International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Some Properties of Cryptographic Functions Employed in Wireless Communication Systems

Deep Singh, Amit Paul

Abstract: ***The wireless transmission of different type of data like images, texts, videos etc. through an open network is considered as prone with respect to several security threats and passive attacks. CDMA communication systems used for various wireless communications requires improved cryptographic algorithms and air interface security checks. The*** q***-ary cryptographic function with suitable properties are key elements in providing secure transmission of data through wireless network. In this paper, we use the Walsh-Hadamard spectrum as a fundamental tool for analysis of some properties of generalized*** q***-ary functions. We generalize some existing results obtained for Boolean functions to the*** q***-ary functions and obtain some new characterization of*** q***-ary functions based on spectral analysis.***

Keywords**: Crosscorrelation, CDMA (Code Division Multiple Access), q-ary functions, Walsh-Hadamard spectrum (WHS), Wireless systems.**

I. INTRODUCTION

CDMA (Code Division Multiple Access) systems like mobiles, computers, internet etc. have become an integral part of modern communication. The CDMA systems used for transmission of various type of signals, images, texts or videos must be capable of maintaining security from unauthorized interruption or atacks. The advent of 3G/4G technologies are more challenging/interesting to the service providers to introduce advanced technologies for encryption or authentication process in CDMA systems. Using suitable cryptographic algorithms, the CDMA systems are enabled to identify the genuine person/information and provide services to them by rejecting all the unauthorized versions. For this purpose a 32/64 bit ESM (Electronic Serial Number) and a 10 digit MIN (Mobile Identification Number) is used. A 64 bit key known as A-key stored in permanent memory of the system is the most precious number with respect to the authentication process in CDMA systems. Several cryptographic tools like CAVE (Cellular Authentication and Voice Encryption), LFSR based ORYX, and ECMEA are different level of communication through CDMA systems. Due to wireless environment and open networks, our communication faces number of security threats. The mobile transacation or mobile commerce Dan et al. [2] needs a high level security that can be achieved through CDMA systems by enabling CDMA message signaling encryption. Because of their spread spectrum communication and comprehensive security algorithms, it is almost impossible to interrupt communication through CDMA systems.

In the recent years, the Walsh-Hadamard spectrum has become an important tool for research in cryptography, especially in the design and characterization of cryptographically significant Boolean functions used in various type of cryptosystems. Xiao and Messey [16] have provided some results on spectrum characterization of correlation immune functions. Sarkar and Maitra [8] have generalized these results and showed that the Walsh-Hadamard spectrum of an n-variable, m correlation immune function is divisible by 2^{m+1}. Recently, Sarkar and Maitra [9], and Zhou et al. [15] have provided some interesting results based on spectrum analysis of Boolean functions.

A function from F_2^n to F_2 is called a Boolean function on n-variables. Several author have proposed several generalization of Boolean functions and analyze the effect of the Walsh-Hadamard spectrum on them. Let $\mathbb{Z}_q$ denote ring of integers modulo q. The additive group $\mathbb{Z}_q$ is isomorphic to $\mathbb{Z}_q = \{1, \xi, \xi^2, \dots, \xi^{q-1}\}$, the multiplicative group of complex q^{th} roots of unity. Kumar et al. [6] have generalized the notion of classical bent functions by considering functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, where $q \geq 2$ and n are positive integers.

Let $\mathcal{B}_{n,q}$ denote the set of generalized q-ary functions. The Walsh-Hadamard spectrum of $f \epsilon \mathcal{B}_{n,q}$ is a complex-valued function from Z_q^n to $\mathbb{C}$, the set of complex numbers and defined as follows

$$\frac{1}{q^{n/2}} W_f(u) = \sum_{x \epsilon Z_q^n} \xi^{f(x)+<x,u>}$$

Where $< x, u >$ denotes the usual inner product in Z_q^n.

