we have the following result.

Corollary 4.10: Let m and n be integers with $m \nmid n$. Then $\chi_{n,m}$ is an involution if and only if $n \leq 2m-1$.

Remark 4.11: By Corollary 4.10, the mapping χ_n can be an involution only if the dimension $n \leq 3$. However, $\chi_{n,m}$ can be involutions for large dimension n.

Based on the theorems presented in this paper, we provide an example which is consistent with numerical experiments conducted on Magma (see [7]).

Example 4.12: Let $\chi_{8,3}\colon \mathbb{F}_2^8 \to \mathbb{F}_2^8$ be the mapping given by $y = \chi_{8,3}(x)$, where the i-th coordinate of y is represented as

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

By Theorem 4.2, we have $\mathrm{ord}(\chi_{8,3}) = 4$. And the compositional inverse of $\chi_{8,3}$ is $\chi_{8,3}^{-1} = \theta_0 + \theta_{3,1} + \theta_{3,2}$ by Corollary 4.4, where the i-th coordinate of the output y is represented as

$$\begin{aligned} y_i &= x_i + x_{i+3}(x_{i+2}+1)(x_{i+1}+1) \\ &\quad + x_{i+6}(x_{i+5}+1)(x_{i+4}+1)(x_{i+2}+1)(x_{i+1}+1) \\ &= x_i + (x_{i+2}+1)(x_{i+1}+1)(x_{i+3} \\ &\quad + x_{i+6}(x_{i+5}+1)(x_{i+4}+1)). \end{aligned}$$

Moreover, $\deg(\chi_{8,3}) = 3$, $\deg(\chi_{8,3}^{-1}) = 5$. By Theorem 4.6, $\chi_{8,3}^2 = \theta_0 + \theta_{3,2}$, where the i-th coordinate of the output y is represented as

$$y_i = x_i + x_{i+6}(x_{i+5}+1)(x_{i+4}+1)(x_{i+2}+1)(x_{i+1}+1),$$

and by Theorem 4.9 the cycle containing $(0,0,0,0,1,1,1,1) \in \mathbb{F}_2^8$ has length 2.

V. A comparative analysis of the χ_n, $\chi_{n,m}$ and $\mathcal{K}_n$ functions on a small scale

This section establishes a comparative evaluation for the χ_n, $\chi_{n,m}$ and $\mathcal{K}_n$ functions, focusing on their cryptographic security properties and implementation costs at reduced parameter scales (specifically for small values of n). To assess these characteristics, we first formalize key cryptographic security metrics, including algebraic degree, differential uniformity, nonlinearity, boomerang uniformity, differential-linear uniformity.

A. Cryptographic security metrics for vectorial Boolean functions

To ensure robustness against modern cryptanalytic techniques, vectorial Boolean functions used in cryptography must satisfy rigorous security criteria. We focus on four fundamental cryptographic properties: differential uniformity, algebraic degree, nonlinearity, boomerang uniformity, and differential-linear uniformity. These metrics collectively characterize a function's resistance to major attack vectors in symmetric cryptography.

Differential cryptanalysis, introduced by Biham and Shamir [5], remains a cornerstone in block cipher cryptanalysis. Following Nyberg's formalization [18], let $F(x)$ be a function from $\mathbb{F}_2^n$ to itself. The *differential uniformity* of F is defined as:

$$\Delta_F = \max_{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\},\ b \in \mathbb{F}_2^n} \delta_F(a,b),$$

where $\delta_F(a,b) = |\{x \in \mathbb{F}_2^n \colon F(x+a) + F(x) = b\}|$. The complete differential behavior is captured by the *differential spectrum*, which is a multiset:

$$\{\delta_F(a,b) \colon a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\},\ b \in \mathbb{F}_2^n\}.$$

Resistance to linear cryptanalysis [16] is quantified through nonlinearity. For a vector Boolean function $F(x)$ from $\mathbb{F}_2^n$ to itself, the *nonlinearity* of $F(x)$ is:

$$\mathrm{NL}_F = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\},\ b \in \mathbb{F}_2^n} |W_F(a,b)|,$$

where $W_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot F(x) + b \cdot x}$ is the Walsh transform, and $\cdot$ denotes the standard inner product. The *Walsh spectrum* comprises all Walsh coefficients as a multiset:

$$\{W_F(a,b) \colon a,b \in \mathbb{F}_2^n\}.$$

To address advanced differential variants, Cid et al. [8] introduced boomerang uniformity. For $a,b \in \mathbb{F}_{2^n}$, let $\beta_F(a,b)$ count solutions to:

$$F^{-1}(F(x)+b) + F^{-1}(F(x+a)+b) = a.$$

The *boomerang uniformity* is:

$$\mathrm{B}_F = \max_{a,b \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}} \beta_F(a,b),$$

with the *boomerang spectrum* given by the multiset:

$$\{\beta_F(a,b) \colon a,b \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}\}.$$

Recent work by Tang et al. [23] formalized resistance to differential-linear attacks through the Differential-Linear Connectivity Table (DLCT) of a vectorial Boolean function $F(x)$ from $\mathbb{F}_2^n$ to itself. This is a $2^n \times 2^n$ table, whose rows correpond to input differences of F and whose columns correspond to bit masks of outputs of F. For $a,b \in \mathbb{F}_2^n$, the value at position (a,b) in the DLCT of F is

$$\mathrm{DLCT}_F(a,b) = |\{x \in \mathbb{F}_2^n \colon b \cdot F(x) = b \cdot F(x+a)\}| - 2^{n-1},$$

yielding the *differential-linear uniformity* of F:

$$\mathrm{DL}_F = \max_{a,b \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}} \mathrm{DLCT}_F(a,b).$$

B. Comprehensive security evaluation

In this subsection, we present a comparative analysis of $\chi_{n,m}$, χ_n, and $\mathcal{K}_n$ based on the aforementioned metrics for security analysis. In Tables I-IV, we conduct a detailed comparative security analysis among $\chi_{n,m}$ (including the mapping χ_5, i.e., $\chi_{5,2}$), $\mathcal{K}_n$ and its variants for $n = 5, 6, 8$.

In order to investigate the algebraic degree of $\mathcal{K}_n^{-1}$, we prove, as a by-product of our study, the conjecture proposed in [3]. The proof of the following theorem is given in Appendix A. It is worth noting that the same result was independently and concurrently proved in [1] by using a different method.

Theorem 5.1: Let k be an even integer. Every non-trivial component of the inverse of $\mathcal{K}_{2k}$ has algebraic degree k.

