TWMS J. App. and Eng. Math. V.11, N.2, 2021, pp. 359-367

ALGEBRAIC CONSTRUCTION OF SEMI BENT FUNCTION VIA KNOWN POWER FUNCTION

P. POOJARY[1], HARIKRISHNAN P. K.[1], VADIRAJA BHATTA G. R.[2], §

Abstract. The study of semi bent functions (2- plateaued Boolean function) has attracted the attention of many researchers due to their cryptographic and combinatorial properties. In this paper, we have given the algebraic construction of semi bent functions defined over the finite field $\mathbb{F}_{2^n}$ (n even) using the notion of trace function and Gold power exponent. Algebraically constructed semi bent functions have some special cryptographical properties such as high nonlinearity, algebraic immunity, and low correlation immunity as expected to use them effectively in cryptosystems. We have illustrated the existence of these properties with suitable examples.

Keywords: Boolean function, trace, cryptography, nonlinearity, algebraic immunity.

AMS Subject Classification: 06E30, 94C10, 11T71.

1. Introduction

A finite field with 2^n elements denoted as $\mathbb{F}_{2^n}$, is basically an extended field of a two element field $\mathbb{F}_2 = \{0, 1\}$ using an irreducible polynomial of degree n over $\mathbb{F}_2$. Moreover $\mathbb{F}_{2^n}$ is isomorphic to n dimensional vector space over $\mathbb{F}_2$. A Boolean function in n variables is an arbitrary function from $\mathbb{F}_2^n \to \mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$ is a Boolean domain and n is a non-negative integer. Plateaued Boolean function was introduced by Zheng and Zhang in 1999 [15], as these functions have various cryptographic properties, these functions are used in the design of cryptographic algorithms that have resistance against some cryptographic attacks. Walsh Hadamard transform is an essential tool to define and design plateaued Boolean functions. If the values of its Walsh Hadamard transform belong to the set $\{0, \pm 2^{\frac{n+r}{2}}\}$ for some fixed r, $0 \leq r \leq n$, then the n-variable Boolean function is said to be r-plateaued. There are mainly three important classes of plateaued function, i.e., 0-plateaued functions, 1-plateaued functions, and 2-plateaued functions which have

[1] Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Karnataka, India.
e-mail: poojaryprasanna34@gmail.com; ORCID: https://orcid.org/0000-0002-0749-8994.
e-mail: pk.harikrishnan@manipal.edu; ORCID: https://orcid.org/0000-0001-7173-9951.
[2] Department of Mathematics, Center for Cryptography, Manipal Institute of Technology, Manipal Academy of Higher Education, Karnataka, India.
e-mail: vadiraja.bhatta@manipal.edu; ORCID: https://orcid.org/0000-0003-0631-0205.
§ Manuscript received: June 19, 2019; accepted: September 11, 2019.

attracted much attention due to their cryptographic algebraic and combinatorial properties [9]. 0-plateaued functions and 2-plateaued functions occur only in even dimension whereas 1-plateaued functions occur in odd dimension.

Bent functions were introduced by Rothaus in [1] and are also known as 0-plateaued functions. These functions are perfectly nonlinear and have interesting implication for designing block ciphers and stream ciphers. But these functions are not compatible with other cryptographic properties like high nonlinearity, balancedness, etc. Near bent functions are 1-plateaued functions and semi bent functions are 2-plateaued functions introduced by Chee et al. in [13]. Similar to bent function, near bent functions and semi bent functions are used to design block ciphers and stream ciphers and are widely used in sequences and cryptography. Unlike bent functions, these functions are compatible with other cryptographic properties like resilience, balancedness, and high nonlinearity.

