Proceedings of the Jangjeon Mathematical Society
25 (2022), No. 2, pp. 159 – 171

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2022.25.2.159

R-ORTHOGONALITY OF LATIN SQUARES USING BIVARIATE PERMUTATION POLYNOMIALS

VADIRAJA BHATTA G. R., SHANKAR B. R., AND PRASANNA POOJARY*

Abstract. Cryptographic applications of Latin squares require to study them in various aspects. In this paper, the formation and observation of Latin squares using bivariate permutation polynomials over some finite rings are established with respect to their properties like self orthogonalization, r-orthogonalization, and r- mirror orthogonalization. We also identified why some particular cases fail to form self orthogonal Latin squares, and we illustrate it by giving examples.

2010 Mathematics Subject Classification. 05B15.

Keywords and phrases. Permutation polynomial; Ring; Self-orthogonality; r-orthogonality; Cryptography.

1. Introduction

A polynomial can represent every function from a finite field to itself. The functions, which are also permutations of the field, give rise to permutation polynomials, which have potential applications in cryptology and coding theory [1, 2]. Permutation polynomials have increasingly attracted the attention of various researchers in the past couple of decades. The structures and properties of Latin squares are explained in detail in [5–8]. Rivest in [3] discussed the formation of Latin squares modulo 2^w using bivariate permutation polynomials. In [4], Vadiraja and Shankar considered the Latin squares formed by Permutation Polynomials modulo $n, n \neq 2^w$. For development in Latin squares and for basic results we refer [10–13].

The motivation for the study of Latin square is due to its use in codding theory and cryptography. A Latin square is an important tool in the construction of codes with good characteristics. They are mainly used for construction and ciphering of binary codes as well as non-binary ones [16]. Superimposed codes are a special combinatorial structure that has many applications in information theory, data communication, and cryptography. Jennifer and Dongvu [18] gave an explicit construction of mutually orthogonal Latin squares and showed a method of generating new larger superimposed codes from an existing one using mutually orthogonal Latin squares. Jiejun in [17] presented an algebraic model for privacy-oriented cryptographic modes of operation and the proposed model extensively explore various roles of Latin Square cipher in cryptanalysis. Design of strong cryptographic schemes based on Latin Squares is studied in [19].

Definition 1.1. *A Latin square of order (or size) n is an $n \times n$ array based on some set S of n symbols (treatments), with the property that every row and every column contains every symbol exactly once.*

Using the concept of permutation functions, we can define Latin squares as follows:

Definition 1.2. *A function $f : S^2 \to S$ on a finite set S of size $n > 1$ is said to be a Latin square (of order n) if for any $a \in S$ both the functions $f(a, .)$ and $f(., a)$ are permutations of S.*

Here, $f(a, .)$ determines the rows and $f(., a)$ determines the columns of the Latin square. Latin squares exist for all n, as an obvious example we can consider addition modulo n.
Example: A Latin square of order 5 over the set $\{a, b, c, d, e\}$ is below:

a	b	c	d	e
b	a	e	c	d
c	d	b	e	a
d	e	a	b	c
e	c	d	a	b

The terminology 'Latin square' originated with Euler who used a set of Latin letters for the set S. *Orthogonality* is a very useful concept in the study of Latin squares, having a lot of applications in cryptography.

Definition 1.3. *[9] Two Latin squares $L_1 : R \times C \to S$ and $L_2 : R \times C \to S$ (with the same row and column sets) are said to be orthogonal when for each ordered pair $(s, t) \in S \times T$, there is a unique cell $(x, y) \in R \times C$ so that*

$$L_1(x, y) = s \text{ and } L_2(x, y) = t.$$

Orthogonolity of Latin squares formed by bivariate polynomials over some finite fields is discussed by [9]. Moreover, they studied orthogonality of a Latin square with its mirror image.

Theorem 1.4. *[9] For odd n, Latin square over Z_n formed by a bivariate permutation polynomial $P(x, y)$ is orthogonal with its mirror image.*

2. Self orthogonal Latin squares

Definition 2.1. *A Latin Square is said to be self orthogonal Latin square if it is orthogonal with its transpose.*

Theorem 2.2. *A bivariate polynomial $P(x, y)$ over Z_n for any n, cannot represent a Latin square, which is self orthogonal, if the univariate polynomial $Q(x) = P(x, x)$ is not a permutation polynomial of Z_n.*

Proof: If $Q(x) = P(x, x)$ is not a permutation polynomial, then some entries on the diagonal are repeated. So, such entries yield the pairs $(P(x, x), P(x, x)$ more than once. So, $P(x, y)$ can not be self orthogonal.