Remark 5.2: While Theorem 5.1 establishes the algebraic degree of $\mathcal{K}_n^{-1}$, a result also obtained independently and concurrently in [1], the underlying methodologies differ substantially. The proof in [1] relies on showing that the function

TABLE I: The boomerang spectra of χ_n, $\chi_{n,m}$, and $\mathbb{X}_n$

n	Function	B_F	Boomerang spectrum
5	$\chi_{5,3}$	24	$\{0^{380}, 2^{80}, 4^{210}, 6^{40}, 8^{155}, 10^{35}, 14^{15}, 16^{30}, 18^5, 22, 24^{10}\}$
5	χ_5	16	$\{0^{445}, 2^{176}, 4^{150}, 8^{110}, 12^{50}, 16^{30}\}$
6	$\chi_{6,4}$	58	$\{0^{36}, 4^{756}, 6^{24}, 8^{1122}, 10^{48}, 12^{372}, 14^{36}, 16^{606}, 18^{36}, 20^{246}, 22^{60}, 24^{210}, 26^{48}, 28^{204}, 30^9, 32^{12}, 34^{24}, 36^{18}, 38^3, 40^{24}, 42^{12}, 44^{12}, 46^{13}, 48^{15}, 50^{24}, 54^6, 58^2\}$
6	$\chi_3 \parallel \chi_3$	64	$\{0^{2247}, 4^{784}, 16^{840}, 64^{98}\}$
8	$\chi_{8,3}$	224	$\{0^{29228}, 2^{1224}, 4^{5550}, 6^{344}, 8^{5848}, 10^{360}, 12^{2068}, 14^{224}, 16^{4772}, 18^{278}, 20^{1552}, 22^{128}, 24^{1784}, 26^{252}, 28^{648}, 30^{112}, 32^{2944}, 34^{168}, 36^{369}, 38^{56}, 40^{800}, 42^{152}, 44^{304}, 46^{24}, 48^{1184}, 50^{48}, 52^{224}, 54^4, 56^{344}, 58^{64}, 60^{160}, 64^{1384}, 66^{24}, 68^{64}, 70^8, 72^{240}, 74^{48}, 76^{80}, 80^{496}, 82^{16}, 84^{28}, 88^{240}, 90^{24}, 92^{44}, 96^{160}, 100^{24}, 104^{64}, 108^8, 112^{200}, 114^8, 116^{16}, 118^8, 120^{40}, 128^{112}, 136^{112}, 140^{24}, 142^8, 144^{56}, 146^8, 152^{64}, 156^{16}, 160^{72}, 176^{32}, 184^8, 192^{40}, 200^{24}, 224^8\}$
8	$\mathbb{X}_8$	256	$\{0^{40639}, 4^{4928}, 8^{4200}, 16^{5720}, 24^{1400}, 32^{3090}, 64^{3414}, 96^{750}, 128^{450}, 256^{434}\}$

TABLE II: The DLCT of χ_n, $\chi_{n,m}$, and $\mathbb{X}_n$

n	Function	DL_F	Differential-linear connectivity table
5	$\chi_{5,3}$	16	$\{0^{285}, -4^{170}, 4^{166}, -8^{180}, 8^{140}, -16^{15}, 16^{36}\}$
5	χ_5	16	$\{0^{870}, -16^{61}, 16^{61}\}$
6	$\chi_{6,4}$	32	$\{0^{246}, -4^{223}, 4^{233}, -8^{386}, 8^{434}, -12^{300}, 12^{279}, -16^{522}, 16^{519}, -20^{146}, 20^{123}, -24^{294}, 24^{230}, -32^{18}, 32^{69}\}$
6	$\chi_3 \parallel \chi_3$	32	$\{0^{3612}, -32^{210}, 32^{210}\}$
8	$\chi_{8,3}$	128	$\{0^{26352}, -16^{7224}, 16^{7230}, -32^{8584}, 32^{8733}, -64^{3298}, 64^{2960}, -128^{384}, 128^{515}\}$
8	$\mathbb{X}_8$	128	$\{0^{62148}, -128^{1566}, 128^{1566}\}$

TABLE III: The algebraic degree and the differential spectra of χ_n, $\chi_{n,m}$, and $\mathbb{X}_n$

n	Function	Degree	Δ_F	Differential spectrum
5	$\chi_{5,3}$	3	14	$\{0^{721}, 2^{126}, 4^{90}, 6^{45}, 8^5, 14^5\}$
5	χ_5	2	8	$\{0^{676}, 2^{176}, 4^{120}, 8^{20}\}$
6	$\chi_{6,4}$	4	38	$\{0^{3441}, 2^{168}, 4^{144}, 6^{120}, 8^{96}, 22^{21}, 24^{15}, 26^{12}, 30^9, 38^6\}$
6	$\chi_3 \parallel \chi_3$	2	16	$\{0^{3192}, 4^{784}, 16^{56}\}$
8	$\chi_{8,3}$	3	112	$\{0^{56681}, 2^{1896}, 4^{2045}, 6^{980}, 8^{1544}, 10^{352}, 12^{720}, 14^{176}, 16^{360}, 18^{106}, 20^{112}, 22^{40}, 24^{64}, 26^8, 28^{48}, 30^{16}, 32^{24}, 34^8, 36^{24}, 38^8, 40^{16}, 44^{12}, 48^{16}, 60^8, 112^8\}$
8	$\mathbb{X}_8$	2	64	$\{0^{56088}, 4^{4928}, 8^{3360}, 16^{736}, 32^{120}, 64^{48}\}$

TABLE IV: The nonlinearities and Walsh spectra of χ_n, $\chi_{n,m}$, and $\mathbb{X}_n$

n	Function	NL_F	Walsh spectrum
5	$\chi_{5,3}$	4	$\{0^{657}, -8^{101}, 8^{230}, -16^{20}, 16^{10}, 24^5, 32\}$
5	χ_5	8	$\{0^{647}, -8^{126}, 8^{210}, -16^{10}, 16^{30}, 32\}$
6	$\chi_{6,4}$	4	$\{0^{2400}, -8^{480}, 8^{936}, -16^{144}, 16^{49}, -24^{24}, 24^6, 32^{15}, 40^{20}, 48^{15}, 64\}$
6	$\chi_3 \parallel \chi_3$	16	$\{0^{3255}, -16^{490}, 16^{294}, -32^{14}, 32^{42}, 64\}$
8	$\chi_{8,3}$	32	$\{0^{42040}, -16^{7332}, 16^{10464}, -32^{1712}, 32^{1650}, -48^{520}, 48^{968}, -64^{257}, 64^{300}, -80^{96}, 80^{40}, -96^{48}, 96^{24}, -112^{32}, -128^{16}, 128^{16}, 144^{12}, 192^8, 256\}$
8	$\mathbb{X}_8$	64	$\{0^{54603}, -32^{4116}, 32^{5292}, -64^{546}, 64^{910}, -128^{17}, 128^{51}, 256\}$

is linearly conjugate, via coordinate permutations $S^{(\alpha,\beta)}$, to a known benchmark function $\mathbb{X}_{m,m'}^{(b,b')}$. Our approach, by contrast, is based on a direct coordinate-wise analysis of $\mathbb{X}_n^{-1}$ itself, without invoking notions of linear or affine equivalence.

