Hindawi
Journal of Mathematics
Volume 2022, Article ID 8992934, 10 pages
https://doi.org/10.1155/2022/8992934

Research Article

On Graph-Transversal Designs and Graph-Authentication Codes Based on Mutually Orthogonal Graph Squares

A. El-Mesady,[1] **Omar Bazighifan**,[2,3] **and H. M. Shabana**[1]

[1] *Department of Physics and Engineering Mathematics, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt*
[2] *Department of Mathematics, Faculty of Science, Hadhramout University, Hadhramout 50512, Yemen*
[3] *Department of Mathematics, Faculty of Education, Seiyun University, Hadhramout 50512, Yemen*

Correspondence should be addressed to Omar Bazighifan; o.bazighifan@gmail.com

Received 3 March 2022; Accepted 22 April 2022; Published 29 May 2022

Academic Editor: Gohar Ali

Combinatorial designs have many interesting and genuine wide applications in areas including analysis and design of algorithms, cryptography, analysis and design of experiments, storage system design, tournament scheduling, optical communications, and computer networks to mention just a few areas. In this paper, we are concerned with the transversal designs and authentication codes as direct applications of combinatorial designs. The novelty of the current paper is demonstrated by the fact that it is the first to introduce the transversal designs and authentication codes by the mutually orthogonal graph squares (MOGS); we call them graph-transversal designs and graph-authentication codes, respectively. Here, the major contributions are the constructions of graph-transversal designs and graph-authentication codes based on several classes of graphs. Also, we present several results such as path-transversal designs, cycle-transversal designs, and disjoint unions of stars-transversal designs.

1. Introduction

The development of combinatorial design theory is considered one of the remarkable successes, deep connections with mathematics, unanticipated applications, and the desire to provide ordered objects from apparent chaos. The celebrated successes of combinatorial design theory have appeared in the eighteenth and nineteenth centuries by the research of Euler, Cayley, Kirkman, Hamilton, Moore, Sylvester, and others. In the 1920s, combinatorial design theory became a field intimately connected to the applications after Fisher and his school evolved the mathematics of experimental designs. Bose and his colleagues discovered deep interactions between the mathematical nascent field and the number theory, finite geometry, error-correcting codes, group theory, and finite fields in the 1930s for a good survey on the combinatorial designs and their applications, see [1, 2].

A decomposition $H = \{H_1, \ldots, H_l\}$ of a graph F is a partition of its edge set $E(F)$ into edge-disjoint isomorphic subgraphs $H_1, \ldots, H_l$. If all these subgraphs are isomorphic to G, then H is a decomposition of F by G. A decomposition of the complete bipartite graph $K_{m,m}$ by mK_2 and a Latin square of the order m are equivalent, where the Latin square can be defined as follows.

Definition 1 (see [2]). Suppose A is an m-set. Then, a Latin square of order m is an $m \times m$ array M with entries from A, such that all the rows and the columns of M are considered permutations of A.

Example 1 (see [2]). Suppose $A = \{1, 2, 3\}$. Then, there are precisely 12 Latin squares defined on A as shown in Table 1.

Definition 2 (see [2]). Let M_1 be a Latin square with order m and entries belong to the set A and M_2 be a Latin square with order m and entries belong to the set B. Then, M_1 and M_2 are orthogonal if, for every $x \in A$ and for every $y \in B$, there is precisely one cell (a, b) where $M_1(a, b) = x$ and $M_2(a, b) = y$. A set of l Latin squares of order m, say

Table 1: The 12 Latin squares of Example 1.

$M_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$	$M_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$	$M_3 = \begin{bmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix}$	$M_4 = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}$
$M_5 = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}$	$M_6 = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \end{bmatrix}$	$M_7 = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{bmatrix}$	$M_8 = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$
$M_9 = \begin{bmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix}$	$M_{10} = \begin{bmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$	$M_{11} = \begin{bmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{bmatrix}$	$M_{12} = \begin{bmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix}$

$M_1, \ldots, M_l$, are called pairwise orthogonal (mutually orthogonal) Latin squares (MOLS) if M_α and M_β are orthogonal for all $1 \le \alpha < \beta \le l$.

Example 2 (see [3]). Let $A = B = \{1, 2, 3, 4\}$. Then, the encoming Latin squares M_1 and M_2 are orthogonal.

$$M_1 = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \\ 2 & 1 & 3 & 4 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 1 & 4 & 3 & 2 \\ 4 & 1 & 2 & 3 \\ 2 & 3 & 4 & 1 \\ 3 & 2 & 1 & 4 \end{bmatrix}. \tag{1}$$

If $H = \{H_1, \ldots, H_m\}$ and $T = \{T_1, \ldots, T_m\}$ are two decompositions of $K_{m,m}$, then H and T are orthogonal if $|E(H_x) \cap E(T_y)| = 1$ for all $x, y \in \{1, 2, \ldots, m\}$. It is clear from the orthogonality that $|E(H_x)| = |E(T_x)| = m$ for all $x \in \{1, 2, \ldots, m\}$.

Let $\mathbb{Z}_m = \{1, 2, \ldots, m\}$ the complete bipartite network $K_{m,m}$ has consisted of two independent sets of vertices, then the first set of the vertices is labeled by $\mathbb{Z}_m \times \{0\}$, and the second set of the nodes is labeled by $\mathbb{Z}_m \times \{1\}$. For any $i, j \in \mathbb{Z}_m$, we will use i_0 for the vertex $(i, 0)$ and j_1 for the vertex $(j, 1)$. Consequently, the edge set of $K_{m,m}$ is $E(K_{m,m}) = \{(i_0, j_1)\colon i, j \in \mathbb{Z}_m\}$.