But even if the diagonal of the square is a permutation of the ring Z_n, the square may not be self orthogonal, as we can see in the following example:

Example 2.3. *The polynomial $2x + 5y + 3xy + 3x^2 + 6y^2$ is such that $Q(x) = P(x, x)$ is a permutation polynomial on the ring Z_9. It permutes the elements of Z_9 in the order, (0, 1, 8, 3, 4, 2, 6, 7, 5). But, it forms a Latin square over Z_9, which is not self orthogonal. The Latin square formed by this polynomial and its transpose is given below:*

0	*5*	*7*	*6*	*2*	*4*	*3*	*8*	*1*
2	*1*	*6*	*8*	*7*	*3*	*5*	*4*	*0*
7	*0*	*8*	*4*	*6*	*5*	*1*	*3*	*2*
6	*2*	*4*	*3*	*8*	*1*	*0*	*5*	*7*
8	*7*	*3*	*5*	*4*	*0*	*2*	*1*	*6*
4	*6*	*5*	*1*	*3*	*2*	*7*	*0*	*8*
3	*8*	*1*	*0*	*5*	*7*	*6*	*2*	*4*
5	*4*	*0*	*2*	*1*	*6*	*8*	*7*	*3*
1	*3*	*2*	*7*	*0*	*8*	*4*	*6*	*5*

0	*2*	*7*	*6*	*8*	*4*	*3*	*5*	*1*
5	*1*	*0*	*2*	*7*	*6*	*8*	*4*	*3*
7	*6*	*8*	*4*	*3*	*5*	*1*	*0*	*2*
6	*8*	*4*	*3*	*5*	*1*	*0*	*2*	*7*
2	*7*	*6*	*8*	*4*	*3*	*5*	*1*	*0*
4	*3*	*5*	*1*	*0*	*2*	*7*	*6*	*8*
3	*5*	*1*	*0*	*2*	*7*	*6*	*8*	*4*
8	*4*	*3*	*5*	*1*	*0*	*2*	*7*	*6*
1	*0*	*2*	*7*	*6*	*8*	*4*	*3*	*5*

Let A be the Latin square formed by the polynomial $2x+5y+3xy+3x^2+6y^2$ over Z_9 and B be its transpose. We can denote the number of pairs got by superimposing these two squares using the following tables. The empty cells indicate the absence of the corresponding pairs.

$A \rightarrow$ $B \downarrow$	0	1	2	3	4	5	6	7	8
0	3			3			3		
1		9							
2			3			3			3
3	3			3			3		
4					9				
5			3			3			3
6	3			3			3		
7								9	
8			3			3			3

In the above pair of squares, out of 81 pairs, 21 are appearing. The 18 pairs (0, 0), (3, 0), (6, 0), (2, 2), (5, 2), (8, 2), (0, 3), (3, 3), (6, 3), (2, 5), (5, 5), (8, 5), (0, 6), (3, 6), (6, 6), (2, 8), (5, 8) and (8, 8) are all appearing 3 times. The three pairs (1, 1), (4, 4) and (7, 7) are appearing 9 times.

Theorem 2.4. *A symmetric bivariate polynomial $P(x, y)$ over Z_n for any n, cannot give a self orthogonal Latin square.*

Proof: In a symmetric bivariate polynomial, we have $P(x, y) = P(y, x)$. So, all entries, except (possibly) the diagonal entries of the Latin square give the pairs $(P(x, y), P(y, x))$ more than once. So, $P(x, y)$ can not be self orthogonal.

Theorem 2.5. *A bivariate polynomial $P(x, y)$ can not represent a self orthogonal Latin square over Z_n if $P(i, j) = P(j, i)$ for atleast one pair of i and j with $i \neq j$.*

Proof: If for some pair (i, j), $P(i, j) = P(j, i)$, the square obtained by the superposition of the Latin square and its transpose square will contain the pair $(L(i, j), L'(i, j))$ twice, where L is the square due to $P(x, y)$ and L' its transpose.