Let $n = 2k$ with even $k > 0$. Due to the above result, $\deg(\mathbb{X}_n^{-1}) = k$ while $\deg(\chi_{n,m}^{-1}) = (m-1)\left\lfloor \frac{n}{m} \right\rfloor + 1 > k$ by Corollary 4.4. Meanwhile, $\deg(\chi_{n,m}) > \deg(\mathbb{X}_n) = 2$ for $n > m \geq 3$ with $m \nmid n$. Notably, $\chi_{6,4}$ and $\chi_{8,3}$ exhibit stronger resistance against boomerang (see Table I) and differential-linear (see Table II) attacks compared to their counterparts $\chi_3 \parallel \chi_3$ and $\mathbb{X}_8$, respectively. Moreover, although $\chi_{5,3}$, $\chi_{6,4}$, and $\chi_{8,3}$ have the same differential-linear uniformity with their counterparts, our newly constructed functions exhibit significantly reduced peak frequencies in their DLCTs. Therefore, from the perspective of differential-linear cryptanalysis, the proposed mappings are slightly superior to their counterparts.

However, our presented mappings exhibit worse performance both in differential uniformity (see Table III) and nonlinearity (see Table IV) for $n = 5, 6, 8$ compared to their counterparts.

C. Implementation cost

Among our generalized χ_n-type mappings, $\chi_{n,3}$ emerges as one of the most lightweight candidates, without considering the original function. To optimize hardware implementation, we propose a modified variant $\chi'_{n,3}$ defined by $\chi'_{n,3}(x) = \chi_{n,3}(x + \mathbf{1})$, which can be equivalently expressed as:

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

where $i \in \{0, 1, \ldots, n-1\}$ and the indices are computed modulo n. Crucially, $\chi'_{n,3}$ preserves all essential cryptographic properties of $\chi_{n,3}$, including differential uniformity, nonlinearity, boomerang uniformity, and differential-linear uniformity, as verified through formal analysis.

We conduct a comparative study of implementation costs among $\chi'_{n,3}$, χ_n (i.e., $\chi_{n,2}$) and $\mathbb{X}_n$ for both odd and even n. Our evaluation using standard Complementary Metal Oxide Semiconductor (CMOS) technology libraries reveals comparable implementation costs across these mappings (see Appendix: Table V). Figure 1 and Figure 2 illustrate circuit implementations for χ_5 and $\chi'_{5,3}$, respectively, revealing their structural similarities.

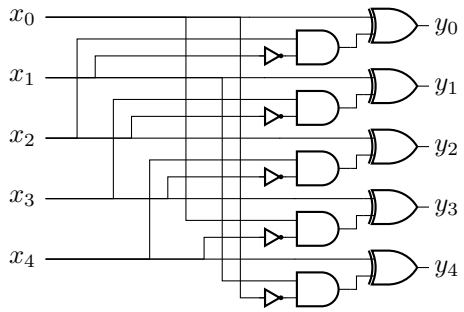

Fig. 1: A circuit implementation of χ_5

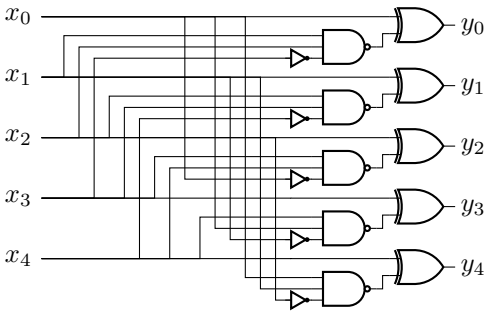

Fig. 2: A circuit implementation of $\chi'_{5,3}$

The component function $y_i = x_i + x_{i+1}x_{i+2}(x_{i+3} + 1)$ in $\chi'_{n,3}$ requires one XOR-gate, one NOT-gate, and one 3-input NAND-gate per bit. In contrast, $\chi_{n,2}$ replaces the 3-input NAND-gate with a 2-input AND-gate. As demonstrated in Table VI, this substitution results in similar implementation areas for both mappings. Moreover, $\chi'_{n,3}$ achieves an implementation area no larger than $\mathbb{X}_n$ by eliminating one NOT-gate.

Latency complexity represents another critical metric for lightweight implementations. Following the framework in [19, Sec.3], which defines latency as the longest path through NAND/NOR-gates using the gate set $\mathcal{G} = \{\text{NOT}, \text{NAND}, \text{NOR}\}$, we analyze critical paths:

- $\chi'_{n,3}$ exhibits a 4-stage latency (2 stages for 3-input NAND + 2 stages for XOR);
- Both χ_n and $\mathbb{X}_n$ show 3-stage latency (1 stage for AND + 2 stages for XOR).

This analysis suggests that while $\chi'_{n,3}$ maintains area efficiency, it incurs a modest latency tradeoff compared to χ_n-type mappings. The choice between these implementations may therefore depend on specific application constraints emphasizing either area or latency optimization.

VI. Conclusion and future work

In this work, we generalize the well-known χ_n permutation to an extensive family of permutations $\chi_{n,m}$, which exists for both odd and even dimension vector spaces over $\mathbb{F}_2$. Our approach closely follows the elegant algebraic framework established by Kriepke and Kyureghyan [13], in which iterates of χ_n are expressed as linear combinations of specific basis maps γ_{2k}. Adopting this fundamental insight, we systematically extend their construction by introducing the broader family of maps $\theta_{m,i}$ and investigating the linear space they generate.