Definition 3 (see [3]). Let G be a subgraph of $K_{m,m}$ and the number of its edges be m. Then, a square matrix M with order m is G-square if each element in $\mathbb{Z}_m = \{1, 2, \ldots, m\}$ is found exactly m times in M, and for any $x \in \mathbb{Z}_m$, all graphs G_x are isomorphic to G, where $E(G_x) = \{(i_0, j_1)\colon M(i_0, j_1) = x\}$. The set $\mathbb{Z}_m \times \{0\}$ is used as an index set for the rows of M, and the set $\mathbb{Z}_m \times \{1\}$ is used as an index set for the columns of M. The Latin square of order m is considered a mK_2-square.

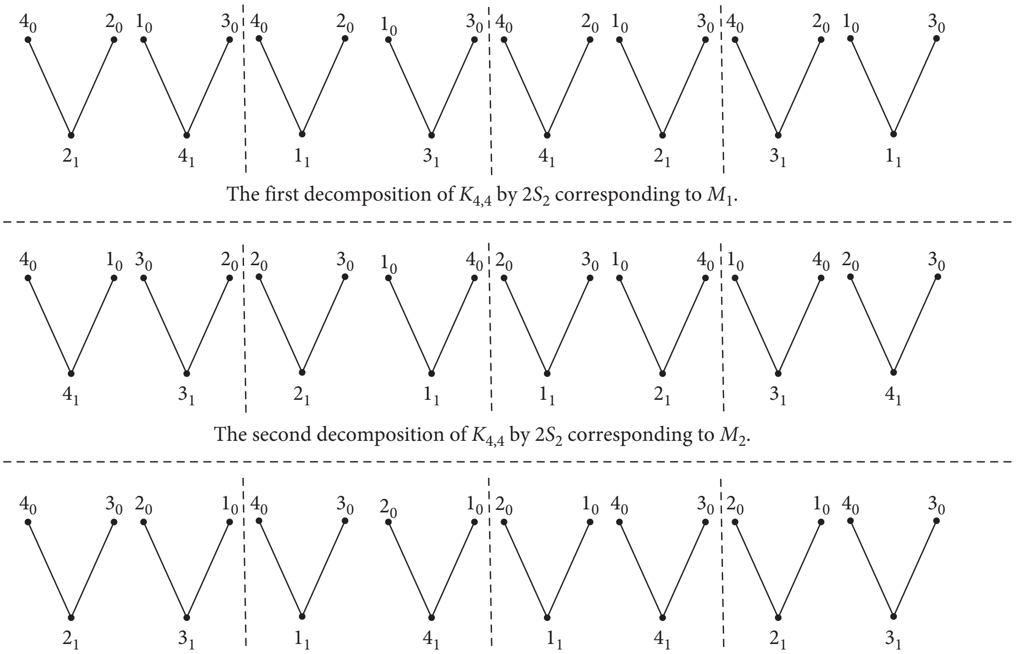
A set of decompositions $\{T_1, T_2, \ldots, T_k\}$ of $K_{m,m}$ is considered a set of k mutually orthogonal graph squares (MOGS) if T_x and T_y are orthogonal for all $x, y \in \{1, 2, \ldots, k\}$ and $x \neq y$.

Example 3 (see [4]). Figure 1 exhibits three mutually orthogonal decompositions of $K_{4,4}$ by $2S_2$. These decompositions can be represented by the following three mutually orthogonal $2S_2$-squares M_1, M_2, and M_3.

$$M_1 = \begin{bmatrix} 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 2 & 3 & 4 & 1 \\ 3 & 2 & 1 & 4 \\ 3 & 2 & 1 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 3 & 4 & 1 & 2 \\ 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 \\ 2 & 1 & 4 & 3 \end{bmatrix}. \tag{2}$$

Great efforts have been made for getting the solution of several problems concerned with the MOLS since Euler first asked about MOLS for solving the thirty-six officers' problem. Bose, Shrikhande, and Parker introduced celebrated theorems concerned with the MOLS [5,6]. Also, Wilson in [7] handled celebrated theorems concerned with the MOLS. For a brief survey on constructions of MOLS, see [8]. El-Shanawany [3] introduced the conjecture, $N(q; P_{q+1}) = q$, where q is a prime number and P_{q+1} is a path on $q + 1$ vertices. The authors in [9] solved this conjecture. In [10], El-Shanawany computed $N(p; G)$ where G is a graph path. El-Shanawany [11] computed $N(n; G) = k \ge 3$, where G consists of disjoint union of isomorphic subgraphs of $K_{n,n}$. Higazy found $N(n; G)$ for all possible subgraphs G with $n = 3$, 4 edges [12]. The Kronecker product of MOGS was defined in [4] and was applied to construct MOGS for disjoint union of star graphs. El-Shanawany et al. [13] introduced the MOGS for some paths. For more results on MOGS, see [14–18].

Motivated by all previous results, the main aim of this paper is to benefit from the results of MOGS in the literature to construct new structures. These structures are called graph-transversal designs and authentication codes. The decomposition of numerous bipartite graphs, for constructing the studied structures, demonstrates the robustness and the advantages of the suggested techniques. The novelty of the current paper is demonstrated by the fact that it is the first to introduce the transversal designs and authentication codes by MOGS.



The first decomposition of $K_{4,4}$ by $2S_2$ corresponding to M_1.

The second decomposition of $K_{4,4}$ by $2S_2$ corresponding to M_2.