A function $f \epsilon \mathcal{B}_{n,q}$ is generalized bent (or q-ary bent) if $|W_f(u)| = 1$ for every $u \epsilon Z_q^n$. The Boolean bent functions were introduced by Rothaus [7]. It can be noted that the generalized bent functions exist for every value of q and n, except when n is odd and $q = 2 \bmod 4$; whereas Boolean bent functions exist only for even n [6]. For more results on q –ary bent functions we refer to [1, 3-5, 13]. Generalized bent functions are widely applicable in Code-Division Multiple-Access communications systems [10].

The derivative of $f, g \epsilon \mathcal{B}_{n,q}$ at $a \epsilon Z_q^n$ is defined as

$D_{f,g}(a) = f(x) - g(x + a)$,

and for $f = g$,

Manuscript published on 30 September 2019
* Correspondence Author
Deep Singh*, Department of Mathematics, Central University of Jammu, Jammu, India. Email:deepsinghspn@gmail.com
Amit Paul, Department of Mathematics, University of Jammu, Jammu, India. Email: amitpaulcuj@gmail.com

$D_f(a) = f(x) - f(x+a)$, is called derivative of f at $a \epsilon Z_q^n$.
Let $f, g \epsilon \mathcal{B}_{n,q}$.

Then the sum

$$C_{f,g}(\alpha) = \sum_{x \epsilon Z_q^n} \xi^{f(x)-g(x+\alpha)}$$

is called the cross-correlation between the function f and g at $\alpha \epsilon Z_q^n$. Moreover, for $f = g$, the sum $C_{f,f}(\alpha) = C_f(\alpha)$ is called the autocorrelation of f at α.
The sum-of-squares-of-modulus indicator (SSMI) [11] of $f, g \epsilon \mathcal{B}_{n,q}$ is defined as

$$\sigma_{f,g} = \sum_{\alpha \epsilon Z_q^n} |C_{f,g}(\alpha)|^2,$$

and in particular, for $f = g$, the sum-of-squares-of-modulus indicator (SSMI) of $f \epsilon \mathcal{B}_{n,q}$ is defined as

$$\sigma_f = \sum_{\alpha \epsilon Z_q^n} |C_f(\alpha)|^2,$$

In this paper, we use the Walsh-Hadamard spectrum as a fundamental tool for analysis of some properties of generalized ternary functions. We generalize some existing results obtained for Boolean functions to the q-ary functions and obtain some new characterization of q -ary functions based on spectral analysis. We provide a relationship between the Walsh-Hadamard spectrum and the decompositions of any two q-ary functions. We provide a relationship between the Walsh-Hadamard spectrum and the autocorrelation of any two q-ary functions.
The following Lemma 1 is an important property and extensively used in the paper.

Lemma 1 [11] Let $\alpha \epsilon Z_q^n$. Then

$$\sum_{x \epsilon Z_q^n} \xi^{<\alpha,x>} = \begin{cases} q^n, & if\ \alpha = 0 \\ 0, & otherwise \end{cases} \qquad (1)$$

The following Lemma 2 provides a relationship between the crosscorrelation and the
autocorrelation of $f, g \epsilon \mathcal{B}_{n,q}$

Lemma 2 [11] Let $f, g \epsilon \mathcal{B}_{n,q}$. Then

$$\sigma_{f,g} = \sum_{\alpha \epsilon Z_q^n} |C_{f,g}(\alpha)|^2 = \sum_{\alpha \epsilon Z_q^n} C_f(\alpha) \overline{C_g(\alpha)}$$

II. MAIN RESULTS

In this section, we have discussed several properties of q-ary cryptographic functions employed in CDMA communication systems. The mathematical aspect of these functions is discussed by using theory of finite fields. In Theorem 1 and Theorem 2 below, we generalize the results of [15] to the q -ary functions.

Theorem 1 Let $f, g \epsilon \mathcal{B}_{n,p}$, where p is prime and V be a subspace of $\mathbb{Z}_p^n$ with $\dim(V) = k$. Then for any $\beta \epsilon \mathbb{Z}_p^n$, we have

$$\sum_{\alpha \epsilon V} W_f(\alpha + \beta)\, \overline{W_g(\alpha)} = p^k \sum_{\varepsilon \epsilon V^{\perp}} W_{D_{f,g}(\varepsilon)}(\beta)$$

Where $V^{\perp}$ denotes the dual of a subspace V, i.e., $V^{\perp} = \{x \epsilon \mathbb{Z}_p^n : \forall\ y \epsilon V, x.y = 0\}$.

