The Fourier spectral characterization for the correlation-immune functions over $\mathbb{F}_p$

Zilong Wang1 · Jinjin Chai1 · Guang Gong2

Received: 18 December 2018 / Accepted: 6 May 2019 / Published online: 16 May 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract
The correlation-immune functions serve as an important metric for measuring resistance of a cryptosystem against correlation attacks. Existing literature emphasize on matrices, orthogonal arrays and Walsh-Hadamard spectra to characterize the correlation-immune functions over $\mathbb{F}_p$ ($p \geq 2$ is a prime). Recently, Wang and Gong investigated the Fourier spectral characterization over the complex field for correlation-immune Boolean functions. In this paper, the discrete Fourier transform (DFT) of non-binary functions was studied. It was shown that a function $f$ over $\mathbb{F}_p$ is $m$th-order correlation-immune if and only if its Fourier spectrum vanishes at a specific location under any permutation of variables. Moreover, if $f$ is a symmetric function, $f$ is correlation-immune if and only if its Fourier spectrum vanishes at only one location.

Keywords Discrete Fourier transform · Correlation-immunity · Resiliency · Non-binary function

Mathematics Subject Classification (2010) 42A38 · 94A60

1 Introduction

Correlation immunity is one of the important properties for cryptographic functions. It was introduced to prevent some cryptosystems from correlation attacks [14, 16] (or ‘divide and

This article is part of the Topical Collection on Special Issue on Sequences and Their Applications

Zilong Wang
zlwang@xidian.edu.cn

Jinjin Chai
jj.chai@163.com

Guang Gong
ggong@uwaterloo.ca

1 State Key Laboratory of Integrated Service Networks, School of Cyber Engineering, Xidian University, Xi’an, China
2 Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
conquer attack’ proposed by Siegenthaler [15]). Moreover, correlation-immune functions are closely related to secret-sharing schemes and error-correcting codes [1, 5, 12, 20]. The constructions of correlation-immune functions with desired nonlinearity, algebraic immunity, propagation and strict avalanche criteria, such as [3, 4, 17, 18, 23], just list a few here, were well studied.

There are several methods to characterize correlation-immune Boolean functions. In 1989, Xiao and Massey [21] showed that a Boolean function is \( m \)-th order correlation-immune if and only if its Walsh-Hadamard transform vanishes for all points with Hamming weights between 1 and \( m \). A similar concept, called invariants of Boolean functions, which measure the distances between a Boolean function and all affine functions, was introduced by Golomb [7, 8] in 1959. In fact, invariants are the same concept of Walsh-Hadamard spectral characterization of correlation-immune functions. But the motivation to propose the invariants of Boolean functions was not explicitly mentioned until 1999 [9]. In addition to Walsh-Hadamard spectral characterization, other methods to characterize correlation-immune Boolean functions, such as matrices [11], orthogonal arrays [1, 2], and Fourier spectra [19] were proposed.

For non-binary functions, the characterization of correlation immunity was also studied. Zhang and Xiao [22] proved that a function \( f \) over \( \mathbb{F}_p \) for \( p \) prime is \( m \)-th order correlation-immune if and only if its Chrestenson cyclic spectrum vanishes for all points with weights between 1 and \( m \) by generalizing Walsh-Hadamard spectral characterization. Gopalakrishnan and Stinson [11] investigated the correlation-immune functions over the finite fields and derived their matrices, spectra, and orthogonal arrays characterizations. Feng [6] obtained two necessary and sufficient conditions for the correlation-immune functions over \( \mathbb{Z}_N \) in terms of Chrestenson linear spectrum and Chrestenson cyclic spectrum. It is clear that the methods to characterize the correlation-immune functions, including Walsh-Hadamard spectra, matrices, orthogonal arrays, were all generalized from the Boolean functions to non-binary functions.

Recently, Wang and Gong [19] investigated discrete Fourier transform over the complex field of Boolean function \( f(x) \), and deduced an equivalent condition for an \( m \)-th order correlation-immune Boolean function, that is, the Fourier spectrum of \( f(x) \) under any permutation of \( n \) variables vanishes at a particular location. Inspired by this result, we try to characterize \( m \)-th order correlation-immune functions over \( \mathbb{F}_p \) for \( p \) prime by discrete Fourier transform over the complex field. However, the method used in [19] cannot be extended to prove the result here. In this paper, we used a different approach than the literature [19], and obtained that a function \( f \) over \( \mathbb{F}_p \) is \( m \)-order correlation-immune if and only if its Fourier spectrum vanishes at a specific location under any permutation of variables. In particular, a symmetric function \( f \) is correlation-immune if and only if its Fourier spectrum vanishes at a specific location. The Fourier spectral characterization for Boolean functions in [19] can be regarded as a special case of the results in this paper for \( p = 2 \).