3. r- orthogonal Latin squares

Orthogonality of Latin squares is a rare possibility over finite rings. But it is interesting to study some pairs of Latin squares in which all n^2 pairs of corresponding entries may not be distinct, but some "r" of them are distinct.

Definition 3.1. *Two Latin squares are r- orthogonal if their superposition produces r distinct pairs.*

It was G.B. Belyavskaya who first systematically treated the following question in 1976: For which integers n and r does a pair of orthogonal Latin squares of order n exist? Evidently, $n \leq r \leq n^2$, and an easy argument establishes that $r \notin \{n + 1,\ n^2 - 1\}$. In a paper by [15], this question has been answered leaving only a possible exception for $r = n^2 - 3$ and $n \in \{6,$ 7, 8, 10, 11, 13, 14, 16, 17, 18, 19, 20, 22, 23, 25, 26$\}$. Again [14] removed these possible exceptions by direct and recursive constructions except two orders $n = 6$ and 14. They tabulated the genuine exceptions for a few values of n:

Order n	Genuine exceptions of r	Possible exceptions of r
2	4	
3	5, 6, 7	
4	7, 10, 11, 13, 14	
5	8, 9, 20, 22, 23	
6	33, 36	
14		$n^2 - 3$

[14] established following lemmas using some direct constructions.

Lemma 3.2. *[14] There does not exist a pair of "(n^2-3)- orthogonal" Latin squares of order $n = 6$.*

Lemma 3.3. *[14] There exists a pair of "(n^2-3)- orthogonal" Latin squares of order $n = 7, 8$.*

Example 3.4. *For $n = 7$.*

0	4	3	6	5	2	1
6	1	4	5	0	3	2
3	5	2	0	1	6	4
5	2	1	3	6	4	0
1	3	6	2	4	0	5
4	6	0	1	2	5	3
2	0	5	4	3	1	6

0	6	5	4	1	3	2
5	1	0	6	3	2	4
6	4	2	1	5	0	3
4	0	6	3	2	1	5
3	5	1	2	4	6	0
2	3	4	0	6	5	1
1	2	3	5	0	4	6

The repeated pairs upon superposition are (3, 5), (5, 4) and (2, 2). The missing pairs are (2, 5), (3, 4) and (5, 2).

Example 3.5. *For* $n = 8$

0	*2*	*5*	*4*	*6*	*7*	*3*	*1*
3	*1*	*7*	*6*	*5*	*0*	*4*	*2*
7	*6*	*2*	*5*	*0*	*4*	*1*	*3*
5	*7*	*6*	*3*	*1*	*2*	*0*	*4*
6	*3*	*0*	*2*	*4*	*1*	*7*	*5*
1	*4*	*3*	*0*	*7*	*5*	*2*	*6*
4	*5*	*1*	*7*	*2*	*3*	*6*	*0*
2	*0*	*4*	*1*	*3*	*6*	*5*	*7*

0	*5*	*3*	*1*	*2*	*4*	*7*	*6*
6	*1*	*7*	*4*	*0*	*2*	*3*	*5*
1	*3*	*2*	*6*	*5*	*7*	*0*	*4*
4	*0*	*5*	*3*	*7*	*6*	*1*	*2*
7	*2*	*6*	*0*	*4*	*3*	*5*	*1*
2	*6*	*1*	*7*	*3*	*5*	*4*	*0*
5	*7*	*4*	*2*	*1*	*0*	*6*	*3*
3	*4*	*0*	*5*	*6*	*1*	*2*	*7*

Further, Zhu and Zhang [14] proved the existence of "(n^2-3) - orthogonal" Latin squares of order $n = 10, 11, 13, 16, 17, 18, 19, 20, 22, 23, 25, 26$. They also conjectured the existence of "$(n^2 - 3)$ - orthogonal" Latin squares of order $n = 14$.