The third decomposition of $K_{4,4}$ by $2S_2$ corresponding to M_3.

Figure 1: Three mutually orthogonal decompositions of $K_{4,4}$ by $2S_2$.

The remaining part of the paper is organized as follows: graph-transversal designs by MOGS are introduced in Section 2. Section 3 investigates the design of message authentication codes based on MOGS. In Section 4, an application of the graph-transversal design in key predistribution in wireless sensor networks is introduced. Section 5 shows the conclusion.

2. Graph-Transversal Designs by MOGS

In this section, we prove that many results of MOGS are equivalent to the transversal designs. Now, we introduce the definition of these objects.

Definition 2. Suppose that $m \geq 2$ and $n \geq 1$. Then, a transversal design $TD[m, \lambda; n]$ is a triple (Z, Σ, χ), where the encoming properties are verified.

(1) $Z = \{z_{xy}, xy \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}\}$ is a set of mn elements. These elements are called points.

(2) $\Sigma = \{\Sigma_i: 1 \leq i \leq m\}$ is a partition of Z into m subsets. These subsets are called groups; they are not considered algebraic groups. The size of each group is n.

(3) χ is a set of m-subsets of Z, which are called blocks.

(4) Every couple of points from different groups is found in precisely λ blocks in χ, and

(5) Any block and any group have precisely one point in common.

Example 4. The blocks and the groups of a $TD[4, 1; 3]$ transversal design are exhibited in Table 2, where the set $Z = \{z_{xy}, xy \in \{1, 2, 3\} \times \{1, 2, 3, 4\}\}$, $\Sigma = \{\Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4\}$, and $\chi = \{\chi_1, \chi_2, \ldots, \chi_9\}$.

In the following proposition, we prove that if we have k mutually orthogonal G-squares of order n, then we can construct the graph-transversal design $G - TD[k, 1; n]$. This proposition is followed by some results concerned with the graph-transversal designs by different graph classes.

Proposition 1. *If there are k mutually orthogonal G-squares of order n, then there is a graph-transversal design G–TD[k,1;n].*

Proof. Let the k mutually orthogonal G-squares of order n are L_i, $1 \leq i \leq k$. Define $Z = \{z_{xy}, xy \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, k\}\}$. For $1 \leq i \leq k$, consider $\Sigma_i = \{z_{xi}: x \in \{1, 2, \ldots, n\}\}$, and then $\Sigma = \{\Sigma_i: 1 \leq i \leq k\}$. For $1 \leq t \leq n^2$, define $\chi_t = \{z_{L_i(\lambda, t-(\lambda-1)n)i}: 1 \leq i \leq k, 1 \leq \lambda \leq n\}$, $(\lambda - 1)n + 1 \leq t \leq \lambda n$, and $\chi = \{\chi_t: 1 \leq t \leq n^2\}$. Hence, Z is a set of kn elements, Σ is a partition of Z into k groups, χ is a set of k-subsets (blocks) of Z, every couple of points from different groups is found in precisely one block, and any block and any group have precisely one point in common. Now, the triple (Z, Σ, χ) satisfies the conditions of the transversal design $TD[k, 1; n]$. We call this design a graph-transversal design $G - TD[k, 1; n]$. □

Example 5. Let the three mutually orthogonal C_4-squares with order four are represented by the encoming matrices, see Figure 2.

Table 2: The blocks and the groups of a $TD[4,1;3]$ transversal design.

Groups	Blocks
	$\chi_1 = \{z_{11}, z_{12}, z_{13}, z_{14}\}$
	$\chi_2 = \{z_{11}, z_{22}, z_{23}, z_{24}\}$
$\Sigma_1 = \{z_{11}, z_{21}, z_{31}\}$	$\chi_3 = \{z_{11}, z_{32}, z_{33}, z_{34}\}$
$\Sigma_2 = \{z_{12}, z_{22}, z_{32}\}$	$\chi_4 = \{z_{21}, z_{12}, z_{23}, z_{34}\}$
$\Sigma_3 = \{z_{13}, z_{23}, z_{33}\}$	$\chi_5 = \{z_{21}, z_{22}, z_{33}, z_{14}\}$
$\Sigma_4 = \{z_{14}, z_{24}, z_{34}\}$	$\chi_6 = \{z_{21}, z_{32}, z_{13}, z_{24}\}$
	$\chi_7 = \{z_{31}, z_{12}, z_{33}, z_{24}\}$
	$\chi_8 = \{z_{31}, z_{22}, z_{13}, z_{34}\}$
	$\chi_9 = \{z_{31}, z_{32}, z_{23}, z_{14}\}$

$$L_1 = \begin{bmatrix} 4 & 4 & 1 & 1 \\ 4 & 4 & 1 & 1 \\ 2 & 2 & 3 & 3 \\ 2 & 2 & 3 & 3 \end{bmatrix},$$
$$L_2 = \begin{bmatrix} 4 & 1 & 4 & 1 \\ 2 & 3 & 2 & 3 \\ 4 & 1 & 4 & 1 \\ 2 & 3 & 2 & 3 \end{bmatrix}, \qquad (3)$$
$$L_3 = \begin{bmatrix} 4 & 2 & 2 & 4 \\ 3 & 1 & 1 & 3 \\ 3 & 1 & 1 & 3 \\ 4 & 2 & 2 & 4 \end{bmatrix}.$$