The innovative tool established by Kriepke and Kyureghyan [13] not only deepens the understanding of the algebraic structure of the χ function itself, but also opens new avenues for the study of vectorial Boolean functions. By translating the composition operation in the linear space generated by γ_{2k} to polynomial multiplication, their framework greatly simplifies the analysis of iteration within this function family. Our work demonstrates that this framework possesses broader generality-the correspondence remains valid beyond the specific family γ_{2k}. Explicitly, given a family of functions ψ_i satisfying

$$\psi_i \circ (\psi_0 + \sum a_j\psi_j) = \sum a_j\psi_{j+i}, \tag{14}$$

where $\psi_i = \theta_{m,i}$ in this paper and $\psi_i = \gamma_{2i}$ in [13], it can be shown that the family $\{\psi_0 + \sum a_i\psi_i\}$ is isomorphic to the unit group of $\mathbb{F}_2[z]/(z^d)$ for some integer d. Consequently, one can obtain a broader class of permutations whose iterative properties can be precisely characterized.

A natural and meaningful question thus arises: which functions have iterations that correspond to polynomial multiplication? Recently, Kriepke and Kyureghyan [2] provided partial answers. For even n, setting $\psi_i = \gamma_{2i}$ still satisfies Eq. (14). Unlike the odd-n case, however, the sequence $\{\gamma_{2k}\}_{k=0}^{\infty}$ does not vanish but eventually repeats for sufficiently large k. In this setting, the set $\{\psi_0 + \sum a_i\psi_i\}$ is homomorphic to the group $\mathbb{F}_2[z]/(z^n + z^{n/2})$. We believe that by suitably modifying $\theta_{m,k}$, one can obtain further varieties of function families homomorphic to polynomial quotient rings.

A more compelling problem remains: do there exist function families homomorphic to polynomial residue rings different from $\mathbb{F}_2[z]/(z^d)$ and $\mathbb{F}_2[z]/(z^n + z^{n/2})$? If ψ_i could be endowed with richer properties, for instance, if for a large i it neither repeats nor vanishes, but eventually reduces to a composition of earlier $\psi_{i'}$ $(i' < i)$, then one might obtain a function group corresponding to a wider variety of polynomial residue rings, perhaps even the finite fields. We leave

this promising direction for future work, inviting interested researchers to pursue these open questions.

In addition to providing a clear algebraic characterization of $\chi_{n,m}$, we conduct a comprehensive comparative analysis between our constructions and their counterparts for small-scale n, covering both implementation costs and relevant security metrics. Our research establishes a solid foundation for subsequent investigations in both theoretical and applied domains. Two clear directions for future work are suggested: since χ_n, $\chi_{n,3}$ and $\mathbb{X}_n$ each exhibit advantages under different security metrics, it would be of interest to investigate their concatenations to trade off these metrics, e.g., $\chi_3 \parallel \chi_{5,3} \parallel \mathbb{X}_8$. Moreover, as the components of $\mathbb{X}_n$ and χ_n are similar and share the same algebraic degree, another promising direction is to study the algebraic structure of $\mathbb{X}_n$ and its iterates using the extended methods introduced here.

Acknowledgment

The authors sincerely thank the associate editor, Dr. Gohar Kyureghyan, and the reviewers for their comments and suggestions that improved the quality of this paper.

References

[1] Samuele Andreoli, Gregor Leander, Enrico Piccione, and Lukas Stennes. Generalizations of ChiChi: Families of Low-Latency Permutations in Any Even Dimension. *IACR Transactions on Symmetric Cryptology*, 2025(3):800–826, 2025.

[2] Björn Kriepke and Gohar M. Kyureghyan. There are siblings of χ which are permutations for n even. Cryptology ePrint Archive, 2025. `https://eprint.iacr.org/2025/1780`.

[3] Yanis Belkheyar, Patrick Derbez, Shibam Ghosh, Gregor Leander, Silvia Mella, Léo Perrin, Shahram Rasoolzadeh, Lukas Stennes, Siwei Sun, Gilles Van Assche, and Damian Vizár. Chilow and chichi: New constructions for code encryption. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025*, pages 212–243, Cham, 2025. Springer Nature Switzerland.

[4] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak specifications. NIST SHA-3 submission (2008). http://keccak.noekeon.org.

[5] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptol.*, 4(1):3–72, 1991.

[6] Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich. Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key (extended abstract). In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 63–84. Springer, 2014.

[7] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 683–714. Springer, 2018.

[9] Joan Daemen. *Cipher and hash function design strategies based on linear and differential cryptanalysis*. PhD thesis, Doctoral Dissertation, March 1995, KU Leuven, 1995.

[10] Joan Daemen, Alireza Mehrdad, and Silvia Mella. Computing the distribution of differentials over the non-linear mapping χ. In Lejla Batina, Stjepan Picek, and Mainack Mondal, editors, *Security, Privacy, and Applied Cryptography Engineering - 11th International Conference, SPACE 2021, Kolkata, India, December 10-13, 2021, Proceedings*, volume 13162 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 2021.

[11] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2: Lightweight authenticated encryption and hashing. *J. Cryptol.*, 34(3):33, 2021.

[12] Anna-Maurin Graner, Björn Kriepke, Lucas Krompholz, and Gohar Kyureghyan. On the bijectivity of the map χ. *Cryptogr. Commun.*, Feb 2025.

[13] Björn Kriepke and Gohar M. Kyureghyan. Algebraic structure of the iterates of χ. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part IV*, volume 14923 of *Lecture Notes in Computer Science*, pages 412–424. Springer, 2024.

[14] Fukang Liu, Vaibhav Dixit, Santanu Sarkar, Willi Meier, and Takanori Isobe. Finding the inverse of some shift invariant transformations. *J. Cryptol.*, 39(1):1–31, 2026.

[15] Fukang Liu, Santanu Sarkar, Willi Meier, and Takanori Isobe. The inverse of χ and its applications to Rasta-Like ciphers. *J. Cryptol.*, 35(4):28, 2022.

[16] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

[17] Silvia Mella, Alireza Mehrdad, and Joan Daemen. Differential and linear properties of vectorial boolean functions based on chi. *Cryptogr. Commun.*, 15(6):1087–1116, 2023.

[18] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer, 1993.

[19] Shahram Rasoolzadeh. Low-latency boolean functions and bijective S-boxes. *IACR Trans. Symmetric Cryptol.*, 2022(3):403–447, 2022.

[20] Jan Schoone and Joan Daemen. Algebraic properties of the maps χ_n. *Des. Codes Cryptogr.*, 92(8):2341–2365, 2024.

[21] Jan Schoone and Joan Daemen. The state diagram of χ. *Des. Codes Cryptogr.*, 92(5):1393–1421, 2024.

[22] NIST Sha. Sha-3 standard: Permutation-based Hash and extendable-output functions. Technical Report 202, Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD, USA, 2015.