Example 3.6. *Consider the ring* Z_{12}. *The two polynomials* $7x + 11y + 6xy + 6x^2$ *and* $11x + 7y + 6x^2 + 6y^2$ *do not produce orthogonal Latin squares. But they have* 18 *distinct pairs of corresponding entries. So, these two are "*18*-orthogonal" Latin squares.*

Latin square formed by $7x + 11y + 6xy + 6x^2$ over Z_{12}

0	1	2	3	4	5	6	7	8	9	10	11
11	6	1	8	3	10	5	0	7	2	9	4
10	11	0	1	2	3	4	5	6	7	8	9
9	4	11	6	1	8	3	10	5	0	7	2
8	9	10	11	0	1	2	3	4	5	6	7
7	2	9	4	11	6	1	8	3	10	5	0
6	7	8	9	10	11	0	1	2	3	4	5
5	0	7	2	9	4	11	6	1	8	3	10
4	5	6	7	8	9	10	11	0	1	2	3
3	10	5	0	7	2	9	4	11	6	1	8
2	3	4	5	6	7	8	9	10	11	0	1
1	8	3	10	5	0	7	2	9	4	11	6

Latin square formed by $11x + 7y + 6x^2 + 6y^2$ over Z_{12}

0	5	10	3	8	1	6	11	4	9	2	7
1	6	11	4	9	2	7	0	5	10	3	8
2	7	0	5	10	3	8	1	6	11	4	9
3	8	1	6	11	4	9	2	7	0	5	10
4	9	2	7	0	5	10	3	8	1	6	11
5	10	3	8	1	6	11	4	9	2	7	0
6	11	4	9	2	7	0	5	10	3	8	1
7	0	5	10	3	8	1	6	11	4	9	2
8	1	6	11	4	9	2	7	0	5	10	3
9	2	7	0	5	10	3	8	1	6	11	4
10	3	8	1	6	11	4	9	2	7	0	5
11	4	9	2	7	0	5	10	3	8	1	6

Let us denote the Latin squares obtained by polynomials $7x+11y+6xy+6x^2$ and $11x+7y+6x^2+6y^2$ over Z_{12} by A and B respectively. We can denote the number of pairs got by superimposing these two squares using the following tables. The empty cells indicate the absence of the corresponding pair.

$A \rightarrow$ $B \downarrow$	0	1	2	3	4	5	6	7	8	9	10	11
0	12											
1						6						6
2											12	
3				6						6		
4									12			
5		6						6				
6							12					
7						6						6
8					12							
9				6						6		
10			12									
11		6						6				

We can observe the following from the above table.

Remark 3.7.

1. Out of 144 *pairs, only* 18 *pairs appear.*

2. Each possible pair appears either 6 *times or* 12 *times.*

3. In each pair that appears, either both elements are odd or both elements are even.

4. All even element pairs appear 12 *times, and all odd element pairs appear* 6 *times.*

5. There are 6 *even element pairs and* 12 *odd element pairs.*

6. The sum of elements in each pair is either 0 *mod* 12 *or* 6 *mod* 12. *It is always* 0 *mod* 12 *for even elements pairs.*

In the above example, both squares have the same diagonal arrangement. Also, the square is given by the polynomial $7x + 11y + 6xy + 6x^2$ has two cycles along the rows namely,(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) and (0, 7, 2, 9, 4, 11, 6, 1 , 8, 3, 10, 5) alternatively. But the other square obtained by the polynomial $11x + 7y + 6x^2 + 6y^2$ has only one cycle (0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7)in all the rows. This type of row arrangement or the column arrangement influences the number of distinct pairs. The next example clarifies it.

Example 3.8. *Both the squares obtained by* $5x + 7y + 6xy + 6y^2$ *and* $x + 11y + 6xy + 6x^2$ *over* Z_{12} *have* 0 *in the main diagonal. Also, in both the squares, only* 2 *cycles appear along the rows alternatively.*

Latin square formed by $5x + 7y + 6xy + 6y^2$ over Z_{12}

0	5	10	3	8	1	6	11	4	9	2	7
1	0	11	10	9	8	7	6	5	4	3	2
2	7	0	5	10	3	8	1	6	11	4	9
3	2	1	0	11	10	9	8	7	6	5	4
4	9	2	7	0	5	10	3	8	1	6	11
5	4	3	2	1	0	11	10	9	8	7	6
6	11	4	9	2	7	0	5	10	3	8	1
7	6	5	4	3	2	1	0	11	10	9	8
8	1	6	11	4	9	2	7	0	5	10	3
9	8	7	6	5	4	3	2	1	0	11	10
10	3	8	1	6	11	4	9	2	7	0	5
11	10	9	8	7	6	5	4	3	2	1	0