By applying the previous technique in Proposition 1 to convert the three mutually orthogonal C_4-squares to $C_4 - TD[3,1;4]$ transversal design, we get $Z = \{z_{xy}, xy \in \{1,2,3,4\} \times \{1,2,3\}\}$, and for $1 \leq i \leq 3$, we have $\Sigma_i = \{z_{xi}\colon x \in \{1,2,3,4\}\}$ and $\Sigma = \{\Sigma_i\colon 1 \leq i \leq 3\}$. For $1 \leq t \leq 16$, we have $\chi_t = \{z_{L_i(\lambda, t-(\lambda-1)n)i}\colon 1 \leq i \leq 3, 1 \leq \lambda \leq 4\}$, $4(\lambda - 1) + 1 \leq t \leq 4\lambda$, and $\chi = \{\chi_t\colon 1 \leq t \leq 16\}$. For illustration, see Table 3. In what follows, we will construct some graph-transversal designs based on the ingredients in Table 4 and Proposition 1 which connects between the MOGS and the graph-transversal designs. We present several results such as path-transversal designs, cycle-transversal designs, and disjoint unions of stars-transversal designs.

Corollary 1. *Let n be a prime >2. Then, there exists a* $(S_1 \cup (n - 1/2)S_2) - TD[n,1;n]$.

Proof. Let the n mutually orthogonal $(S_1 \cup (n - 1/2)S_2)$-squares of order n are M_i, $1 \leq i \leq n$. Define $Z = \{z_{xy}, xy \in \{1,2,\ldots,n\} \times \{1,2,\ldots,n\}\}$. For $1 \leq i \leq n$, consider $\Sigma_i = \{z_{xi}\colon x \in \{1,2,\ldots,n\}\}$, and then, $\Sigma = \{\Sigma_i\colon 1 \leq i \leq n\}$. For $1 \leq t \leq n^2$, define $\chi_t = \{z_{M_i(\lambda, t-(\lambda-1)n)i}\colon 1 \leq i \leq n, 1 \leq \lambda \leq n\}$, $(\lambda - 1)n + 1 \leq t \leq \lambda n$, and $\chi = \{\chi_t\colon 1 \leq t \leq n^2\}$. Hence, Z is a set of n^2 elements, Σ is a partition of Z into n groups, χ is a set of n-subsets (blocks) of Z, every couple of points from different groups is found in precisely one block, and any block and any group have precisely one point in common. Now, the triple (Z, Σ, χ) satisfies the conditions of the graph-transversal design $(S_1 \cup (n - 1/2)S_2)$-$TD[n,1;n]$. □

Corollary 2. *Let n be a prime >2. Then, there exists a* $((n-2)S_1 \cup S_2)$-$TD[n-1,1;n]$.

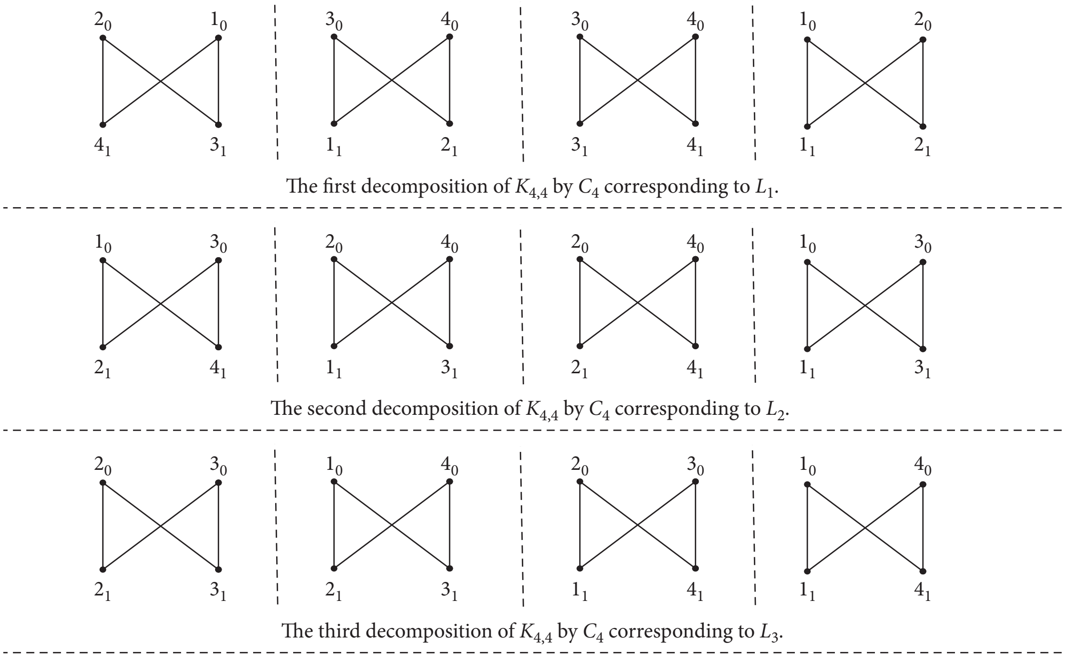
Proof. Let the $n-1$ mutually orthogonal $((n-2)S_1 \cup S_2)$-squares of order n are M_i, $1 \leq i \leq n-1$. Define $Z = \{z_{xy}, xy \in \{1,2,\ldots,n\} \times \{1,2,\ldots,n-1\}\}$. For $1 \leq i \leq n-1$, consider $\Sigma_i = \{z_{xi}\colon x \in \{1,2,\ldots,n\}\}$, and then, $\Sigma = \{\Sigma_i\colon 1 \leq i \leq n-1\}$. For $1 \leq t \leq n^2$, define $\chi_t = \{z_{M_i(\lambda, t-(\lambda-1)n)i}\colon 1 \leq i \leq n-1\}$, $1 \leq \lambda \leq n$, $(\lambda - 1)n + 1 \leq t \leq \lambda n$, and $\chi = \{\chi_t\colon 1 \leq t \leq n^2\}$. Hence, Z is a set of $(n^2 - n)$ elements, Σ is a partition of Z into $(n-1)$ groups, χ is a set of $(n-1)$-subsets (blocks) of Z, every couple of points from different groups is found in precisely one block, and any block and any group have precisely one point in common. Now, the triple (Z, Σ, χ) satisfies the conditions of the graph-transversal design $((n-2)S_1 \cup S_2)$-$TD[n-1,1;n]$. □