[23] Deng Tang, Bimal Mandal, and Subhamoy Maitra. Construction of balanced vectorial Boolean functions with almost optimal nonlinearity and very low differential-linear uniformity. *Finite Fields Their Appl.*, 76:101903, 2021.

[24] Meltem Sönmez Turan, Kerry McKay, Donghoon Chang, Jinkeon Kang, and John Kelsey. Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, Hash, and extendable output functions. Draft, U.S. Department of Commerce, November 2024.

TABLE V: Frequently-used logic gates in common CMOS technology libraries

Gate	Domain $\to$ Range	Logic formulas	Algebraic normal form
NOT	$\mathbb{F}_2 \to \mathbb{F}_2$	$x_0 \to \neg x_0$	$x_0 \to x_0 + 1$
AND	$\mathbb{F}_2^2 \to \mathbb{F}_2$	$x_0, x_1 \to x_0 \wedge x_1$	$x_0, x_1 \to x_0 x_1$
OR	$\mathbb{F}_2^2 \to \mathbb{F}_2$	$x_0, x_1 \to x_0 \vee x_1$	$x_0, x_1 \to x_0 x_1 + x_0 + x_1$
NAND	$\mathbb{F}_2^2 \to \mathbb{F}_2$	$x_0, x_1 \to \neg(x_0 \wedge x_1)$	$x_0, x_1 \to x_0 x_1 + 1$
NOR	$\mathbb{F}_2^2 \to \mathbb{F}_2$	$x_0, x_1 \to \neg(x_0 \vee x_1)$	$x_0, x_1 \to x_0 x_1 + x_0 + x_1 + 1$
XOR	$\mathbb{F}_2^2 \to \mathbb{F}_2$	$x_0, x_1 \to x_0 \oplus x_1$	$x_0, x_1 \to x_0 + x_1$
XNOR	$\mathbb{F}_2^2 \to \mathbb{F}_2$	$x_0, x_1 \to \neg(x_0 \oplus x_1)$	$x_0, x_1 \to x_0 + x_1 + 1$
AND3	$\mathbb{F}_2^3 \to \mathbb{F}_2$	$x_0, x_1, x_2 \to x_0 \wedge x_1 \wedge x_2$	$x_0, x_1, x_2 \to x_0 x_1 x_2$
NAND3	$\mathbb{F}_2^3 \to \mathbb{F}_2$	$x_0, x_1, x_2 \to \neg(x_0 \wedge x_1 \wedge x_2)$	$x_0, x_1, x_2 \to x_0 x_1 x_2 + 1$
XOR3	$\mathbb{F}_2^3 \to \mathbb{F}_2$	$x_0, x_1, x_2 \to x_0 \oplus x_1 \oplus x_2$	$x_0, x_1, x_2 \to x_0 + x_1 + x_2$

TABLE VI: Implementation area of frequently-used logic gates in common CMOS technology libraries

Gate	UMC 180nm	TSMC 65nm	TSMC 28nm	SMIC 130nm	SMIC 65nm	Nangate 45nm	Nangate 15nm	STD 350nm	STM 65nm
NOT	0.67	0.50	0.67	0.67	0.75	0.67	0.75	0.67	0.50
AND	1.33	1.50	1.33	1.33	1.50	1.33	1.50	1.33	1.50
OR	1.33	1.50	1.33	1.33	1.50	1.33	1.50	1.33	1.50
NAND	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
NOR	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
XOR	2.67	2.50	3.00	2.33	2.25	2.00	2.25	2.33	2.00
XNOR	2.00	2.50	3.00	2.33	2.25	2.00	2.25	2.33	2.00
AND3	2.33	2.00	1.67	1.67	1.75	1.67	2.00	1.67	2.00
NAND3	1.33	1.50	1.33	1.33	1.25	1.33	1.50	1.33	1.50
XOR3	4.67	5.50	4.33	5.67	4.75	N/A	N/A	4.00	

Cheng Lyu received the B.S. degree in mathematics from Hubei Engineering University, Hubei, China, in 2021, and the M.S. degree in mathematics from Hubei University, Hubei, China, in 2024. Since 2024, he has been pursuing the Ph.D. degree in mathematics at Hubei University. His research interest focuses on cryptographic functions.

Mu Yuan received the B.S., M.S., and Ph.D. degrees in mathematics from Hubei University, Wuhan, China, in 2015, 2019, and 2022, respectively. From February to November 2021, he was a Visiting Ph.D. Student with the Department of Mathematics, University of Paris VIII, Saint-Denis, France. From September 2022 to June 2025, he was a Post-Doctoral Researcher with the College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, China. Since July 2025, he has been with the School of Mathematics and Statistics, Hubei University, Wuhan, China, where he is currently a Lecturer. His research interests include coding theory and cryptography.

Dabin Zheng received the B.S. degree in mathematics from Hubei Normal University, Huangshi, China, in 2000, and the M.S. and Ph.D. degrees in applied mathematics from Hubei University and Academy of Mathematics and Systems Science, CAS, in 2003 and 2006, respectively. Since June 2006, he has been with Hubei University, where he is currently a Professor. From September 2009 to April 2012, he was a Post-Doctoral Researcher with the State Key Laboratory of Information Security, Beijing, China. From March 2015 to February 2016, he visited the Department of Mathematics, University of Delaware, USA. His research interests include coding theory and cryptography.

Siwei Sun received the B.S. degree in mathematics from Beijing University of Technology, Beijing, China, in 2008, and the Ph.D. degree in information security from the University of Chinese Academy of Sciences, Beijing, China, in 2013. From July 2013 to July 2021, he was an Assistant Researcher and later an Associate Researcher with the Institute of Information Engineering, Chinese Academy of Sciences. Since July 2021, he has been a Professor with the University of Chinese Academy of Sciences. His research interests include symmetric cryptography and hash-based post-quantum signatures.

Shun Li received the B.S. degree in mathematics and applied mathematics from Peking University, Beijing, China, in 2014, and the Ph.D. degree in cyberspace security from the University of Chinese Academy of Sciences, Beijing, China, in 2019. From November 2019 to November 2021, he was a Post-Doctoral Researcher with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China. From November 2020 to December 2023, he was a Research Fellow with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Since January 2024, he has been with the School of Cryptology, University of Chinese Academy of Sciences, Beijing, China, where he is currently an Assistant Researcher. His research interests include symmetric-Key cryptography and quantum cryptanalysis.