Latin square formed by $x + 11y + 6xy + 6x^2$ over Z_{12}

0	7	2	9	4	11	6	1	8	3	10	5
11	0	1	2	3	4	5	6	7	8	9	10
10	5	0	7	2	9	4	11	6	1	8	3
9	10	11	0	1	2	3	4	5	6	7	8
8	3	10	5	0	7	2	9	4	11	6	1
7	8	9	10	11	0	1	2	3	4	5	6
6	1	8	3	10	5	0	7	2	9	4	11
5	6	7	8	9	10	11	0	1	2	3	4
4	11	6	1	8	3	10	5	0	7	2	9
3	4	5	6	7	8	9	10	11	0	1	2
2	9	4	11	6	1	8	3	10	5	0	7
1	2	3	4	5	6	7	8	9	10	11	0

These two squares have 12 distinct pairs each appearing 12 times. i.e., each entry from the first square has a corresponding unique entry in all the rows or columns. Those pairs are; (0, 0), (1, 11), (2, 10), (3,9), (4,8), (5, 7), (6, 6),(7, 5), (8, 4), (9, 3), (10, 2), (11, 1). Here, we get 18 distinct pairs. So, these two are 18-orthogonal Latin squares. The positions of those pairs are shown below:

$A \rightarrow$ $B \downarrow$	0	1	2	3	4	5	6	7	8
0	6			3					
1						6			3
2		6			3				
3	3						6		
4			6			3			
5		3						6	
6				6			3		
7			3						6
8					6			3	

Theorem 3.9. *For a pair of Latin squares formed by a bivariate permutation polynomial over a ring of even order, always* $r \leq n^2/2$.

Proof: We already know that Latin squares formed by bivariate permutation polynomials over a ring of even order can be divided into four equal parts, pair of two diagonally opposite parts being the same. So, if we look at the pairs of corresponding entries of a pair of such squares, the pairs will be repeated in the same order after $n/2$th row or column onwards. i.e., the first $n^2/2$ pairs of corresponding

entries from the two squares will repeat in the same order like the last $n^2/2$ pairs. So, $r \leq n^2/2$.

Remark 3.10. *In case of Latin squares of even order, to know the r distinct pairs of corresponding entries from a pair of Latin squares, it is sufficient to go through the first $n/2$ rows or columns of the squares, because the remaining $n/2$ rows and columns can be got using the first $n/2$ of them.*

Example 3.11. *The two tables below are the first* 5 *rows of the squares formed by the polynomials $3x + 8y + 5y^2$ and $4x + 6y + 5x^2 + 5y^2$ over Z_{10}.*

0	*3*	*6*	*9*	*2*	*5*	*8*	*1*	*4*	*7*
3	*6*	*9*	*2*	*5*	*8*	*1*	*4*	*7*	*0*
6	*9*	*2*	*5*	*8*	*1*	*4*	*7*	*0*	*3*
9	*2*	*5*	*8*	*1*	*4*	*7*	*0*	*3*	*6*
2	*5*	*8*	*1*	*4*	*7*	*0*	*3*	*6*	*9*

0	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*
1	*0*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*
2	*1*	*0*	*9*	*8*	*7*	*6*	*5*	*4*	*3*
3	*2*	*1*	*0*	*9*	*8*	*7*	*6*	*5*	*4*
4	*3*	*2*	*1*	*0*	*9*	*8*	*7*	*6*	*5*

We get the following table of pairs of corresponding entries form above two parts of the Latin squares(as earlier, A and B denote the above two squares) :

$A \rightarrow$ $B \downarrow$	0	1	2	3	4	5	6	7	8	9
0	1		1		1		1		1	
1		1		1		1		1		1
2	1		1		1		1		1	
3		1		1		1		1		1
4	1		1		1		1		1	
5		1		1		1		1		1
6	1		1		1		1		1	
7		1		1		1		1		1
8	1		1		1		1		1	
9		1		1		1		1		1

$r = 50$(i.e., $n^2/2$) in this case.