Khoo et al. in 2002 [17] gave the construction of n- variable quadratic semi bent functions in polynomial forms for both odd and even n. Before his work, most of the researchers constructed semi bent functions from power polynomials for suitably chosen d, $f(x) = Tr(x^d)$. Later Charpin et al. in 2005 [2] showed the link between bent and semi bent function and presented the treatment of semi bent function. Then Dong et al. in 2013 presented a new method for constructing a semi bent function in polynomial form for both odd and even n with the help of few trace terms [3]. Cao et al. gave the general construction of semi bent functions in univariate representation and provided a link between some exponential sums involving Dickson polynomials and the semi bentness property of some infinite classes of Boolean function in univariate representation [5]. Then Mesnager and Zhang during 2017 in [6] constructed semi bent functions and Walsh Hadamard transform values built from the bent function. For recent results on the construction and the treatment of semi bent function, we refer [11, 9, 20, 7].

Most of the researchers have focused on the construction of semi bent functions of the form $Tr(x^d)$. And a few researchers gave the link between semi bent functions and bent functions. Also, a few of them constructed functions using multiple trace term. Here, in this paper we provide some supportive definitions which are used to construct and analyze semi bent functions over finite fields $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^6}$. Concerning some important cryptographic properties, the constructed functions are found to be useful in designing effective cryptosystems.

2. Preliminaries

For completeness, we give the following definition.

Definition 2.1. [11] *The Walsh Hadamard transform of a function f in n variables is the integer-valued function on $\mathbb{F}_2^n$, whose value at $a \in \mathbb{F}_2^n$ is defined as*

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+<a \cdot x>}.$$

Definition 2.2. [9] *A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called a semi bent if its Walsh Hadamard transform satisfies:*

$$W_f(a) \in \{0, \pm 2^{\frac{n+2}{2}}\} \text{ for all } a \in \mathbb{F}_{2^n}.$$

Semi bent functions on $\mathbb{F}_{2^n}$ exist only when n is even.

Definition 2.3. [10] *If c is an element of $K = GF(q^n)$, its trace relative to the subfield $F = GF(q)$ is defined as follows:*

$$Tr_F^K(c) = c + c^q + c^{q^2} + \ldots + c^{q^{n-1}}.$$

Definition 2.4. [4] *The vector space of n tuples of elements from $GF(2)$ is denoted as V_n. Let f and g be functions on V_n, which is a vector of n bits. Then, $d(f,g) = \sum_{f(x)\neq g(x)} 1$, where the addition is over the reals, is called the Hamming distance between f and g.*

Definition 2.5. [4] *Let $\psi_0, \ldots, \psi_{2^{n+1}-1}$ be the affine functions on V_n. Then, $N_f = min_{i=0,\ldots,2^{n+1}-1} d(f,\psi_i)$ is called the nonlinearity of f, where d denotes the Hamming Distance between the two functions f and ψ_i. It is well known that the nonlinearity of f on V_n satisfies $N_f \leq 2^{n-1} - 2^{n/2-1}$, when n is even.*

Definition 2.6. [9] *Let f be a Boolean function in n variables. A nonzero Boolean function g is called an annihilator of f if $fg = 0$.*

Definition 2.7. [9] *The algebraic immunity of f, denoted by $Al(f)$, is the minimum value of d such that f or its complement $1 + f$ admits an annihilator of algebraic degree d.*

Definition 2.8. [8] *A Boolean function f is said correlation immune of order t if and only if the walsh tranform of f vanishes at all non zero vectors of Hamming weight at most t.*

3. Algebraic construction of semi bent function using Gold power function exponent

Theorem 3.1. *The function defined on $\mathbb{F}_{2^4}$ by*

$$f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1}),$$

is a semi bent function for all odd i.

Proof. The field $\mathbb{F}_{2^4}$ is constructed with the rule $\alpha^4 = \alpha + 1$, where α is a zero of an irreducible polynomial of degree 4 over $\mathbb{F}_2$.
So, $x^{12} = x^3 + x^2 + x + 1$, i.e $(\alpha^{12})^{2^i+1})$ for odd i reduces to either α^3 or α^6. Hence, the function $f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1})$ for odd i reduces to either $Tr(\alpha^3) = Tr(x^3)$ or $Tr(\alpha^6) = Tr(x^3 + x^2)$. It is sufficient to prove that these functions are semi bent.
Calculating Walsh Hadamard transform we get, $W_f(a) \epsilon \{0, \pm 8\}$ for all $a \epsilon \mathbb{F}_{2^4}$, which means that $W_f(a) \epsilon \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $a \epsilon \mathbb{F}_{2^4}$. So the above functions are semi bent.
Hence, the functions defined on $\mathbb{F}_{2^4}$ by

$$f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1}),$$

is a semi bent function. □

Theorem 3.2. *The function defined on $\mathbb{F}_{2^4}$ by*

$$f(x) = Tr((x^3 + x^2 + x + 1)^{2^{4i}+1}),$$

is a semi bent function for all i.