APPENDIX

Proof of Theorem 5.1: Based on (2), we first attempt to express x_i in terms of $x_{k-3}, x_{k-2}, x_{k-1}, x_k$, and $y_0, y_1, \ldots, y_{2k-1}$. Since $y_i = x_i + \overline{x}_{i+1}x_{i+2}$ for $i < k-3$ or $k < i < n-2$, x_{k-4} can be expressed as:

$$x_{k-4} = y_{k-4} + \bar{x}_{k-3}x_{k-2}.$$

From x_{k-4} we can further derive an alternative expression for x_{k-5}:

$$x_{k-5} = y_{k-5} + \bar{x}_{k-4}x_{k-3} = y_{k-5} + \bar{y}_{k-4}x_{k-3}.$$

Therefore, we can recursively express x_i as follows for $0 \le i \le k-4$:

$$x_i = \begin{cases} y_i + \bar{y}_{i+1}\Big(y_{i+2} + \bar{y}_{i+3}\big(\cdots \bar{y}_{k-5}\,(y_{k-4} + \bar{x}_{k-3}x_{k-2})\cdots\big)\Big), & \text{if } i \text{ is even,} \\ y_i + \bar{y}_{i+1}\Big(y_{i+2} + \bar{y}_{i+3}\big(\cdots \bar{y}_{k-6}(y_{k-5} + \bar{y}_{k-4}x_{k-3})\cdots\big)\Big), & \text{if } i \text{ is odd.} \end{cases} \tag{15}$$

Note that the first two terms are

$$\begin{cases} x_1 = y_1 + \bar{y}_2\Big(y_3 + \bar{y}_4\big(\cdots \bar{y}_{k-6}(y_{k-5} + \bar{y}_{k-4}x_{k-3})\cdots\big)\Big), \\ x_0 = y_0 + \bar{y}_1\Big(y_2 + \bar{y}_3\big(\cdots \bar{y}_{k-5}(y_{k-4} + \bar{x}_{k-3}x_{k-2})\cdots\big)\Big). \end{cases} \tag{16}$$

Similarly, for $k+1 \le i \le 2k-1$, x_i can be recursively expressed as follows:

$$\begin{cases} x_{2k-1} = y_{2k-1} + \bar{x}_{k-1}x_k, \\ x_{2k-2} = y_{2k-2} + \bar{x}_{2k-1}x_{k-1} = y_{2k-2} + \bar{y}_{2k-1}x_{k-1}, \\ \quad\vdots \\ x_{k+2t+1} = y_{k+2t+1} + \bar{y}_{k+2t+2}\big(\cdots \bar{y}_{2k-2}(y_{2k-1} + \bar{x}_{k-1}x_k)\cdots\big), \\ x_{k+2t} = y_{k+2t} + \bar{y}_{k+2t+1}\big(\cdots \bar{y}_{2k-3}(y_{2k-2} + \bar{y}_{2k-1}x_{k-1})\cdots\big), \\ \quad\vdots \\ x_{k+2} = y_{k+2} + \bar{y}_{k+3}\big(\cdots \bar{y}_{2k-3}(y_{2k-2} + \bar{y}_{2k-1}x_{k-1})\cdots\big), \\ x_{k+1} = y_{k+1} + \bar{y}_{k+2}\big(\cdots \bar{y}_{2k-2}(y_{2k-1} + \bar{x}_{k-1}x_k)\cdots\big). \end{cases} \tag{17}$$

The remaining four terms could not be simply represented recursively and are as follows:

$$\begin{cases} x_{k-3} = \bar{y}_{k-1} + \bar{x}_k\bar{x}_{k+1}, \\ x_{k-2} = y_k + \bar{x}_{k+1}x_{k+2} = y_k + \bar{y}_{k+1}x_{k+2}, \\ x_{k-1} = y_{k-2} + \bar{x}_0x_1 = y_{k-2} + \bar{y}_0x_1, \\ x_k = y_{k-3} + \bar{x}_{k-2}x_0. \end{cases}$$

By substituting the expressions of x_{k+1}, x_{k+2} in (17) and x_1, x_0 in (16) into the expressions for x_{k-3}, x_{k-2}, x_{k-1}, and x_k respectively, we obtain:

$$\begin{cases} x_{k-3} = \bar{y}_{k-1} + \bar{x}_k\Big(\bar{y}_{k+1} + \bar{y}_{k+2}\big(\cdots \bar{y}_{2k-2}(y_{2k-1} + \bar{x}_{k-1}x_k)\cdots\big)\Big) \\ \qquad = \bar{y}_{k-1} + \bar{x}_k\Big(\bar{y}_{k+1} + \bar{y}_{k+2}\big(\cdots (y_{2k-3} + \bar{y}_{2k-2}y_{2k-1})\cdots\big)\Big), \\ x_{k-2} = y_k + \bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots \bar{y}_{2k-3}(y_{2k-2} + \bar{y}_{2k-1}x_{k-1})\cdots\big)\Big) \\ \qquad = y_k + \bar{y}_{k+1}\bar{y}_{k+3}\cdots\bar{y}_{2k-1}x_{k-1} \\ \qquad\quad + \bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots (y_{2k-4} + \bar{y}_{2k-3}y_{2k-2})\cdots\big)\Big), \\ x_{k-1} = y_{k-2} + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots \bar{y}_{k-6}(y_{k-5} + \bar{y}_{k-4}x_{k-3})\cdots\big)\Big) \\ \qquad = y_{k-2} + \bar{y}_0\bar{y}_2\cdots\bar{y}_{k-4}x_{k-3} + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots (y_{k-7} + \bar{y}_{k-6}y_{k-5})\cdots\big)\Big), \\ x_k = y_{k-3} + \bar{x}_{k-2}\Big(y_0 + \bar{y}_1\big(\cdots \bar{y}_{k-5}(y_{k-4} + \bar{x}_{k-3}x_{k-2})\cdots\big)\Big) \\ \qquad = y_{k-3} + \bar{x}_{k-2}\Big(y_0 + \bar{y}_1\big(\cdots (y_{k-6} + \bar{y}_{k-5}y_{k-4})\cdots\big)\Big). \end{cases} \tag{18}$$