Corollary 3. *There exists a* $(S_3 \cup 3S_2)$-$TD[3,1;9]$.

Proof. Let the 3 mutually orthogonal $(S_3 \cup 3S_2)$-squares of order 9 are M_i, $1 \leq i \leq 3$. Define $Z = \{z_{xy}, xy \in \{1,2,\ldots,9\} \times \{1,2,3\}\}$. For $1 \leq i \leq 3$, consider $\Sigma_i = \{z_{xi}\colon x \in \{1,2,\ldots,9\}\}$, and then $\Sigma = \{\Sigma_i\colon 1 \leq i \leq 3\}$. For $1 \leq t \leq 81$, define $\chi_t = \{z_{M_i(\lambda, t-(\lambda-1)n)i}\colon 1 \leq i \leq 3, 1 \leq \lambda \leq 9\}, 9(\lambda - 1) + 1 \leq t \leq 9\lambda$, and $\chi = \{\chi_t\colon 1 \leq t \leq 81\}$. Hence, Z is a set of 27 elements, Σ is a partition of Z into 3 groups, χ is a set of 3-subsets (blocks) of Z, every couple of points from different groups is found in precisely one block, and any block and any group have precisely one point in common. Now, the triple (Z, Σ, χ) satisfies the conditions of the graph-transversal design $(S_3 \cup 3S_2)$-$TD[3,1;9]$. □

Corollary 4. *Let n be a prime >2. Then, there exists a* P_{n+1}-$TD[n,1;n]$.

Proof. Let the n mutually orthogonal P_{n+1}-squares of order n are M_i, $1 \leq i \leq n$. Define $Z = \{z_{xy}, xy \in \{1,2,\ldots,n\} \times \{1,2,\ldots,n\}\}$. For $1 \leq i \leq n$, consider $\Sigma_i = \{z_{xi}\colon x \in \{1,2,\ldots,n\}\}$, and then $\Sigma = \{\Sigma_i\colon 1 \leq i \leq n\}$. For $1 \leq t \leq n^2$, define $\chi_t = \{z_{M_i(\lambda, t-(\lambda-1)n)i}\colon 1 \leq i \leq n, 1 \leq \lambda \leq n\}$, $(\lambda - 1)n + 1 \leq t \leq \lambda n$, and $\chi = \{\chi_t\colon 1 \leq t \leq n^2\}$. Hence, Z is a set of n^2 elements, Σ is a partition of Z into n groups, χ is a set of n-subsets (blocks) of Z, and every couple of points from different groups is found in precisely one block; since M is an orthogonal array, any block and any group have precisely one point in common. Now, the triple (Z, Σ, χ) satisfies the conditions of the graph-transversal design P_{n+1}-$TD[n,1;n]$. □



The first decomposition of $K_{4,4}$ by C_4 corresponding to L_1.

The second decomposition of $K_{4,4}$ by C_4 corresponding to L_2.

The third decomposition of $K_{4,4}$ by C_4 corresponding to L_3.

Figure 2: Three mutually orthogonal decompositions of $K_{4,4}$ by C_4.

Table 3: The blocks and the groups of a $C_4 - TD[3, 1; 4]$ transversal design.

$\Sigma_1 = \{z_{11}, z_{21}, z_{31}, z_{41}\}$	$\chi_1 = \{z_{41}, z_{42}, z_{43}\}$
$\Sigma_2 = \{z_{12}, z_{22}, z_{32}, z_{42}\}$	$\chi_2 = \{z_{41}, z_{12}, z_{23}\}$
$\Sigma_3 = \{z_{13}, z_{23}, z_{33}, z_{43}\}$	$\chi_3 = \{z_{11}, z_{42}, z_{23}\}$
	$\chi_4 = \{z_{11}, z_{12}, z_{43}\}$
	$\chi_5 = \{z_{41}, z_{22}, z_{33}\}$
	$\chi_6 = \{z_{41}, z_{32}, z_{13}\}$
	$\chi_7 = \{z_{11}, z_{22}, z_{13}\}$
	$\chi_8 = \{z_{11}, z_{32}, z_{33}\}$
	$\chi_9 = \{z_{21}, z_{42}, z_{33}\}$
	$\chi_{10} = \{z_{21}, z_{12}, z_{13}\}$
	$\chi_{11} = \{z_{31}, z_{42}, z_{13}\}$
	$\chi_{12} = \{z_{31}, z_{12}, z_{33}\}$
	$\chi_{13} = \{z_{21}, z_{22}, z_{43}\}$
	$\chi_{14} = \{z_{21}, z_{32}, z_{23}\}$
	$\chi_{15} = \{z_{31}, z_{22}, z_{23}\}$
	$\chi_{16} = \{z_{31}, z_{32}, z_{43}\}$

Corollary 5. *There exists a C_4-*TD[3, 1;4].