Proof. By rule of construction, in $\mathbb{F}_{2^4}$, $x^{12} = x^3 + x^2 + x + 1$, i.e $(\alpha^{12})^{2^{4i}+1})$ for any i reduces to α^9. Hence, the function $f(x) = Tr((x^3 + x^2 + x + 1)^{2^{4i}+1})$ for any i reduce to $Tr(x^9) = Tr(x^3 + x)$.
It is sufficient to prove that these functions are semi bent.
Calculating Walsh Hadamard transform we get, $W_f(a) \epsilon \{0, \pm 8\}$ for all $a \epsilon \mathbb{F}_{2^4}$, which

means that $W_f(a) \epsilon \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $a \epsilon \mathbb{F}_{2^4}$. So the above functions are semi bent. Hence, the functions defined on $\mathbb{F}_{2^4}$ by

$$f(x) = Tr((x^3 + x^2 + x + 1)^{2^{4i}+1}),$$

is a semi bent function. □

If i is neither odd nor a multiple of 4, then the functions $f(x) = Tr((x^3+x^2+x+1)^{2^i+1})$ and $f(x) = Tr((x^3+x^2+x+1)^{2^{4i}+1})$ cannot be semi bent functions, which can be observed from the following examples.

Example 3.1. *Over $\mathbb{F}_{2^4}$, the function $f(x) = Tr((x^3+x^2+x+1)^{2^2+1})$ is not a semi bent function.*
In fact, the Walsh Hadamard transform values $W_f(a)$ are 0 or -16, for all $a \epsilon \mathbb{F}_{2^4}$. Hence $Tr(x^3 + x^2 + x + 1)^5$ is a not a semi bent function.

Example 3.2. *Over $\mathbb{F}_{2^4}$, the function $f(x) = Tr((x^3+x^2+x+1)^{2^6+1})$ is not a semi bent function.*
In fact, the Walsh Hadamard transform values $W_f(a)$ are 0 or -16, for all $a \epsilon \mathbb{F}_{2^4}$. Hence $Tr(x^3 + x^2 + x + 1)^{65}$ is a not a semi bent function.

Theorem 3.3. *The function defined on $\mathbb{F}_{2^6}$ by*

$$f(x) = Tr((x^4 + x)^{2^i+1}),$$

is a semi bent function with $\gcd(i, 6) = 1$.

Proof. In $\mathbb{F}_{2^n}$, $x^{14} = x^4 + x$, i.e $(\alpha^{14})^{2^i+1})$ reduces to α^{21} or α^{42} if $\gcd(i, 6) = 1$. Hence, the function $f(x) = Tr((x^4+x)^{2^i+1})$ for $\gcd(i, 6) = 1$ reduce to $Tr(x^{21}) = Tr(x^3+x^2+x)$ or $Tr(x^{42}) = Tr(x^3 + x^2 + x + 1)$.
It is sufficient to prove that these functions are semi bent.
Calculating Walsh Hadamard transform we get, $W_f(a) \epsilon \{0, \pm 16\}$ for all $a \epsilon \mathbb{F}_{2^6}$, which means that $W_f(a) \epsilon \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $a \epsilon \mathbb{F}_{2^6}$. So the above functions are semi bent. Hence, the functions defined on $\mathbb{F}_{2^6}$ by

$$f(x) = Tr((x^4 + x)^{2^i+1}),$$

is a semi bent function if $\gcd(i, 6) = 1$. □

If $\gcd(i, 6) \neq 1$, then the functions $f(x) = Tr((x^4+x)^{2^i+1})$ cannot be semi bent function, which we can be observed from the following examples.