Furthermore, by substituting the expressions of x_k and x_{k-1} into the expressions for x_{k-3} and x_{k-2}, respectively, we have

$$\begin{cases} x_{k-3} = \bar{y}_{k-1} + \Big(\bar{y}_{k-3} + \bar{x}_{k-2}\Big(y_0 + \bar{y}_1\big(\cdots(y_{k-6} + \bar{y}_{k-5}y_{k-4})\cdots\big)\Big)\Big) \\ \qquad\quad \cdot \Big(\bar{y}_{k+1} + \bar{y}_{k+2}\big(\cdots(y_{2k-3} + \bar{y}_{2k-2}y_{2k-1})\cdots\big)\Big) \\ \qquad = \bar{y}_{k-1} + \bar{x}_{k-2}\cdot f\cdot g + \bar{y}_{k-3}\cdot g, \\ x_{k-2} = y_k + \bar{y}_{k+1}\bar{y}_{k+3}\cdots\bar{y}_{2k-1}\Big(y_{k-2} + \bar{y}_0\bar{y}_2\cdots\bar{y}_{k-4}x_{k-3} \\ \qquad + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots(y_{k-7} + \bar{y}_{k-6}y_{k-5})\cdots\big)\Big)\Big) \\ \qquad + \bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots(y_{2k-4} + \bar{y}_{2k-3}y_{2k-2})\cdots\big)\Big) \\ \qquad = y_k + h\cdot\Big(y_{k-2} + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots(y_{k-7} + \bar{y}_{k-6}y_{k-5})\cdots\big)\Big)\Big) \\ \qquad + x_{k-3}\cdot e\cdot h + \bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots(y_{2k-4} + \bar{y}_{2k-3}y_{2k-2})\cdots\big)\Big), \end{cases} \tag{19}$$

where

$$\begin{cases} f = y_0 + \bar{y}_1\Big(y_2 + \bar{y}_3\big(\cdots(y_{k-6} + \bar{y}_{k-5}y_{k-4})\cdots\big)\Big), \\ g = \bar{y}_{k+1} + \bar{y}_{k+2}\Big(y_{k+3} + \bar{y}_{k+4}\big(\cdots(y_{2k-3} + \bar{y}_{2k-2}y_{2k-1})\cdots\big)\Big), \\ e = \bar{y}_0\bar{y}_2\cdots\bar{y}_{k-4}, \\ h = \bar{y}_{k+1}\bar{y}_{k+3}\cdots\bar{y}_{2k-1}. \end{cases}$$

The degrees of f, g, e, and h are $\frac{k}{2}-1$, $\frac{k}{2}$, $\frac{k}{2}-1$, and $\frac{k}{2}$ respectively. Some interesting properties include $g\cdot h = h$ and $f\cdot e = 0$.

Substituting x_{k-2} into the expression of x_{k-3}, or x_{k-3} into the expression of x_{k-2} would lead to a multiplication of $f\cdot g\cdot e\cdot h$ which equals 0 since $f\cdot e = 0$, we know that the expressions of x_{k-3} and x_{k-2} involve only y_i.

The second term of x_{k-3} in (19)

$$\begin{aligned} &\bar{x}_{k-2}\cdot f\cdot g \\ &= \bar{y}_k\cdot f\cdot g + h\cdot\Big(y_{k-2} + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots(y_{k-7} + \bar{y}_{k-6}y_{k-5})\cdots\big)\Big)\Big)\cdot f\cdot g \\ &\quad + \bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots(y_{2k-4} + \bar{y}_{2k-3}y_{2k-2})\cdots\big)\Big)\cdot f\cdot g \end{aligned} \tag{20}$$

has degree k, since the second term of $\bar{x}_{k-2}\cdot f\cdot g$ in (20)

$$\begin{aligned} &h\cdot\Big(y_{k-2} + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots(y_{k-7} + \bar{y}_{k-6}y_{k-5})\cdots\big)\Big)\Big)\cdot f\cdot g \\ &= h\cdot g\cdot\Big(\Big(y_{k-2} + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots(y_{k-7} + \bar{y}_{k-6}y_{k-5})\cdots\big)\Big)\Big)\cdot f\Big) \\ &= \bar{y}_{k+1}\bar{y}_{k+3}\cdots\bar{y}_{2k-1}y_{k-2}\cdot f \end{aligned}$$

has degree k, and the last term of $\bar{x}_{k-2}\cdot f\cdot g$ in (20)

$$\begin{aligned} &\bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots(y_{2k-4} + \bar{y}_{2k-3}y_{2k-2})\cdots\big)\Big)\cdot f\cdot g \\ &= \bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots(y_{2k-4} + \bar{y}_{2k-3}y_{2k-2})\cdots\big)\Big)\cdot f \end{aligned}$$

has degree of $k-1$. Combining this with the fact that the last term of x_{k-3} in (19) is $\bar{y}_{k-3}\cdot g$, which has degree of $\frac{k}{2}+1$. So the algebraic degree x_{k-3} is k. Similarly, we can obtain that the degree of x_{k-2} is k.

Rewriting the expression for x_{k-3} yields

$$\begin{aligned} x_{k-3} &= \bar{y}_{k-1} + \bar{y}_{k-3}\Big(\bar{y}_{k+1} + \bar{y}_{k+2}\big(\cdots(y_{2k-3} + \bar{y}_{2k-2}y_{2k-1})\cdots\big)\Big) \\ &\quad + f\cdot y_{k-2}\bar{y}_{k+1}\bar{y}_{k+3}\cdots\bar{y}_{2k-1} + f\cdot\bar{y}_{k+1}\Big(y_{k+2} \\ &\quad + \bar{y}_{k+3}\big(\cdots(y_{2k-4} + \bar{y}_{2k-3}y_{2k-2})\cdots\big)\Big) + f\cdot\bar{y}_k\cdot g \\ &= \bar{y}_{k-1} + \bar{y}_{k-3}\cdot g + f\cdot h\cdot y_{k-2} + f\cdot F + f\cdot\bar{y}_k\cdot g, \end{aligned} \tag{21}$$

where

$$F = \bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots(y_{2k-4} + \bar{y}_{2k-3}y_{2k-2})\cdots\big)\Big),$$

has degree $\frac{k}{2}$ and $g\cdot F = F$.