The rest of this paper is organized as follows. In Section 2, we introduce the definitions of the correlation immunity, resiliency and discrete Fourier transform over the complex field of the functions, review previous results on the characterizations of correlation-immune functions over \( \mathbb{F}_p \) as well. In Section 3, we present the main result on Fourier spectral characterization of correlation-immune functions. In Section 4, we show an equivalent condition for \( m \)-order resilient functions. Section 5 concludes the paper.
2 Preliminaries

Let \( f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p \) be a function with variable \( x = (x_1, x_2, \ldots, x_n) \), where \( \mathbb{F}_p \) denotes Galois Field with \( p \) elements for prime \( p \), and \( \mathbb{F}_p^n = \{(x_1, x_2, \ldots, x_n)|x_i \in \mathbb{F}_p, 1 \leq i \leq n\} \) represents an \( n \)-dimensional vector space over \( \mathbb{F}_p \).

2.1 Correlation immunity and resiliency

**Definition 1** Let \( X_1, X_2, \ldots, X_n \) be independent and uniformly distributed random variables (that is, for any \( a \in \mathbb{F}_p \), assume that \( P(X_i = a) = \frac{p-1}{p}, 1 \leq i \leq n \)). A function \( f \) is said to be \( m \)-th order correlation-immune if the random variable \( Z = f(X_1, X_2, \ldots, X_n) \) is statistically independent of every \( m \)-subset of random variables chosen from \( X_1, X_2, \ldots, X_n \), which means

\[
P_r(Z = t|X_{ij} = a_j, 1 \leq j \leq m) = P_r(Z = t),
\]

for every \( m \)-subset \( \{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} \), \( a_j \in \mathbb{F}_p (1 \leq j \leq m) \), and \( t \in \mathbb{F}_p \).

A function \( f \) is said to be balanced if every possible output occurs with equal probability \( \frac{1}{p^n} \). Furthermore, if \( f \) is \( m \)-th order correlation-immune and balanced, then \( f \) is said to be \( m \)-resilient.

2.2 Associated polynomial

We describe a sequence \( f \) of length \( p^n \) corresponding to the function \( f \) by listing the values taken by \( f(x_1, x_2, \ldots, x_n) \) as \( (x_1, x_2, \ldots, x_n) \) which ranges over all its \( p^n \) values in lexicographic order. In other words, sequence \( f \) is defined by

\[
f = (f(0), f(1), \ldots, f(p^n - 1)),
\]

where \( f(k) = f(x_1, x_2, \ldots, x_n) \) and \( (x_1, x_2, \ldots, x_n) \) is the \( p \)-adic representation of the integer \( k \) for \( 0 \leq k \leq p^n - 1 \), i.e., \( k = \sum_{i=1}^{n} x_i p^{i-1} \).

Let \( \omega = \exp\left(\frac{2\pi \sqrt{-1}}{p}\right) \) be a \( p \)-th primitive root of unity over the complex field. The polynomial associated with the function \( f(x_1, x_2, \ldots, x_n) \) is defined by the \( Z \)-transform of the sequence \( \omega^f = (\omega^{f(0)}, \omega^{f(1)}, \ldots, \omega^{f(p^n-1)}) \), i.e.,

\[
F(z) = \sum_{k=0}^{p^n-1} \omega^{f(k)} z^k.
\]

2.3 Discrete Fourier transform

We now introduce the concept of the discrete Fourier transform (DFT) over the complex field of the function \( f(x_1, x_2, \ldots, x_n) \), which actually is the DFT of the sequence described by function \( f \). Note that DFT over the complex field introduced here is the traditional DFT, which is different from the DFT over the finite field [10].
**Definition 2** Let $\xi = \exp \left( \frac{2\pi\sqrt{-1}}{N} \right)$ ($N = p^n$) be an $N$th primitive root of unity over the complex field. The discrete Fourier transform (DFT) of function $f(x_1, x_2, \cdots, x_n)$ over the complex field is defined by

$$\mathcal{F}_f (j) = \sum_{k=0}^{N-1} \omega_f^{(k)} \xi^{-kj}, \ 0 \leq j \leq N - 1.$$ (3)