Example 3.3. *Over $\mathbb{F}_{2^6}$, the function $f(x) = Tr((x^4+x)^{2^3+1})$ is not a semi bent function. In fact, the Walsh Hadamard transform values $W_f(a)$ are 0 or -64, for all $a \epsilon \mathbb{F}_{2^6}$. Hence $Tr(x^4 + x)^9$ is a not a semi bent function.*

Example 3.4. *Over $\mathbb{F}_{2^6}$, the function $f(x) = Tr((x^4+x)^{2^{12}+1})$ is not a semi bent function. In fact, the Walsh Hadamard transform values $W_f(a)$ are 0 or -64, for all $a \epsilon \mathbb{F}_{2^6}$. Hence $Tr(x^4 + x)^{4097}$ is a not a semi bent function.*

4. Cryptographic properties of semi bent functions constructed above

4.1. **Nonlinearity.** Application of Boolean functions as cryptographic tools requires nonlinearity behavior. High nonlinearity is expected to achieve a secured cryptosystem. Linear attacks and fast correlation attacks on the cryptosystems can be prevented in case of stream ciphers, by high nonlinearity. Moreover, the nonlinearity property is most useful in

case of block ciphers to prevent linear cryptanalysis [14, 16, 12]. Nonlinearity is, as defined in the definition of 2.5. Over a small range of values of i, say $1 \leq i \leq 13$, nonlinearity of the semi bent functions constructed in Theorem [3.1,3.2] is observed to be maximum in the Tables [1,2] when compared with the Table [3].

TABLE 1. Nonlinearity of the function $f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1})$ for odd i over $\mathbb{F}_{2^4}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Nonlinearity	4		4		4		4		4		4		4

TABLE 2. Nonlinearity of the function $f(x) = Tr((x^3 + x^2 + x + 1)^{2^{4i}+1})$ for any i or it can be written as $f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1})$, where i is multiple of 4 over $\mathbb{F}_{2^4}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Nonlinearity				4				4				4	

TABLE 3. Nonlinearity of the function $f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1})$, where i is not multiple of 4 and even over $\mathbb{F}_{2^4}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Nonlinearity		0				0				0			

In case of the function $f(x) = Tr(x^4+x)^{2^i+1}$ with $\gcd(i, 6) = 1$ over $\mathbb{F}_{2^6}$, the nonlinearity can be observed as follows.

TABLE 4. Nonlinearity of the function $f(x) = Tr((x^4 + x)^{2^i+1})$ with $\gcd(i, 6) = 1$ over $\mathbb{F}_{2^6}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Nonlinearity	24				24		24				24		24

TABLE 5. Nonlinearity of the function $f(x) = Tr((x^4 + x)^{2^i+1})$ with $\gcd(i, 6) \neq 1$ over $\mathbb{F}_{2^6}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Nonlinearity		24	0	24		0		24	0	24		0	

Nonlinearity of the semi bent functions constructed in Theorem [3.3] is observed to be maximum or equal in the Tables [4] when compared with the Table [5].

4.2. **Algebraic immunity.** Another cryptographic property which plays an important role to discuss about a Boolean function is algebraic immunity. Algebraic immunity is a sort of measurement of the resistance against algebraic attacks over stream ciphers. The concept of algebraic imunity of a Boolean functions was proposed by Courtois and Meier [19]. Lee et al., Wu and Feng in [18, 12] proved that this property prevents the system from algebraic attacks, in case of both stream ciphers and block ciphers.

TABLE 6. Algebraic immunity of the function $f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1})$ for odd i.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Algebraic immunity	1		1		1		1		1		1		1

TABLE 7. Algebraic immunity of the function $f(x) = Tr((x^3 + x^2 + x + 1)^{2^{4i}+1})$ for any i or it can be written as $f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1})$, where i is multiple of 4.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Algebraic immunity				1				1				1	

TABLE 8. Algebraic immunity of the function $f(x) = Tr((x^3 + x^2 + x + 1)^{2^i+1})$, where i is not multiple of 4 and even.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Algebraic immunity		0				0				0			

Algebraic immunity of semi bent function constructed in Theorem [3.1,3.2] is observed in Table [6,7] is high when compared to other Boolean function in Table [8].