Remark 3.12. *From the above table we note;*
1. Only 50 *distinct pairs appear, and each pair appear only once.*
2. In each case, both the entries are either even or odd.
3. The diagonal cells are all filled. i.e., all pairs (a, a) appear.
4. The table above is symmetric about the diagonal.
5. All even-even and all odd-odd pairs appear. The 50 *missing pairs are all even-odd (odd-even) pairs.*
6. To get the above table for the pair of complete Latin squares, all the 1*'s are replaced by* 2*. i.e., each pair is repeated to get a total of* 100 *pairs.*

If we consider the two polynomials $x + 5y + 4xy + 2x^2 + 6y^2$ and $3x + 7y + 2xy + 2x^2 + 4y^2$ over Z_8, the squares they formed by them have 22 distinct pairs of corresponding entries. So, $r = 22$ in this case. The distribution of the pairs is given below:

$A \rightarrow$ $B \downarrow$	0	1	2	3	4	5	6	7
0	4							
1		1		1		1		1
2			2				2	
3		1		1		1		1
4					4			
5		1		1		1		1
6			2				2	
7		1		1		1		1

If we double these entries, we get all the 64 pairs.

4. r- self orthogonal Latin squares

Definition 4.1. *A Latin square is said to be r-self orthogonal if the superposition of the square and its transpose produces exactly r distinct ordered pairs.*

Example 4.2. *The Latin square formed by the polynomial* $5x+2y+3xy+3x^2+6y^2$ *over* Z_9 *and its transpose (i.e., Latin square formed by the polynomial* $2x + 5y + 3xy + 6x^2 + 3y^2$*) over* Z_9 *are given below:*

0	*8*	*4*	*6*	*5*	*1*	*3*	*2*	*7*
8	*1*	*0*	*5*	*7*	*6*	*2*	*4*	*3*
1	*6*	*8*	*7*	*3*	*5*	*4*	*0*	*2*
6	*5*	*1*	*3*	*2*	*7*	*0*	*8*	*4*
5	*7*	*6*	*2*	*4*	*3*	*8*	*1*	*0*
7	*3*	*5*	*4*	*0*	*2*	*1*	*6*	*8*
3	*2*	*7*	*0*	*8*	*4*	*6*	*5*	*1*
2	*4*	*3*	*8*	*1*	*0*	*5*	*7*	*6*
4	*0*	*2*	*1*	*6*	*8*	*7*	*3*	*5*

0	*8*	*1*	*6*	*5*	*7*	*3*	*2*	*4*
8	*1*	*6*	*5*	*7*	*3*	*2*	*4*	*0*
4	*0*	*8*	*1*	*6*	*5*	*7*	*3*	*2*
6	*5*	*7*	*3*	*2*	*4*	*0*	*8*	*1*
5	*7*	*3*	*2*	*4*	*0*	*8*	*1*	*6*
1	*6*	*5*	*7*	*3*	*2*	*4*	*0*	*8*
3	*2*	*4*	*0*	*8*	*1*	*6*	*5*	*7*
2	*4*	*0*	*8*	*1*	*6*	*5*	*7*	*3*
7	*3*	*2*	*4*	*0*	*8*	*1*	*6*	*5*

There are 21 distinct pairs. So, $r = 21$. In the first square above, there are three distinct cycles along the first three rows and the same cycles repeat twice in the last six rows.

The three distinct cycles are;

(0, 8, 4, 6, 5, 1, 3, 2, 7)
(8, 1, 0, 5, 7, 6, 2, 4, 3)
(1, 6, 8, 7, 3, 5, 4, 0, 2)

Along the columns, there is only one cycle: (0, 8, 1, 6, 5, 7, 3, 2, 4). Its transpose, the second square above contains three distinct cycles along the first three columns, and the same cycles repeat twice in the last six columns. The only cycle along all the rows of this square is (0, 8, 1, 6, 5, 7, 3, 2, 4). So, we get all the 21 distinct pairs to form the first three rows only. They are distributed with respect to the first three rows as follows:

$A \rightarrow$ $B \downarrow$	0	1	2	3	4	5	6	7	8
0	1			1			1		
1		1			1			1	
2			3						
3	1			1			1		
4		1			1			1	
5						3			
6	1			1			1		
7		1			1			1	
8									3

The next two sets of three consecutive rows give exactly same type of distribution. So, the distribution for the entire square has all the above entries multiplied by three which is shown below:

$A \rightarrow$ $B \downarrow$	0	1	2	3	4	5	6	7	8
0	3			3			3		
1		3			3			3	
2			9						
3	3			3			3		
4		3			3			3	
5						9			
6	3			3			3		
7		3			3			3	
8									9