Proof. Let the 3 mutually orthogonal C_4-squares of order 4 are M_i, $1 \le i \le 3$. Define $Z = \{z_{xy}, xy \in \{1,2,3,4\} \times \{1,2,3\}\}$. For $1 \le i \le 3$, consider $\Sigma_i = \{z_{xi}\colon txn \in q\{1,2,3,4\}$, and then, $\Sigma = \{\Sigma_i\colon 1 \le i \le 3\}$. For $1 \le t \le 16$, define $\chi_t = \{z_{M_i(\lambda, t-(\lambda-1)n)i}\colon 1 \le i \le 3, 1 \le \lambda \le 4\}, 4(\lambda-1)+1 \le t \le 4\lambda$, and $\chi = \{\chi_t\colon 1 \le t \le 16\}$. Hence, Z is a set of 12 elements, Σ is a partition of Z into 3 groups, χ is a set of 3-subsets (blocks) of Z, every couple of points from different groups is found in precisely one block, and any block and any group have precisely one point in common. Now, the triple (Z, Σ, χ) satisfies the conditions of the graph-transversal design $C_4 - TD[3, 1; 4]$. □

Corollary 6. *There exists a $2S_2 - TD[3, 1; 4]$.*

Proof. Let the 3 mutually orthogonal $2S_2$-squares of order 4 are M_i, $1 \le i \le 3$. Define $Z = \{z_{xy}, xy \in \{1,2,3,4\} \times \{1,2,3\}\}$. For $1 \le i \le 3$ consider $\Sigma_i = \{z_{xi}\colon x \in \{1,2,3,4\}\}$, and then $\Sigma = \{\Sigma_i\colon 1 \le i \le 3\}$. For $1 \le t \le 16$, define $\chi_t = \{z_{M_i(\lambda, t-(\lambda-1)n)i}\colon 1 \le i \le 3, 1 \le \lambda \le 4\}, 4(\lambda-1)+1 \le t \le 4\lambda$ and $\chi = \{\chi_t\colon 1 \le t \le 16\}$. Hence, Z is a set of 12 elements, Σ is a partition of Z into 3 groups, χ is a set of 3-subsets (blocks) of Z, every couple of points from different groups is found in precisely one block, and any block and any group have precisely one point in common. Now, the triple (Z, Σ, χ) satisfies the conditions of the graph-transversal design $2S_2 - TD[3, 1; 4]$. □

3. Constructing Graph-Authentication Codes Based on Mutually Orthogonal Graph Squares

Firstly, we retrieve some basic fundamentals of authentication codes. More details on authentication codes can be found in [1, 2].

An authentication code is defined as a four tuple $A = (S, K, T, \delta)$ where S, K, T are three nonempty finite sets defined as source states set, keys set, tags set (authenticators set), respectively, and $\delta\colon K \times S \longrightarrow T$ is the encoding map. The map δ is needed not to be injective, but it should be surjective. For each key $\sigma \in K$, there is an authentication rule $e_\sigma \in \delta$, where $e_\sigma\colon S \longrightarrow T$.

The cardinalities $|S|, |K|, |T|$ are called the size parameters of the code A. For a specific authentication code A with $|S|, |K|, |T|$ as size parameters, we may describe it as $Ac(|S|, |K|, |T|)$.

Let $A = (S, K, T, \delta)$ be an authentication code. A graph $G(A)$ induced from A is constructed as follows:

(1) $V(G(A)) = K \cup T$

(2) $E(G(A)) = \{\{\sigma, t\} | \sigma \in K, t \in T, \exists s \in S\}$ such that $\{\delta(s, \sigma) = t\}$

(3) If $\{\sigma, t\} \in E(G(A))$, then such edge has a label s where $\delta(s, \sigma) = t$

This construction implies that the graph $G(A)$ is isomorphic to a bipartite graph with partition sets K and T. Moreover, the degree of each vertex in K equals $|S|$.

The motivation for using authentication codes is usually that the sender and receiver want to have a guarantee that any manipulations of a message s during transit are detected. For this, they randomly choose a private key $\sigma \in K$. A source state is simply the information that the sender wants to transmit to the receiver. When the sender needs to transmit the source state $s \in S$ to the receiver, he (or she) uses the authentication rule e_σ to construct the tag (authenticator) $t = e_\sigma(s)$. Then, an authenticated message m is formed by concatenating s and t and then sent over the channel, that is, $m = (s, t)$. When the receiver receives m, he or she computes $t' = e_\sigma(s)$. If $t' = t$, then the message is accepted as authentic; otherwise, it is rejected.

Authentication codes are used in communication channels in which an opponent is present in addition to the sender and the receiver. Such an opponent may play an impersonation attack or substitution attack. Through impersonation attacks, the opponent sends a message over the channel to the receiver and expects that the receiver will authentically accept it. In substitution attack, the opponent watches a message transmitted by the sender, and he replaces this message with another message and wants it to be accepted as authentic from the receiver. For each of these types of attacks, there is an associated probability such that the opponent may succeed to deceive the receiver. Let P_I stands for the probability, the opponent will succeed in the impersonation attack, and P_s stands for the probability of a successful substitution attack. For more security, the sender and receiver need to establish an authentication code with small values of P_I and P_s.

In the following theorem, we prove that mutually orthogonal graph squares MOGS can be used to construct an authentication code with $P_I = P_s = (1/|T|)$. We call this special code *a graph authentication code* $G - Ac(|S|, |K|, |T|)$.