Then the inverse discrete Fourier transform (IDFT) of the function $f(x_1, x_2, \cdots, x_n)$ is given by

$$\omega_f^{(k)} = \frac{1}{N} \sum_{j=0}^{N-1} \mathcal{F}_f (j) \xi^{kj}, \ 0 \leq k \leq N - 1.$$ 

Let $F_N = (f_{kj})$ be an $N \times N$ matrix whose entries are defined by $f_{kj} = \xi^{-kj}, \ 0 \leq k, j \leq N - 1$, i.e.,

$$F_N = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi^{-1} & \xi^{-2} & \cdots & \xi^{-(N-1)} \\ 1 & \xi^{-2} & \xi^{-4} & \cdots & \xi^{-2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{-(N-1)} & \xi^{-2(N-1)} & \cdots & \xi^{-1} \end{pmatrix}.$$ 

This is called the DFT matrix. Under this notation, we have DFT and IDFT respectively:

$$\begin{pmatrix} \mathcal{F}_f (0) \\ \mathcal{F}_f (1) \\ \vdots \\ \mathcal{F}_f (N - 1) \end{pmatrix} = F_N \begin{pmatrix} \omega_f^{(0)} \\ \omega_f^{(1)} \\ \vdots \\ \omega_f^{(N-1)} \end{pmatrix} \text{ and } \begin{pmatrix} \omega_f^{(0)} \\ \omega_f^{(1)} \\ \vdots \\ \omega_f^{(N-1)} \end{pmatrix} = \frac{1}{N} F_N^* \begin{pmatrix} \mathcal{F}_f (0) \\ \mathcal{F}_f (1) \\ \vdots \\ \mathcal{F}_f (N - 1) \end{pmatrix}$$

where $F_N^*$ is the Hermitian transpose of $F_N$, and the entries $f_{kj}^* = \xi^{kj}, \ 0 \leq k, j \leq N - 1$.

The relationship of DFT spectra of a sequence and its auto-correlation function has been studied before.

**Definition 3** Let $f$ be the sequence described by function $f(x): \mathbb{F}_p^n \rightarrow \mathbb{F}_p$. The auto-correlation function of $f$ is defined by

$$C_f (t) = \sum_{k=0}^{N-1} \omega_f^{(k+t)-f(k)}, \ 0 \leq t < N,$$

where $f(k)$ is defined by (1) and the addition in $(k+t)$ is over $\mathbb{Z}_N$.

It is known that the squared magnitude of the DFT spectra of $f(x)$ and the auto-correlation of sequence described by function $f(x)$ are a DFT pair, i.e.,

$$|\mathcal{F}_f (j)|^2 = \sum_{t=0}^{N-1} C_f (t) \xi^{-tj}, \ 0 \leq j < N$$

and

$$C_f (t) = \frac{1}{N} \sum_{j=0}^{N-1} |\mathcal{F}_f (j)|^2 \xi^{jt}, \ 0 \leq t < N.$$
Recall the definition of the DFT and associated polynomial of the function $f(x_1, x_2, \cdots, x_n)$, it is obvious that $F_f(j) = F(z = \xi^{-j})$. We shall use polynomial $F(z)$ to explore the DFT of function $f$ in the rest of the paper.

### 2.4 Previous results on the characterizations of correlation-immunity

Correlation-immune and resilient functions were initially defined by the probabilistic terminology (Definition 1), but it is difficult to determine the correlation-immune functions by probabilistic method. Therefore, some algebraic and combinatorial methods were proposed to characterize the correlation-immune functions. For $p = 2$, these methods to study Boolean functions refer to Walsh spectra [21], matrices [11], orthogonal arrays [2], and Fourier spectra [19]. For general prime $p$, the above first three characterizations of the correlation-immune functions were generalized to Chrestenson spectra [6], matrices [11], and orthogonal arrays [11], respectively.

Chrestenson transform, which is also referred to generalized Walsh-Hadamard transform in the literature, was introduced in [6, 22] to study the correlation-immunity of the non-binary functions. For a vector $c = (c_1, c_2, \cdots, c_n) \in \mathbb{F}_p^n$, let $wt(c)$ denotes the Hamming weight of $c$.

**Definition 4** Chrestenson linear spectrum of $f(x)$ is defined by

$$S_f(c) = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} f(x)\omega^{c \cdot x},$$

and Chrestenson cyclic spectrum of $f(x)$ is given by

$$S(f)(c) = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} \omega^ {f(x) - c \cdot x},$$

respectively, where $\omega = exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$, $c \cdot x = c_1x_1 + c_2x_2 + \cdots + c_nx_n$ is the inner product of $c$ and $x$.