Consider the polynomial $3x + 5y + 4xy + 2x^2 + 6y^2$ over Z_8. The Latin square formed by this polynomial and the square which is the transpose of this square (i.e., formed by the polynomial $5x + 3y + 4xy + 6x^2 + 2y^2$) are shown below:

0	5	6	3	4	1	2	7
3	4	1	2	7	0	5	6
2	7	0	5	6	3	4	1
5	6	3	4	1	2	7	0
4	1	2	7	0	5	6	3
7	0	5	6	3	4	1	2
6	3	4	1	2	7	0	5
1	2	7	0	5	6	3	4

0	3	2	5	4	7	6	1
5	4	7	6	1	0	3	2
6	1	0	3	2	5	4	7
3	2	5	4	7	6	1	0
4	7	6	1	0	3	2	5
1	0	3	2	5	4	7	6
2	5	4	7	6	1	0	3
7	6	1	0	3	2	5	4

Here the square and its transpose both have only one cycle in the rows; (0, 5, 6, 3, 4, 1, 2, 7) and (0, 3, 2, 5, 4, 7, 6, 1), respectively. Also, the corresponding positions of 0's of the two squares are coinciding in all the eight rows. Hence, the pairs of the other corresponding entries in all the rows are nothing but the pairs of corresponding entries of these two cycles. Hence, the pairs (0, 0),(5, 3),(6, 2),(3, 5),(4, 4),(1, 7),(2, 6) and (7, 1) are the distinct pairs, all appearing eight times. So, $r = 8$ for this polynomial. But this fact is not always true. The polynomial $5x + 3y + 2x^2$ gives a Latin square over Z_8, which has 12 distinct pairs of corresponding entries with its transpose. In this case, the four pairs (1, 1), (3, 7), (5, 5) and (7, 3) are appearing 8 times and the remaining eight pairs (0, 0), (0, 4), (2, 2), (2, 6), (4, 0), (4, 4), (6, 2) and (6, 6) are all appearing 4 times.

5. r-mirror orthogonal Latin squares

Definition 5.1. *A Latin square is said to be r-mirror orthogonal if the superposition of the square and its mirror image produces exactly r distinct ordered pairs.*

Remark 5.2. *From Theorem 1.4, for rings of odd order, all Latin squares formed by permutation polynomials are orthogonal with their mirror images. But in case of rings of even order, $n^2/2$ pair of corresponding entries are repeated. So, we have the following theorem:*

Theorem 5.3. *For n even, the Latin square formed by a bivariate permutation polynomial $P(x, y)$ over Z_n is $r-$orthogonal with its mirror image, with $r = n^2/2$.*

Proof: The arguments in the proof of Theorem 1.4 hold good for the first $n/2$ rows of the square in case of even n too. So, the first $n^2/2$ pairs are distinct. And those pairs repeat for the remaining half of the square. So, $r = n^2/2$.

Example 5.4. *The Latin square and its mirror image formed by the polynomial $2x + 4y + 3x^2 + 3y^2$ over Z_6 are given below:*

0	*5*	*4*	*3*	*2*	*1*
1	*0*	*5*	*4*	*3*	*2*
2	*1*	*0*	*5*	*4*	*3*
3	*2*	*1*	*0*	*5*	*4*
4	*3*	*2*	*1*	*0*	*5*
5	*4*	*3*	*2*	*1*	*0*

1	*2*	*3*	*4*	*5*	*0*
2	*3*	*4*	*5*	*0*	*1*
3	*4*	*5*	*0*	*1*	*2*
4	*5*	*0*	*1*	*2*	*3*
5	*0*	*1*	*2*	*3*	*4*
0	*1*	*2*	*3*	*4*	*5*

The two squares above have 18 distinct pairs when they are superimposed. The pairs are of the form (a, b), where one of a and b is odd and the other is even and all pairs that appear are of this form. They are as follows:

(0,1), (0,3), (0,5)
(1,0), (1,2), (1,4)
(2,1), (2,3), (2,5)
(3,0), (3,2), (3,4)
(4,1), (4,3), (4,5)
(5,0), (5,2), (5,4).