Theorem 1. *Suppose there are k mutually orthogonal graph squares MOGS* $L_1, L_2, \ldots, L_k$ *each of order n. The entries of any* $L_i | 1 \leq i \leq k$ *are elements of* $\mathbb{Z}_n$*. Then, there is a graph authentication code* $G - Ac(|S|, |K|, |T|)$ *with* $|K| = n^2, |S| = k, |T| = n$*, and* $P_I = P_s = (1/n)$*.*

Proof

Claim 1: Mutually orthogonal graph squares $L_i | 1 \leq i \leq k$ can be reduced to a graph-authentication code $A = (S, K, T, \delta)$ as follows: let $|S| = k$, $|K| = n^2$, and $T = \mathbb{Z}_n$. For any $s_i \in S$, and $\sigma_j \in K, 1 \leq j \leq n^2$, set $\delta(\sigma_j, s_i) = L_i(x, y)$, and

$$(x, y) = \begin{cases} (1, j) & \text{if} \quad 1 \leq j \leq n \\ (2, j - n) & \text{if} \quad n + 1 \leq j \leq 2n \\ (3, j - 2n) & \text{if} \quad 2n + 1 \leq j \leq 3n \\ \vdots & \vdots \quad \vdots \\ \left(n, j - n^2 + n\right) & \text{if} \quad n^2 - n \leq j \leq n^2. \end{cases} \tag{4}$$

$L_i(x, y)$ is the element in the cell (x, y) of the graph squares L_i. Formula (4) is equivalent to $e_{\sigma_j}(s_i) = L_i(x, y) = t \in \mathbb{Z}_n$. Consequently, each $t \in T$ occurs exactly n times in each graph square, and then, the map δ is surjective. Hence, this reduction yields to an authentication code $A = (S, K, T, \delta)$.

Claim 2: Here, we will compute the probability P_I. Suppose that an opponent transmits any message $m = (s_i, t)$ into the channel. Then, m is accepted as authentic if and only if $t = e_{\sigma_j}(s_i)$, which occurs if and only if $\delta(\sigma_j, s_i) = t$. Since σ_j chosen randomly, it is only known to the sender and the receiver but not by the opponent. Let $\rho(s_i, t) = \left\{\sigma_j \colon \delta(\sigma_j, s_i) = t\right\}$. Since our code constructed from mutually orthogonal graph squares of order n, then each entry occurs exactly n times in each square. Following formula (4), it is easy to see that $|\rho(s_i, t)| = n$, and opponent's deception will succeed if and only if $\sigma_j \in \rho(s_i, t)$. Since $|K| = n^2$, it yields that the opponent will succeed to deceive the receiver with probability $(|\rho(s_i, t)|/|K|) = (1/n)$. Since this probability is independent of the message $m = (s_i, t)$ that opponent submits into the channel, so

$$P_I = \frac{1}{n}. \tag{5}$$

Claim 3: The second probability that we will compute is the substitution probability P_s. Suppose that an opponent observes an authentic message $m = (s_i, t)$ passing the channel. He or she changes it to another message $m' = (s_i', t')$ where $s_i \neq s_i'$ and desires that the receiver will accept it. As we have done in P_I, let $\rho(s_i, t) = \left\{\sigma_j \colon \delta(\sigma_j, s_i) = t\right\}$. Since the opponent is able to see the message m, this makes it easy for him or her to guess that $\sigma_j \in \rho(s_i, t)$. This means that the number of expected keys is reduced to n. The opponent will deceive the receiver if and only if $\sigma_j \in \rho(s_i', t')$. As it is known to the opponent that $\sigma_j \in \rho(s_i, t)$, then the private key σ_j satisfies that $\sigma_j \in \rho(s_i', t') \cap \rho(s_i, t)$. This code is constructed from mutually orthogonal graph squares of order n. Consequently, for any two of such squares, that is, L_u and L_v and for every $t \in \mathbb{Z}_n$ and every $t' \in \mathbb{Z}_n$, there is a unique cell (x, y) such that $L_u(x, y) = t$ and $L_v(x, y) = t'$. Hence, we conclude that $|\rho(s_i', t') \cap \rho(s_i, t)| = 1$. Till now, it is known to the opponent that $\sigma_j \in \rho(s_i, t)$, and he or she will succeed if and only if $\sigma_j \in \rho(s_i', t') \cap \rho(s_i, t)$. Therefore, the probability of a successful substitution attack is

Table 4: Some ingredients of MOGS from literature, see [3].

Ingredient	Order	Graph	Squares	k
(a)	n is a prime >2	$S_1 \cup (n-1/2)S_2$	$M_i = (a^i_{xy}), a^i_{xy} = \gamma, x = \delta,\ y = \gamma + (i-1)\delta + \delta^2; \gamma, \delta \in \mathbb{Z}_n, i \in \{1, \ldots, n\}.$	n
(b)	n is a prime >2	$(n-2)S_1 \cup S_2$	$M_i = (a^i_{xy}), a^i_{xy} = ix + y - h_x,\ i \in \{1, \ldots, n-1\},\ h_x = \begin{cases} 1 & \text{if } x = 1 \\ 0 & \text{otherwise} \end{cases}$	$n-1$
(c)	9	$S_3 \cup 3S_2$	$M_i = (a^i_{xy}), i \in \{1, 2, 3\}, a^i_{xy} = \delta, x = \gamma,\ y = \gamma^2 + (i-1)\gamma + \delta$, and $\gamma, \delta \in \mathbb{Z}_9$.	3
(d)	n is a prime >2	P_{n+1}	$M_i = (a^i_{xy}), a^i_{xy} = \gamma, x = \gamma + i\delta - \delta^2,\ y = \gamma + i\delta - \delta^2; \gamma, \delta, i \in \{1, \ldots, n\}.$	n

Note that k is the number of MOGS.