Correlation-immune functions are characterized by their Chrestenson spectra.

**Fact 1** [6] $f$ is $m$th-order correlation-immune $\iff S_{f+a}(c) = 0$ for $\forall a \in \mathbb{F}_p$ and $\forall c \in \mathbb{F}_p^n$ with $1 \leq wt(c) \leq m$.

**Fact 2** [6, 22] $f$ is $m$th-order correlation-immune $\iff S_{(f)}(c) = 0$ for $\forall c \in \mathbb{F}_p^n$ with $1 \leq wt(c) \leq m$.

For $\forall c \in \mathbb{F}_p^n$, define a $p \times p$ matrix $N = N(c) = (n_{ij})$, where

$$n_{ij} = p^n \cdot P_{\xi}(x \cdot c = i \text{ and } f(x) = j), i, j \in \mathbb{F}_p.$$

Correlation-immune functions are characterized by the following matrix method.

**Fact 3** [11] $f$ is $m$th-order correlation-immune $\iff$ the rows of the matrix $N(c)$ are all identical for $\forall c \in \mathbb{F}_p^n$ with $1 \leq wt(c) \leq m$.

An $M \times n$ matrix $A$ with entries from a set of $p$ elements is an orthogonal array if any set of $m$ columns of $A$ contains all $p^m$ possible row vectors exactly $M/p^n$ times. Such an array
is denoted by \((M, n, p, m)\). Define \(W_i = \{ x \in \mathbb{F}_p^n : f(x) = i \}\) and \(b_i = |W_i|\). Construct an array \(B_i\) whose rows are elements of \(W_i\). Then \(B_i\) is a \(b_i \times n\) array for \(0 \leq i \leq p - 1\).

**Fact 4** \([11]\) \(f\) is \(m\)th-order correlation-immune \(\iff B_i\) is a \((b_i, n, p, m)\) orthogonal array for every \(i\) with \(0 \leq i \leq p - 1\).

Fourier spectrum characterization for the correlation-immune Boolean functions was proposed by Wang and Gong in \([19]\). We shall generalize these results to functions from \(\mathbb{F}_p^n\) to \(\mathbb{F}_p\) for prime \(p\).

### 3 Fourier spectrum characterization for correlation-immune functions

Let \(\pi\) be a permutation of symbols \(\{1, 2, \cdots, n\}\), \(f_\pi = f(x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(n)})\) a function obtained by permuting the variables in \(f(x_1, x_2, \cdots, x_n)\), and \(F_\pi(z)\) the polynomial associated with the function \(f_\pi\).

For any integer \(d\), let \(\Phi_d(z)\) denote the \(d\)th cyclotomic polynomial \([13]\). Then \(\Phi_d(z)\), a monic polynomial with integer coefficients, is the minimal polynomial over the rational field of any primitive \(d\)th-root of unity. The main result of the paper is given as follows.

**Theorem 1** Let \(f(x_1, x_2, \cdots, x_n)\) be a function from \(\mathbb{F}_p^n\) to \(\mathbb{F}_p\) for \(p\) prime. Then \(f\) is \(m\)th-order correlation-immune if and only if

\[
\Phi_{pm}(z) | F_\pi(z),
\]

for any permutation \(\pi\).

Since \(\Phi_{pm}(z)\) is the minimal polynomial of \(\xi^{-p^n-m}\) with respect to polynomial ring with rational coefficients, where \(\xi = \exp\left(\frac{2\pi \sqrt{-1}}{p^n}\right)\) in Definition 2, \(\Phi_{pm}(z) | F_\pi(z)\) if and only if \(F_\pi\left(\xi^{-p^n-m}\right) = 0\). Recall the definition of DFT of the function, we have \(\mathcal{F}_{f_\pi}(p^{n-m}) = F_\pi\left(z = \xi^{-p^n-m}\right)\). Fourier spectrum characterization of the correlation-immune functions is obtained immediately.

**Corollary 1** Let \(f(x_1, x_2, \cdots, x_n)\) be a function from \(\mathbb{F}_p^n\) to \(\mathbb{F}_p\) for \(p\) prime. Then \(f\) is \(m\)th-order correlation-immune if and only if

\[
\mathcal{F}_{f_\pi}(p^{n-m}) = 0,
\]

for any permutation \(\pi\).