***Proof*:** By the definition of the Walsh-Hadamard transform, we have

$$\sum_{\alpha \epsilon V} W_f(\alpha)\ \overline{W_g(\alpha + \beta)}$$

$$= \sum_{\alpha \epsilon V} \left(\frac{1}{p^{\frac{n}{2}}} \sum_{x \epsilon Z_p^n} \xi^{f(x)+<\alpha,x>} \right) \overline{\sum_{\alpha \epsilon V} \left(\frac{1}{p^{\frac{n}{2}}} \sum_{y \epsilon Z_p^n} \xi^{g(y)+<\alpha+\beta,y>} \right)}$$

$$= \frac{1}{p^n} \sum_{\alpha \epsilon V} \sum_{x,y \epsilon Z_p^n} \xi^{f(x)+<\alpha,x>-g(y)-<\alpha+\beta,y>}$$

$$= \frac{1}{p^n} \sum_{x,y \epsilon Z_p^n} \xi^{f(x)-g(y)-<\beta,y>} \sum_{\alpha \epsilon V} \xi^{<\alpha,x-y>}$$

Where $\sum_{\alpha \epsilon V} \xi^{<\alpha,x-y>} \neq 0$ if and only if $x - y\ \epsilon\ V^{\perp}$.
Therefore, we have

$$\frac{1}{p^n} \sum_{x,y \epsilon Z_p^n} \xi^{f(x)-g(y)-<\beta,y>} \sum_{\alpha \epsilon V} \xi^{<\alpha,x-y>}$$

$$= p^{k-n} \sum_{x,y \epsilon Z_p^n,\ x-y \epsilon V^{\perp}} \xi^{f(x)-g(y)-<\beta,y>}$$

$$= p^{k-n} \sum_{x,y \epsilon Z_p^n} \sum_{\varepsilon \epsilon V^{\perp}, y=x-\varepsilon} \xi^{f(x)-g(x-\varepsilon)-<\beta,x-\varepsilon>}$$

$$= p^{k-n} \sum_{\varepsilon \epsilon V^{\perp}} \xi^{<\beta,\varepsilon>} \sum_{x \epsilon Z_p^n} \xi^{f(x)-g(x-\varepsilon)-<\beta,x>}$$

$$= p^{k-n} \sum_{\varepsilon \epsilon V^{\perp}} \xi^{<\beta,\varepsilon>} \overline{\sum_{x \epsilon Z_p^n} \xi^{-f(x)+g(x-\varepsilon)+<\beta,x>}}$$

$$= p^{k-n} \sum_{\varepsilon \epsilon V^{\perp}} \xi^{<\beta,\varepsilon>} \overline{\sum_{z \epsilon Z_p^n} \xi^{g(z)-f(z+\varepsilon)+<\beta,z+\varepsilon>}}$$

$$= p^{k-n} \sum_{\varepsilon \epsilon V^{\perp}} p^{n/2}\, \overline{W_{D_{f,g}(\varepsilon)}(\beta)}$$

$$= p^{\frac{2k-n}{2}} \sum_{\varepsilon \epsilon V^{\perp}} p^{n/2}\, \overline{W_{D_{f,g}(\varepsilon)}(\beta)}$$

In particular, if $f = g$; then we have the following corollary
Corollary 1. Let $f, g \epsilon \mathcal{B}_{n,p}$, where p is prime and V be a subspace of $\mathbb{Z}_p^n$ with $\dim(V) = k$. Then

$$\sum_{\alpha \epsilon V} |W_f(\alpha + \beta)|^2 = p^k \sum_{\varepsilon \epsilon V^{\perp}} \xi^{<\beta,\varepsilon>}\, \overline{W_{D_f(\varepsilon)}(0)}\ \forall\ \beta \epsilon \mathbb{Z}_p^n$$

Let W be a subspace of $\mathbb{Z}_p^n$ $\dim(W) = k$. The decomposition of f with respect to W is the sequence $\{f_a : a \epsilon V\}$

where V is a subspace such that $\mathbb{Z}_p^n$ is the direct sum of W and V, and f_a is the function of k variables from W to $\mathbb{Z}_p$, defined as $f_a(x) = f(a+x)$ for any $x \epsilon W$.