TABLE 9. Algebraic immunity of the function $f(x) = Tr((x^4+x)^{2^i+1})$ with $\gcd(i, 6) = 1$ over $\mathbb{F}_{2^6}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Algebraic immunity	2				2		2				2		2

TABLE 10. Algebraic immunity of the function $f(x) = Tr((x^4 + x)^{2^i+1})$ with $\gcd(i, 6) \neq 1$ over $\mathbb{F}_{2^6}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Algebraic immunity		2	0	2		0		2	0	2		0	

Algebraic immunity of semi bent function constructed in Theorem [3.3] is observed in Table [9] is high or equal when compared to other Boolean function in Table [10].

4.3. **Correlation immunity.** Prevention of correlation attacks on the cryptosystems is a challenging part in most of the time. In this regard, correlation immunity is an important cryptographic property to achieve. Correlation immunity is required to measure the resistance level against correlation attacks. The concept of correlation immunity was proposed by Siegenthaler in 1984. It is a safety measure implemented to resist the correlation attack of nonlinear combiners. As a combining function used in a stream ciphers for linear feedback shift registers, Boolean functions with low order correlation immunity is considered to be more susceptible when compared with a function having correlation immunity of high order [9, 12]. The Tables below compare the correlation immunity of the semi bent functions which are constructed in the previous sections.

TABLE 11. Correlation immunity of the function $f(x) = Tr((x^3+x^2+x+1)^{2^i+1})$ for odd i.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Correlation immunity	0		0		0		0		0		0		0

TABLE 12. Correlation immunity of the function $f(x) = Tr((x^3+x^2+x+1)^{2^{4i}+1})$ for any i or it can be written as $f(x) = Tr((x^3+x^2+x+1)^{2^i+1})$, where i is multiple of 4.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Correlation immunity				0				0				0	

TABLE 13. Correlation immunity of the function $f(x) = Tr((x^3+x^2+x+1)^{2^i+1})$, where i is not multiple of 4 and even.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Correlation immunity		3				3				3			

The correlation immunity for the constructed semi bent functions in Theorem [3.1,3.2] found to have the low number in Tables [11] when compared to the Boolean function of the form in the Table [13].

TABLE 14. Correlation immunity of the function $f(x) = Tr((x^4+x)^{2^i+1})$ with $\gcd(i,6) = 1$ over $\mathbb{F}_{2^6}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Correlation immunity	0				0		0				0		0

TABLE 15. Correlation immunity of the function $f(x) = Tr((x^4+x)^{2^i+1})$ with $\gcd(i,6) \neq 1$ over $\mathbb{F}_{2^6}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Correlation immunity		0	5	0		5		0	5	0		5	

The correlation immunity for the constructed semi bent functions in Theorem [3.3] found to have the low number or equal in Tables [14] when compared to the Boolean function of the form in the Table [15].

4.4. **Conclusion.** Semi bent functions are constructed algebraically using the trace of certain functions with a Gold exponent. Such a constructed function exhibits cryptographic properties nonlinearity, algebraic immunity, and zero correlation immunity. Attractive values of the functions concerning these properties may lead to use the semi bent functions effectively in cryptosystems.

Acknowledgment. The authors would like to thank the editor and referees for their valuable comments and suggestions which improved this article. The corresponding author and the second author acknowledges Manipal Institute of Technology (MIT), Manipal Academy of Higher Education, India, for their kind encouragement. The first author is grateful to Manipal Academy of Higher Education for their support through the Dr. T. M. A. Pai Ph. D. scholarship program.