Before giving a proof for Theorem 1, we study the cyclotomic polynomial \(\Phi_{pm}(z)\) first. It is obvious from the definition of cyclotomic polynomial that

\[
\Phi_{pm}(z) = \prod \left\{ \left( z - \xi^j \right) : 0 \leq j \leq p^n - 1, \gcd\left(j, p^n\right) = p^{n-m} \right\},
\]

where \(\gcd\) denotes the great common divisor. On the other hand, since

\[
z^N - 1 = \prod_{d|N} \Phi_d(z),
\]

\(\xi\) Springer
we have
\[ z^{p^m} - 1 = \prod_{j=0}^{m} \Phi_{p^j}(z) = \Phi_{p^m}(z) \Phi_{p^{m-1}}(z) \cdots \Phi_{p}(z) \Phi_1(z), \]
and
\[ z^{p^{m-1}} - 1 = \prod_{j=0}^{m-1} \Phi_{p^j}(z) = \Phi_{p^{m-1}}(z) \Phi_{p^{m-2}}(z) \cdots \Phi_{p}(z) \Phi_1(z). \]

So we conclude that
\[ \Phi_{p^m}(z) = \frac{z^{p^m} - 1}{z^{p^{m-1}} - 1} = \sum_{j=0}^{p-1} \left( z^{p^{m-1}} \right)^j. \]  \hspace{1cm} (4)

For ease of illustration, we first consider permutation \( \pi \) to be identity, and describe the connection between \( \Phi_{p^m}(z) |_{F(z)} \) and probabilistic expression.

**Lemma 1** Let \( f(x_1, x_2, \ldots, x_n) \) be a function from \( \mathbb{F}_p^m \) to \( \mathbb{F}_p \). Then \( \Phi_{p^m}(z) |_{F(z)} \) if and only if
\[ X_m \to X_1, X_2, \ldots, X_{m-1} \to f(X_1, X_2, \ldots, X_n) \]
is a markov chain, or alternatively, for \( \forall t \in \mathbb{F}_p \),
\[ P_r(f(x) = t | x_1, \ldots, x_{m-1}, x_m) = P_r(f(x) = t | x_1, \ldots, x_{m-1}). \]

**Proof** Since
\[ F(z) = \sum_{k=0}^{p^m-1} \omega_f^f(k) z^k = \sum_{x \in \mathbb{F}_p^m} \omega_f(x) \prod_{i=1}^{n} \left( z^{p^i-1} \right)^{x_i}, \]
we have
\[ \Phi_{p^m}(z) |_{F(z)} \iff F(z) \equiv 0(\text{mod } \Phi_{p^m}(z)) \iff \sum_{x \in \mathbb{F}_p^m} \omega_f(x) \prod_{i=1}^{n} \left( z^{p^i-1} \right)^{x_i} \equiv 0(\text{mod } \Phi_{p^m}(z)). \]

From the definition of the cyclotomic polynomial, we know
\[ \Phi_{p^m}(z) |_{z^{p^i} - 1}, \text{ for } \forall i \geq m, \]
so
\[ \Phi_{p^m}(z) |_{F(z)} \iff \sum_{x \in \mathbb{F}_p^m} \omega_f(x) \prod_{i=1}^{n} \left( z^{p^i-1} \right)^{x_i} \equiv 0(\text{mod } \Phi_{p^m}(z)). \]  \hspace{1cm} (5)

From the formula of the cyclotomic polynomial in (4), we have
\[ \left( z^{p^{m-1}} \right)^{p-1} \equiv -\sum_{j=0}^{p-2} \left( z^{p^{m-1}} \right)^j (\text{mod } \Phi_{p^m}(z)). \]

Then the summation in (5) can be divided into two parts, where the first part is for \( x_m \neq p - 1 \) and the second part is for \( x_m = p - 1 \). Hence \( \Phi_{p^m}(z) |_{F(z)} \) is equivalent to
\[ \sum_{x_1, \ldots, x_{m-1}} \omega_f^f(x) \prod_{i=1}^{m} \left( z^{p^i-1} \right)^{x_i} + \sum_{x_1, \ldots, x_{m-1}} \omega_f^f(x) |_{x_m = p-1} \prod_{i=1}^{m-1} \left( z^{p^i-1} \right)^{x_i} \left( -\sum_{j=0}^{p-2} \left( z^{p^{m-1}} \right)^j \right) \equiv 0(\text{mod } \Phi_{p^m}(z)). \]
Combining like terms about \( z \), the above condition is equivalent to \( x_m \neq m - 1, j \)

\[
\sum_{j=0}^{p-2} \sum_{x_{m+1}, \ldots, x_n} \left( \sum_{x_m=j, x_{m+1}, \ldots, x_n} (\omega^f(x)|_{x_m=j} - \omega^f(x)|_{x_m=p-1}) \right) z^{j p^{m-1} + \sum_{i=1}^{m-1} p^{i-1} x_i} \equiv 0 \pmod{\Phi_{p^m}(z)}.
\]