Their distribution is shown below:

$A \rightarrow$ $B \downarrow$	0	1	2	3	4	5
0		2		2		2
1	2		2		2	
2		2		2		2
3	2		2		2	
4		2		2		2
5	2		2		2	

6. Conclusion

Orthogonality of Latin squares is a rare possibility over finite rings using bivariate permutation polynomials. A single bivariate permutation polynomial yielding a Latin square which is orthogonal to its transpose is a highly unusual concept to expect. Formations and simple observations with regard to r-orthogonal, r-self orthogonal and r-mirror orthogonal Latin squares are made taking small examples.

Acknowledgment. The first author acknowledges the Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India, for their kind encouragement. The corresponding author acknowledges the Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India, for their kind encouragement.

References

1. I. Janiszczak, and R. Staszewski, *Isometry invariant permutation codes and mutually orthogonal Latin squares*, Journal of Combinatorial Designs, **27**(9), (2019), 541-551.
2. G. Otokar, and S. Marek *Isotopy of Latin squares in cryptography.* Tatra Mountains Mathematical Publications **45**(1), (2010), 27-36.
3. R. L. Rivest, *Permutation polynomials modulo* 2^w, Finite Fields Appl., **7**(2), (2001), 287-292.
4. B. G. R. Vadiraja, and B. R. Shankar, *Permutation Polynomials modulo n,* $n = 2^w$ *and Latin Squares*, Mathematical Combinatorics, **2**, (2009), 58-65.
5. J. H. Lint, and R. M. Wilson, *A course in combinatorics*, Cambridge university press, (2001).
6. B. G. R. Vadiraja, and B. R. Shankar, *A study of permutation polynomials as latin squares*, in: Nearrings, Near fields and Related Topics, World Scientific, (2017), 270-281.
7. B. G. R. Vadiraja, B. R. Shankar, V. N. Mishra, and P. Prasanna *Sequences of numbers via permutation polynomials over some finite rings*, Proyecciones (Antofagasta), **39**(5), 1295-1313.
8. B. G. R. Vadiraja, B. R. Shankar, P. Prasanna, K. J. Manasa, V. N. Mishra, *Variations of diagonal cyclicity of Latin squares formed by permutation polynomials*, Italian Journal of Pure and Applied Mathematics, **46**, (2021), 438-452.
9. B. G. R. Vadiraja, and B. R. Shankar, *Variations of Orthogonality of Latin Squares*, Mathematical Combinatorics, **3**, (2015), 55-61.
10. R. Lidl, and H. Niederreiter, *Finite fields*, **20**, Cambridge university press, (1997).
11. O. Krafft, H. Pahlings, and M. Schaefer, *Diagonal-complete Latin squares*, Eur. J. Combin., **24**, (2003), 229-237.
12. Y. Zhang, K. Chen, N. Cao, and H. Zhang, *Strongly symmetric self-orthogonal diagonal Latin squares and Yang Hui type magic squares*, Discrete Math., **328**, (2014), 79-87.
13. E. Vatutin, S. Kochemazov, and O. Zaikin, *On some features of symmetric diagonal latin squares*, in: CEUR Workshop Proceedings, 1940, (2017), 74-79.
14. Z. Lie, and Z. Hantao, *A few more r-orthogonal Latin squares*, Discrete Mathematics, **238**, (2001), 183-191.
15. C. L. Colbourn, and L. Zhu, *The spectrum of r-Orthogonal Latin squares*, in: Combinatorics advances, Springer, (1995), 49-75.
16. J. Dénes, and A. D. Keedwell. *Latin squares: New developments in the theory and applications. 46, 1991.*
17. J. Kong. *The role of latin square in cipher systems: Matrix approach to model encryption modes of operation.* UCLA Computer Science Department Technical Report CSTR030038.(2008).
18. J. Seberry, and D. Tonien. *Some constructions of mutually orthogonal latin squares and superimposed codes.* Discrete Mathematics, Algorithms and Applications **4**(3), (2012).
19. S. K. Pal, S. Kapoor, A. Arora, R. Chaudhary, and J. Khurana, *Design of strong cryptographic schemes based on Latin Squares.* Journal of Discrete Mathematical Sciences and Cryptography **13**(3), (2010), 233-256.

Department of Mathematics, Centre for cryptography, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.
Email address: vadiraja.bhatta@manipal.edu

Department of Mathematical and Computational Sciences, National Institute of Technology Karnataka, Surathkal, Karnataka, India.
Email address: brs@nitk.ac.in

Department of Mathematics, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India.
Email address: poojaryprasanna34@gmail.com; poojary.prasanna@manipal.edu