References

[1] Rothaus, O. S., (1976), On bent functions, J. Combin. Theory Ser. A, 20(3), pp.300-305.
[2] Charpin, P., Pasalic, E., and Tavernierr, C., (2005), On bent and semi-bent quadratic boolean functions. IEEE Trans. Inform. Theory, 51(12), pp.4286 - 4298.
[3] Dong, D., Qu, L., Fu, S., and Li, C., (2013), New constructions of semi- bent functions in polynomial forms, Math. Comput. Model., 57(5), pp.1139 - 1147.
[4] Mukhopadhyay, D. and Chowdhury, D. R., (2011), A Parallel Efficient Architecture for Large Cryptographically Robust $n \times k(k > n/2)$ Mappings, IEEE Trans. Computers, 60(3), pp. 375-385.
[5] Cao, X., Chen, H., and Mesnager, S., (2016), Further results on semi-bent functions in polynomial form, Adv. Math. Commun., 10(4), pp. 725-741.
[6] Mesnager, S. and Zhang, F., (2017). On constructions of bent, semi-bent and five valued spectrum functions from old bent functions, Adv. Math. Commun., 11(2), pp.339- 345.
[7] Xie, T. and Luo, G., (2018), More constructions of semi-bent and plateaued functions in polynomial forms, Cluster Computing, pp 1-11.
[8] Xiao, G.Z. and Massey, J. L., (1988), A spectral characterization of correlation-immune combining functions, IEEE Trans. Inform. Theory, 34(3), pp.569-571.
[9] Mesnager, S., (2016), Bent functions, Springer.
[10] McEliece, R. J., (2012), Finite fields for computer scientists and engineers, volume 23, Springer Science & Business Media.
[11] Tokareva, N., (2015), Bent functions: results and applications to cryptography, Academic Press.
[12] Wu, C.K. and Feng, D., (2016), Boolean Functions and Their Applications in Cryptography, Springer-Verlag Berlin Heidelberg.
[13] Chee, S., Lee, S., and Kim, K., (1995), Semi-bent functions, pp 105-118, Springer Berlin Heidelberg, Berlin, Heidelberg.
[14] Meier, W. and Staffelbach, O., (1988), Fast corrrelation attacks on stream ciphers, pp. 301-314, Springer, Berlin, Heidelberg.
[15] Zheng, Y. and Zhang, X.M., (1999), Plateaued Functions, pp. 284-300, Springer Berlin Heidelberg.
[16] Carlet, C., (2011), Nonlinearity of Boolean Functions, pp 848-849, Springer US, Boston, MA.
[17] Khoo, K., Gong, G., and Stinson, D. R., (2002), A new family of gold-like sequences, In Information Theory, 2002. Proceedings, 2002 IEEE International Symposium on, pp. 181. IEEE.
[18] Lee, D. H., Kim, J., Hong, J., Han, J. W., and Moon, D., (2004), Algebraic attacks on summation generators, In International Workshop on Fast Software Encryption, pp. 34-48, Springer.
[19] Courtois, N. T. and Meier, W., (2003), Algebraic Attacks on Stream Ciphers with Linear Feedback, pp 345-359, Springer Berlin Heidelberg, Berlin, Heidelberg.
[20] Tang, D., Yang, Y., and Fu, S., (2017), Semi-bent functions with perfect three-level additive autocorrelation, In Signal Design and Its Applications in Communications (IWSDA), 2017 Eighth International Workshop on, pp. 164-168, IEEE.

Prasanna Poojary received his M.Sc degrees from Manipal Academy Higher Education. He is currently pursuing his Ph.D. degree in the Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal. His research interests include Boolean functions, cryptography and codding theory.

Harikrishnan P. K. completed his Ph.D. degree in Functional Analysis from Kannur University, Kerala. He is currently an Associate Professor with the Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education. His research interests include Operator Theory, C*-Algebra, Linear 2-normed spaces, 2-innerproduct Spaces, Probabilistic Normed Spaces, Topological Vector Spaces, Number theory and Cryptography.

Vadiraja Bhatta G. R. received his M.Sc degree from Mangalore University. He completed Ph.D. degree with the Department of Mathematical and Computational Sciences (MACS), National Institute of Technology Karnataka, Surathkal. He is currently an associate professor with the Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal. His research interests include Latin squares, permutation polynomial, Boolean functions and cryptography..