Since \( j p^{m-1} + \sum_{i=1}^{m-1} p^{i-1} x_i \), the degree of the item \( z^{j p^{m-1} + \sum_{i=1}^{m-1} p^{i-1} x_i} \), must be less than Euler function \( \varphi(p^m) = p^m - p^{m-1} \), which is the degree of \( \Phi_{p^m}(z) \), for \( j \leq p - 2 \), it follows that, for \( 0 < x_1, x_2, \ldots, x_{m-1} \leq p - 1 \), and \( 0 < j \leq p - 2 \),

\[
\sum_{x_{m+1}, \ldots, x_n} \left( \omega^f(x)|_{x_m=j, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} - \omega^f(x)|_{x_m=p-1, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} \right) = 0,
\]

which is equivalent to

\[
\sum_{t=0}^{p-1} \left( \#\{x : f(x)|_{x_m=j, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} - \#\{x : f(x)|_{x_m=p-1, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} \right) \omega^t = 0,
\]

where \( \#\{\cdot\} \) denotes the number of elements in the collection \( \{\cdot\} \).

Recall that the minimal polynomial of \( \omega \) is \( \Phi_p(z) = 1 + z + z^2 + \cdots + z^{p-1} \) with respect to integer polynomial ring, any polynomial \( g(z) \) in integer polynomial ring with \( g(\omega) = 0 \) must be a multiple of \( \Phi_p(z) \). Therefore,

\[
\#\{x : f(x)|_{x_m=j, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} - \#\{x : f(x)|_{x_m=p-1, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} = c
\]

for all \( t \), where \( c \) is a constant. Since

\[
\sum_{t=0}^{p-1} \#\{x : f(x)|_{x_m=j, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} = p^{n-m}
\]

for \( 0 < j \leq p - 2 \), and

\[
\sum_{t=0}^{p-1} \#\{x : f(x)|_{x_m=p-1, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} = p^{n-m},
\]

we obtain that

\[
\sum_{t=0}^{p-1} \left( \#\{x : f(x)|_{x_m=j, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} - \#\{x : f(x)|_{x_m=p-1, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} \right) = 0.
\]

It follows from (6) and (7) that

\[
\#\{x : f(x)|_{x_m=j, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} - \#\{x : f(x)|_{x_m=p-1, x_{m+1}, \ldots, x_m=p-1, x_{m+1}, \ldots, x_n} = t\} = 0.
\]

In other words,

\[
P_r(f(x) = t|x_m = j, x_1, \ldots, x_{m-1}) = P_r(f(x) = t|x_m = p - 1, x_1, \ldots, x_{m-1})
\]

for \( \forall t \) and \( \forall j \), i.e.,

\[
P_r(f(x) = t|x_1, \ldots, x_{m-1}, x_m) = P_r(f(x) = t|x_1, \ldots, x_{m-1}),
\]

which complete the proof.

We now prove Theorem 1 by applying permutation \( \pi \) and Lemma 1.

**Proof** From Lemma 1, we know that \( \Phi_{p^m}(z)|F(z) \) is equivalent to

\[
P_r(f(x) = t|x_m = j_1, x_1, \cdots, x_{m-1}) = P_r(f(x) = t|x_m = j_2, x_1, \cdots, x_{m-1}).
\]
For $1 \leq s \leq m - 1$, let $\pi = (s, m)$ denote a transposition. Such a permutation exchange the place of two elements $s$ and $m$, leaving the others fixed. $\Phi_{\rho^m}(z)|F_\pi(z)$ for all $\pi = (s, m)$ is equivalent to that $P_r(f(\mathbf{x}) = t)$ does not depend on the values of $x_1, x_2, \cdots x_m$, i.e,

$$P_r(f(\mathbf{x}) = t|x_1, x_2 \cdots x_m) = P_r(f(\mathbf{x}) = t).$$

Then consider all the permutations, we obtain

$$P_r(f(\mathbf{x}) = t|x_{\pi(1)}, x_{\pi(2)} \cdots , x_{\pi(m)}) = P_r(f(\mathbf{x}) = t),$$

which is exactly the definition of the $m$th-order correlation-immune function.