Back to $x_0, \ldots, x_{k-4}$, we need to prove that $\bar{y}_{2i+1}\bar{y}_{2i+3}\cdots\bar{y}_{k-5}\bar{x}_{k-3}x_{k-2}$ has degree of k, where $i \in \{0, 1, \cdots, \frac{k}{2}-2\}$, and $\bar{y}_{2j}\bar{y}_{2j+2}\cdots\bar{y}_{k-4}x_{k-3}$ has degree of k, where $j \in \{1, \ldots, \frac{k}{2}-2\}$. Note that

$$\bar{x}_{k-3}x_{k-2} = \bar{x}_{k-3}(y_k + x_{k-3}\cdot e\cdot h + h\cdot G + F), \tag{22}$$

where

$$G = y_{k-2} + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots(y_{k-7} + \bar{y}_{k-6}y_{k-5})\cdots\big)\Big),$$

has degree $\frac{k}{2}-1$. Then, substituting x_{k-3} in (21) into (22), we have

$$\begin{aligned}
\bar{x}_{k-3}x_{k-2} &= (y_{k-1} + \bar{y}_{k-3}\cdot g + f\cdot h\cdot y_{k-2} + f\cdot F + f\cdot\bar{y}_k\cdot g)(y_k + h\cdot G + F)\\
&= y_{k-1}y_k + \bar{y}_{k-3}y_k\cdot g + y_{k-2}y_k\cdot f\cdot h + y_k\cdot f\cdot F + y_{k-1}\cdot h\cdot G + \bar{y}_{k-3}\cdot h\cdot G\\
&\quad + y_{k-2}\cdot f\cdot h + y_{k-2}\bar{y}_k\cdot f\cdot h + y_{k-1}\cdot F + \bar{y}_{k-3}\cdot F + f\cdot F + \bar{y}_k\cdot f\cdot F\\
&= y_{k-1}y_k + \bar{y}_{k-3}y_k\cdot g + (y_{k-1} + \bar{y}_{k-3})\cdot F + (y_{k-1} + \bar{y}_{k-3})\cdot h\cdot G.
\end{aligned}$$

Next, we consider the last term of $\bar{x}_{k-3}x_{k-2}$. Note that

$$\begin{aligned}
&\bar{y}_{2t+1}\bar{y}_{2t+3}\cdots\bar{y}_{k-5}\cdot G\\
&= \bar{y}_{2t+1}\bar{y}_{2t+3}\cdots\bar{y}_{k-5}\Big(y_{k-2} + \bar{y}_0\Big(y_1 + \bar{y}_2\big(\cdots(y_{2t-3} + \bar{y}_{2t-2}y_{2t-1})\cdots\big)\Big)\Big)
\end{aligned}$$

always has degree $\frac{k}{2}-1$ for $t \in [\frac{k}{2}-2]$. Therefore, combining with the fact that the degree of h is $\frac{k}{2}$, we know that the degrees of $x_0, x_2, \ldots, x_{k-4}$ are all k by (15). Similarly,

$$\bar{y}_{2t}\bar{y}_{2t+2}\bar{y}_{k-4}\cdot f = \bar{y}_{2t}\bar{y}_{2t+2}\cdots\bar{y}_{k-4}\Big(y_0 + \bar{y}_1\big(\cdots(y_{2t-4} + \bar{y}_{2t-3}y_{2t-2})\cdots\big)\Big)$$

always has degree $\frac{k}{2}-1$ for $t \in \{1, 2, \cdots, \frac{k}{2}-2\}$. Thus, the degrees of $x_0, x_1, \ldots, x_{k-4}$ are all k.
To investigate the algebraic degrees of $x_{k+1}, x_{k+2}, \ldots, x_{2k-1}$, we need to consider x_{k-1} and x_k. By (18) and (21),

$$\begin{aligned}
x_{k-1} &= y_{k-2} + (\bar{y}_{k-1} + \bar{y}_{k-3}\cdot g + f\cdot h\cdot y_{k-2} + f\cdot F + f\cdot\bar{y}_k\cdot g)\cdot e + (G + y_{k-2})\\
&= G + \bar{y}_{k-1}\cdot e + \bar{y}_{k-3}\cdot g\cdot e + (h\cdot y_{k-2} + F + \bar{y}_k\cdot g)\cdot f\cdot e\\
&= G + \bar{y}_{k-1}\cdot e + \bar{y}_{k-3}\cdot g\cdot e
\end{aligned}$$

has degree k since the degrees of g and e are $\frac{k}{2}$ and $\frac{k}{2}-1$, respectively. Then

$$\begin{aligned}
&\bar{y}_{2t+1}\bar{y}_{2t+3}\cdots\bar{y}_{2k-1}\cdot g\\
&= \bar{y}_{2t+1}\bar{y}_{2t+3}\cdots\bar{y}_{2k-1}\Big(\bar{y}_{k+1} + \bar{y}_{k+2}\Big(y_{k+3} + \bar{y}_{k+4}\big(\cdots(y_{2t-3} + \bar{y}_{2t-2}y_{2t-1})\cdots\big)\Big)\Big)
\end{aligned}$$

always has degree $\frac{k}{2}$ for $t \in \{\frac{k}{2}+1, \frac{k}{2}+2, \ldots, k-1\}$. This implies that $\bar{y}_{2t+1}\bar{y}_{2t+3}\cdots\bar{y}_{2k-1}\cdot x_{k-1}$ always has degree k for $t \in \{\frac{k}{2}+1, \frac{k}{2}+2, \ldots, k-1\}$. So $x_{k+2}, x_{k+4}, \ldots, x_{2k-2}$ have degree k by (17). Similarly,

$$x_k = y_{k-3} + \bar{x}_{k-2}\cdot f = y_{k-3} + f\cdot(\bar{y}_k + h\cdot x_{k-1} + F),$$

has degree k since the degrees of f and h are $\frac{k}{2}-1$ and $\frac{k}{2}$, respectively. Then

$$\begin{aligned}
\bar{x}_{k-1}x_k &= \bar{x}_{k-1}\cdot(y_{k-3} + f\cdot\bar{y}_k + f\cdot F)\\
&= (\bar{G} + \bar{y}_{k-1}\cdot e)y_{k-3} + \bar{y}_{k-2}\bar{y}_k\cdot f + \bar{y}_{k-2}\cdot f\cdot F,
\end{aligned}$$

and

$$\begin{aligned}
&\bar{y}_{2t}\bar{y}_{2t+2}\cdots\bar{y}_{2k-2}\cdot F\\
&= \bar{y}_{2t}\bar{y}_{2t+2}\cdots\bar{y}_{2k-2}\Big(\bar{y}_{k+1}\Big(y_{k+2} + \bar{y}_{k+3}\big(\cdots(y_{2t-4} + \bar{y}_{2t-3}y_{2t-2})\cdots\big)\Big)\Big)
\end{aligned}$$

always has degree $\frac{k}{2}$ for $t \in \{\frac{k}{2}+2, \frac{k}{2}+3, \ldots, k-1\}$, and is 0 when $t = \frac{k}{2}+1$. So $x_{k+1}, x_{k+3}, \ldots, x_{2k-1}$ have degree k. This completes proof. ■