In the following theorem, we investigate a relationship between the Walsh-Hadamard spectrum of $f, g \epsilon \mathcal{B}_{n,p}$ and the Walsh-Hadamard spectrum of the decompositions of f and g with respect to a subspace V of $\mathbb{Z}_p^n$.

Theorem 2 Let W be a subspace of $\mathbb{Z}_p^n$ with dim $(W) = k$; and $\{f_a : a \epsilon V\}$ and $\{g_a : a \epsilon V\}$ be the decompositions of f and g with respect to W. Then

$$\sum_{a \epsilon V^{\perp}} W_f(\alpha)\overline{W_g(\alpha)} = p^k \sum_{a \epsilon V} W_{f_a}(0)\overline{W_{g_a}(0)}$$

Proof: For any $e \epsilon \mathbb{Z}_p^n$, we have

$$C_{f,g}(e) = \sum_{z \epsilon \mathbb{Z}_p^n} \xi^{f(z)-g(z+e)}$$

$$= \sum_{a \epsilon V} \sum_{x \epsilon W} \xi^{f_a(x)-g_a(z+e)}$$

$$= \sum_{a \epsilon V} \sum_{x \epsilon W} \xi^{f(a+x)-g(a+x+e)}$$

From Theorem 1, for $\beta = 0$; we have

$$\sum_{a \epsilon W^{\perp}} W_f(\alpha)\overline{W_g(\alpha)} = p^k \sum_{e \epsilon W} C_{f,g}(e)$$

$$= p^k \sum_{e \epsilon W} \left(\sum_{z \epsilon \mathbb{Z}_p^n} \xi^{f(z)-g(z+e)} \right)$$

$$= p^k \sum_{e \epsilon W} \left(\sum_{a \epsilon V} \sum_{x \epsilon W} \xi^{f(a+x)-g(a+x+e)} \right)$$

$$= p^k \sum_{a \epsilon V} \sum_{x \epsilon W} \xi^{f(a+x)} \sum_{e \epsilon W} \xi^{-g(a+x+e)}$$

$$= p^k \sum_{a \epsilon V} \sum_{x \epsilon W} \xi^{f(a+x)} \sum_{y \epsilon W} \xi^{-g(a+y)}$$

$$= p^k \sum_{a \epsilon V} W_{f_a}(0)\overline{W_{g_a}(0)} \qquad (2)$$

In particular, if $f = g$, then we have the following corollary

Corollary 2. Let W be a subspace of $\mathbb{Z}_p^n$ of dimension k and $\{f_a : a \epsilon V\}$ be the decomposition of f with respect to W. Then

$$\sum_{a \epsilon W^{\perp}} |W_f(\alpha)|^2 = p^{\frac{2k-n}{2}} \sum_{a \epsilon V} |W_{f_a}(0)|^2$$

For any $\alpha \epsilon \mathbb{Z}_q^n$, where q is any integer, we have

$$|W_f(\alpha)|^2 = \sum_{a \epsilon \mathbb{Z}_p^n} \xi^{<a,\alpha>} \overline{C_f(a)} = \sum_{a \epsilon \mathbb{Z}_p^n} \xi^{<-a,\alpha>} C_f(a) \qquad (3)$$

In particular, if $\alpha = 0$ then

$$|W_f(\alpha)|^2 = \sum_{a \epsilon \mathbb{Z}_p^n} C_f(a)$$

In Theorem 3 below, we present a generalization of [14, Theorem 1] (obtained for q = 2) to the q-ary functions. To prove the result, we need following lemma.