**Definition 5** A function $f$ is called a symmetric function if permuting its variables $(x_1, x_2, \cdots , x_n)$ leads to itself.

For symmetric function $f$, since $f = f_\pi$ for all permutations, the Fourier spectral characterization of the correlation-immunity is much simpler.

**Corollary 2** Let $f(x_1, x_2, \cdots , x_n) : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ be a symmetric function. Then $f$ is $m$th-order correlation-immune if and only if

$$F_f\left(p^n-m\right) = 0.$$

**Example 1** For $p = 3, n = 4$, $f(x_1, x_2, x_3, x_4) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 + x_1x_2 + x_2x_3 + x_3x_4 + x_1x_3 + x_1x_4 + x_2x_4$ is a symmetric function.

Calculate the Fourier spectrum of $f(x_1, x_2, x_3, x_4)$ at position $3^4-1$. We have

$$F_f\left(3^4-1\right) = 0,$$

so $f$ is a first-order correlation-immune function.

Calculate the Fourier spectrum of $f(x_1, x_2, x_3, x_4)$ at position $3^4-2$. We have

$$F_f\left(3^4-2\right) \neq 0,$$

so $f$ is not a second-order correlation-immune function.

**4 Fourier spectrum characterization for resilient function**

In cryptographic applications, for avoiding statistical dependence between the plaintext and the ciphertext, the function $f(x_1, x_2, \cdots x_n)$ is always required to be balanced. The function $f(x_1, x_2, \cdots x_n)$ is said to be the $m$th-order resilient if $f(x_1, x_2, \cdots x_n)$ is balanced by fixing $m$ or fewer variables. From Section 3, we know that $f(x_1, x_2, \cdots x_n)$ is $m$th-order resilient function if and only if $F_f(0) = 0$ and $F_f(\rho^n-m) = 0$ for any permutation $\pi$. Here we show more results on the associated polynomial of function $f(x_1, x_2, \cdots x_n)$.

**Theorem 2** $f(x_1, x_2, \cdots x_n) : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ is $m$th-order resilient function if and only if

$$(z^{p^m} - 1)|F_\pi(z),$$

for any permutation $\pi$. 
Proof} For ease of illustration, first we consider permutation \( \pi \) to be an identity.

\[
(z^p - 1)|F(z) \iff F(z) \equiv 0 \left( \mod z^p - 1 \right)
\]

\[
\iff \sum_{x \in \mathbb{F}_p^n} \omega^f(x) \prod_{i=1}^n (z^{p^i-1})^{x_i} \equiv 0 \left( \mod z^p - 1 \right)
\]

\[
\iff \sum_{x \in \mathbb{F}_p^n} \omega^f(x) \prod_{i=1}^m (z^{p^i-1})^{x_i} = 0
\]

\[
\iff \sum_{x_1, \ldots, x_n} \left( \sum_{x_{m+1}, \ldots, x_n} \omega^f(x) \right) z^{\sum_{i=1}^m p^{i-1}x_i} = 0
\]

\[
\iff \sum_{x_m+1, \ldots, x_n} \omega^f(x) = 0 \text{ for any fixed } x_1, x_2, \cdots, x_m.
\]

(8)

Similar to proof of Theorem 1, we obtain

\[
\#\{x : f(x) | x_1, \ldots, x_{m-1} = t\}
\]

all have the same value for \( 0 \leq t \leq p - 1 \). Then \( f(x) \) is balanced for any fixed \( x_1, x_2, \cdots, x_m \). It is obvious that \( f(x) \) is balanced for any fixed \( x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(m)} \) when we apply permutation \( \pi \). Thus, \( f(x) \) is \( m \)-th-order resilient function. \( \square \)

5 Conclusions

In this paper, we introduced the discrete Fourier transform over the complex field of the function \( f(x) : \mathbb{F}_p^n \rightarrow \mathbb{F}_p \), and obtained the Fourier spectral characterization of correlation-immune and resilient functions. That is,

1. \( f(x) \) is \( m \)-order correlation-immune if and only if \( \mathcal{F}_{f_\pi}(p^{n-m}) = 0 \) for any permutation \( \pi \).
2. If \( f(x) \) is a symmetric function, \( f(x) \) is \( m \)-order correlation-immune if and only if \( \mathcal{F}_{f}(p^{n-m}) = 0 \).
3. \( f(x) \) is \( m \)-th-order resilient if and only if \( \mathcal{F}_{f}(0) = 0 \) and \( \mathcal{F}_{f_\pi}(p^{n-m}) = 0 \) for any permutation \( \pi \).
4. The method used in [19] cannot be extended to prove the result for \( p > 2 \). However, Fourier spectral characterization for Boolean functions in [19] can be regarded as a special case of the results in this paper for \( p = 2 \).

Acknowledgments Z. Wang was supported in part by NSFC (No. 61671013, 61672410), NSF of Shaanxi Province (No. 2018JM6076), and the Programme of Introducing Talents of Discipline to Universities (China 111 Project, No. B16037)

References

1. Bierbrauer, J., Gopalakrishnan, K., Stinson, D.R.: Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds. SIAM J. Discret. Math. 9(3), 424–452 (1996)
2. Camion, P., Carlet, C., Charpin, P., Sendrier, N.: On correlation-immune functions. In: Advances in cryptology: Crypto’91 proceedings (lecture notes in computer science), vol. 576, pp. 86–100 (1991)
3. Carlet, C.: Boolean functions for cryptography and error correcting codes. Boolean models and methods in mathematics, computer science, and engineering 2, 257–397 (2010)
4. Carlet, C., Chen, X.: Constructing low-weight $\delta$th-order correlation-immune boolean functions through the fourier-hadamard transform. IEEE Trans. Inf. Theory 64(4), 2969–2978 (2018)
5. Ding, C., Xiao, G., Shan, W.: The stability theory of stream ciphers. Springer Science & Business Media (1991)
6. Feng, D.: Three characterizations of correlation-immune functions over rings $\mathbb{Z}_n$. Theor. Comput. Sci. 226(1-2), 37–43 (1999)
7. Golomb, S.W.: On the classification of boolean functions. IRE Trans. circuit theory 6(5), 176–186 (1959)
8. Golomb, S.W.: Shift Register Sequences. San Francisco CA: Holden-Day (1967)
9. Golomb, S.W.: On the cryptanalysis of nonlinear sequences [invited paper]. In: Walker, M. (ed.) IMA International Conference on Cryptography and Coding Cryptography and Coding 1999. (Lecture Notes in Computer Science), vol. 1746. Springer, Berlin (1999)
10. Golomb, S.W., Gong, G.: Signal design for good correlation for wireless communication, cryptography, and radar. Cambridge University Press (2005)
11. Gopalakrishnan, K., Stinson, D.R.: Three characterizations of non-binary correlation-immune and resilient functions. Des. Codes Cryptogr. 5(3), 241–251 (1995)
12. Gopalakrishnan, K., Stinson, D.R.: Applications of designs to cryptography. The CRC handbook of combinatorial designs, pp. 549–557 (1996)
13. McEliece, R.J.: Finite field for scientists and engineers. Kluwer Academic Publishers (1987)
14. Rueppel, R.A.: Analysis and design of stream ciphers. Springer, Berlin (1986)
15. Siegenthaler, T.: Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inf. Theory 30(5), 776–780 (1984)
16. Siegenthaler, T.: Decrypting a class of stream ciphers using ciphertext only. IEEE Trans. Inf. Computers 34(1), 81–85 (1985)
17. Su, S., Tang, X.: Construction of rotation symmetric boolean functions with optimal algebraic immunity and high nonlinearity. Des. Codes Cryptogr. 71(2), 183–199 (2014)
18. Tang, D., Carlet, C., Tang, X.: A class of 1-resilient boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. Int. J. Found. Comput. Sci. 25(06), 763–780 (2014)
19. Wang, Z., Gong, G.: Discrete Fourier transform of boolean functions over the complex field and its applications. IEEE Trans. Inf. Theory 64(4), 3000–3009 (2018)
20. Wu, C., Dawson, E.: On construction of resilient functions. In: Australasian conference on information security and privacy, pp. 79–86 (1996)
21. Xiao, G., Massey, J.L.: A spectral characterization of correlation-immune combining functions. IEEE Trans. Inf. Theory 34(3), 569–571 (1988)
22. Zhang, M., Xiao, G.: Spectral characterization of the correlation-immunity of multiple-valued logic functions. Chin. Sci. Bull. 40(3), 182–184 (1995)
23. Zhang, W., Pasalic, E.: Generalized maiorana–mcfarland construction of resilient boolean functions with high nonlinearity and good algebraic properties. IEEE Trans. Inf. Theory 60(10), 6681–6695 (2014)

Publisher's note  Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.