Lemma 3 Let $f, g, h \epsilon \mathcal{B}_{n,q}$ such that $h(x) = f(x) - g(x)$. Then

$$W_h(v) = \frac{1}{q^{n/2}} \sum_{u \epsilon \mathbb{Z}_q^n} W_f(u+v)\overline{W_g(u)} \quad \forall\, v \epsilon \mathbb{Z}_q^n$$

Proof **:** For any $v \epsilon \mathbb{Z}_q^n$; using Lemma 1, we have

$$\sum_{u \epsilon \mathbb{Z}_q^n} W_f(u+v)\overline{W_g(u)}$$

$$= \frac{1}{q^n} \sum_{u \epsilon \mathbb{Z}_q^n} \sum_{x \epsilon \mathbb{Z}_q^n} \xi^{f(x)+<u+v,x>} \sum_{y \epsilon \mathbb{Z}_q^n} \xi^{-g(y)-<u,y>}$$

$$= \sum_{x,y \epsilon \mathbb{Z}_q^n} \xi^{f(x)-g(y)+<v,x>} \sum_{u \epsilon \mathbb{Z}_q^n} \xi^{<u,x-y>}$$

$$= q^n \sum_{x \epsilon \mathbb{Z}_q^n} \xi^{f(x)-g(x)+<v,x>}$$

$$= q^n \sum_{x \epsilon \mathbb{Z}_q^n} \xi^{h(x)+<v,x>}$$

$$= q^{n/2} W_h(v)$$

This completes proof

Theorem 3 If $f, g \epsilon \mathcal{B}_{n,q}$ and $e \epsilon \mathbb{Z}_q^n$, then for any $v \epsilon \mathbb{Z}_q^n$, we have

$$W_{D_e(f,g)}(v) = \frac{1}{q^{n/2}} \sum_{u \epsilon \mathbb{Z}_q^n} \xi^{<u,e>} W_f(u+v)\overline{W_g(u)} \qquad (4)$$

and

$$W_f(u+v)\overline{W_g(u)} = \frac{1}{q^{n/2}} \sum_{e \epsilon \mathbb{Z}_q^n} \xi^{-<u,e>} W_{D_e(f,g)}(v) \qquad (5)$$

Proof: Let $g_e(x) = g(e+x)$. Then

$$W_{g_e}(u) = \xi^{-<u,e>} W_g(u) \qquad (6)$$

From Lemma 3, replacing g by g_e and h by $D_e(f,g)$, we get

$$W_{D_e(f,g)}(v) = \frac{1}{q^{n/2}} \sum_{u \epsilon \mathbb{Z}_q^n} \xi^{<u,e>} W_f(u+v)\overline{W_{g_e}(u)} \qquad (7)$$

Combining equations (6) and (7), we obtain the desired result in (4). Now from Lemma 1 and (4), we have

$$\sum_{e\epsilon Z_q^n} \xi^{-<u,e>} W_{D_e(f,g)}(v)$$

$$= \frac{1}{q^{n/2}} \sum_{e\epsilon Z_q^n} \xi^{-<u,e>} \sum_{x\epsilon Z_q^n} \xi^{<x,e>} W_f(x+v)\overline{W_g(x)}$$

$$= \frac{1}{q^{n/2}} \sum_{x\epsilon Z_q^n} W_f(x+v)\overline{W_g(x)} \sum_{e\epsilon Z_q^n} \xi^{<e,x-u>}$$

$$= q^{n/2} W_f(u+v)\overline{W_g(u)}$$

Hence the result.

If $f = g$ and $v = 0$ in equation (4), then we get following corollary

Corollary 3. If $f \epsilon \mathcal{B}_{n,q}$, then the autocorrelation of f is given by

$$C_f(e) = \frac{1}{q^{n/2}} \sum_{u\epsilon Z_q^n} \xi^{<u,e>} |W_f(u)|^2 \qquad (8)$$

By putting $e = 0$ in above equation (8), we obtain

$$\sum_{u\epsilon Z_q^n} |W_f(u)|^2 = q^n$$

which is known as Parseval's identity in q-ary setup.

III. CONCLUSION

The CDMA air interface security systems requires improved cryptographic tools and algorithms. The cryptographic techniques addressing information/ message transmission security issues needed for quick and secure encryption and decryption of data and also for getting digital signatures with real times transmission are at the heart of CDMA systems. This paper is an attempt to address the mathematical concept of cryptographic algorithms with the help of q-ary functions. We have discussed some properties of q-ary functions which are useful in CDMA systems.

REFERENCES

1. C. Carlet, C. Dubuc, "On generalized bent and q-ary perfect nonlinear functions", Finite Fields and Their Applications, Springer-Verlag, 2001, pp. 81-94.
2. C. Dan, L. Yijun, and T. Jiali, "Analysis of security based on CDMA air interface system", Energy Procedia, Elsevier, 2012, pp. 2003-2010.
3. X. Hou , " q-ary bent functions constructed from chain rings", Finite Fields and Their Applications, Springer-Verlag, 1998, pp. 55-61.
4. X. Hou , "Bent functions, partial difference sets and quasi-Frobenius rings, Designs, Codes and Cryptography, Vol. 20, 2000, pp. 251-268.
5. X. Hou, " p-ary and q-ary versions of certain results about bent functions and resilient functions", Finite Fields and Applications, 2004, pp. 566-582.
6. P.V. Kumar, R. A. Scholtz, and L. R. Welch,"Generalized bent functions and their properties", Journal of Combinatirial Theory, Ser. A 1(40), 1985, pp.90-107.
7. O. S. Rothaus, "On Bent functions", Journal of Combinatorial Theory , Vol. 20, 1976, pp. 300-305.
8. Sarkar, P. and Maitra, S.: Constructions of nonlinear Boolean functions with important cryptographic properties', In Advances in Cryptology-Eurocrypt 2000, LNCS 1807, Vol. 20, 2000, pp. 485-506.
9. P. Sarkar, and S. Maitra, "Cross-correlation analysis of cryptographically useful Boolean functions", Theory of Computing Systems, Vol. 20, 2002, pp. 39-57.
10. K-U. Schmidt,."Quaternary constant-amplitude codes for multicode CDMA", IEEE Transactions on Information Theory , Vol. 55 No. 4, 2009, pp.1824-1832.
11. D. Singh, M. Bhaintwal, and B. K. Singh, "Some results on q-ary bent functions", Cryptology ePrint Archives, 2012, http://www.eprint.iacr.org/2012/037.pdf.
12. P. Sole, N. Tokareva, (2009) "Connections between quaternary and binary bent functions", Cryptology ePrint Archives, http://www.eprint.iacr.org/2009/544.
13. N. Tokareva, "Generalizations of bent functions: A survey", Cryptology ePrint Archives, 2011, http://eprint.iacr.org/2011/111.pdf.
14. Z. Zhuo, J. Chong, H. Cao, and G. Xiao, "Spectral analysis of two Boolean functions and their derivatives", Chinese Journal of Electronics , Vol. 20 No. 4, 2011, pp.747-749.
15. Y. Zhou, M. Xie, and G. Xiao, "On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity", Information Sciences , Vol. 180, 2010, pp.256-265.
16. Xiao, G. Z. and Messey, J. L.: A Spectral Characterization of Correlation-Immune Combing Functions, IEEE Transactions on Information Theory , Vol. 34, No. 3, 1988, pp. 569-571.

AUTHORS PROFILE

Deep Singh received his PhD in Mathematics at the Indian Institute of Technology, Roorkee, India. He is an Assistant Professor at the Department of Mathematics, Central University of Jammu, Samba, India. His research interests include theoretical cryptography, abstract algebra and discrete mathematics. He has published several research papers at national and international journals, conference proceedings.

Amit Paul received his PhD in Mathematics at the Department of Mathematics, Central University of Jammu, Samba, India. He is a Lecturer at the Department of Mathematics, University of Jammu, Jammu, India His research interests are theoretical cryptography, abstract algebra and discrete mathematics. He has published research papers at national and international journals, conference proceedings.