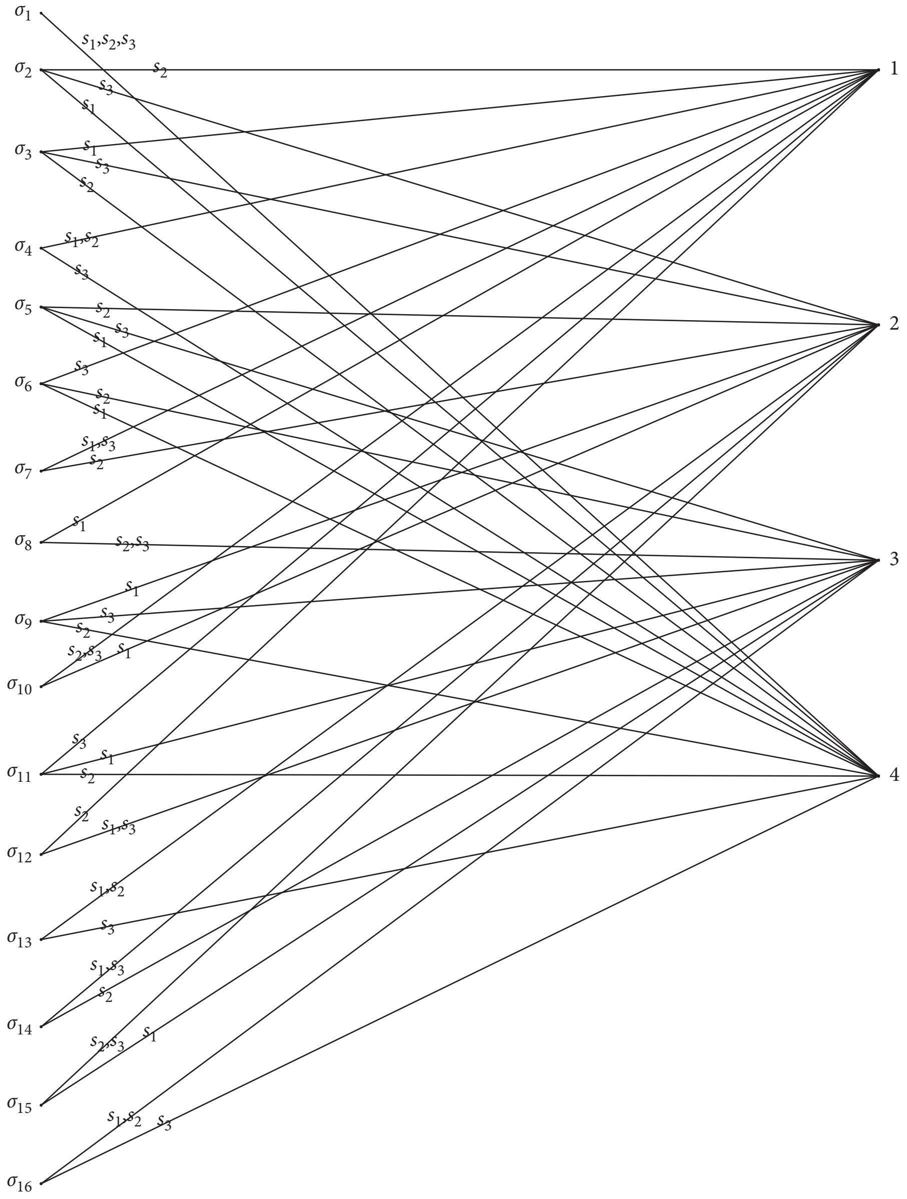


Figure 3: The induced graph of the code $C_4 - Ac(3, 16, 4)$.

Table 5: The blocks and the groups of a $2S_2 - TD[3,1;4]$ transversal design.

	$\chi_1 = \{z_{41}, z_{22}, z_{33}\}$
	$\chi_2 = \{z_{31}, z_{32}, z_{43}\}$
	$\chi_3 = \{z_{21}, z_{42}, z_{13}\}$
	$\chi_4 = \{z_{11}, z_{12}, z_{23}\}$
	$\chi_5 = \{z_{21}, z_{32}, z_{33}\}$
	$\chi_6 = \{z_{11}, z_{22}, z_{43}\}$
$\Sigma_1 = \{z_{11}, z_{21}, z_{31}, z_{41}\}$	$\chi_7 = \{z_{41}, z_{12}, z_{13}\}$
$\Sigma_2 = \{z_{12}, z_{22}, z_{32}, z_{42}\}$	$\chi_8 = \{z_{31}, z_{42}, z_{23}\}$
$\Sigma_3 = \{z_{13}, z_{23}, z_{33}, z_{43}\}$	$\chi_9 = \{z_{41}, z_{32}, z_{23}\}$
	$\chi_{10} = \{z_{31}, z_{22}, z_{13}\}$
	$\chi_{11} = \{z_{21}, z_{12}, z_{43}\}$
	$\chi_{12} = \{z_{11}, z_{42}, z_{33}\}$
	$\chi_{13} = \{z_{21}, z_{22}, z_{23}\}$
	$\chi_{14} = \{z_{11}, z_{32}, z_{13}\}$
	$\chi_{15} = \{z_{41}, z_{42}, z_{43}\}$
	$\chi_{16} = \{z_{31}, z_{12}, z_{33}\}$

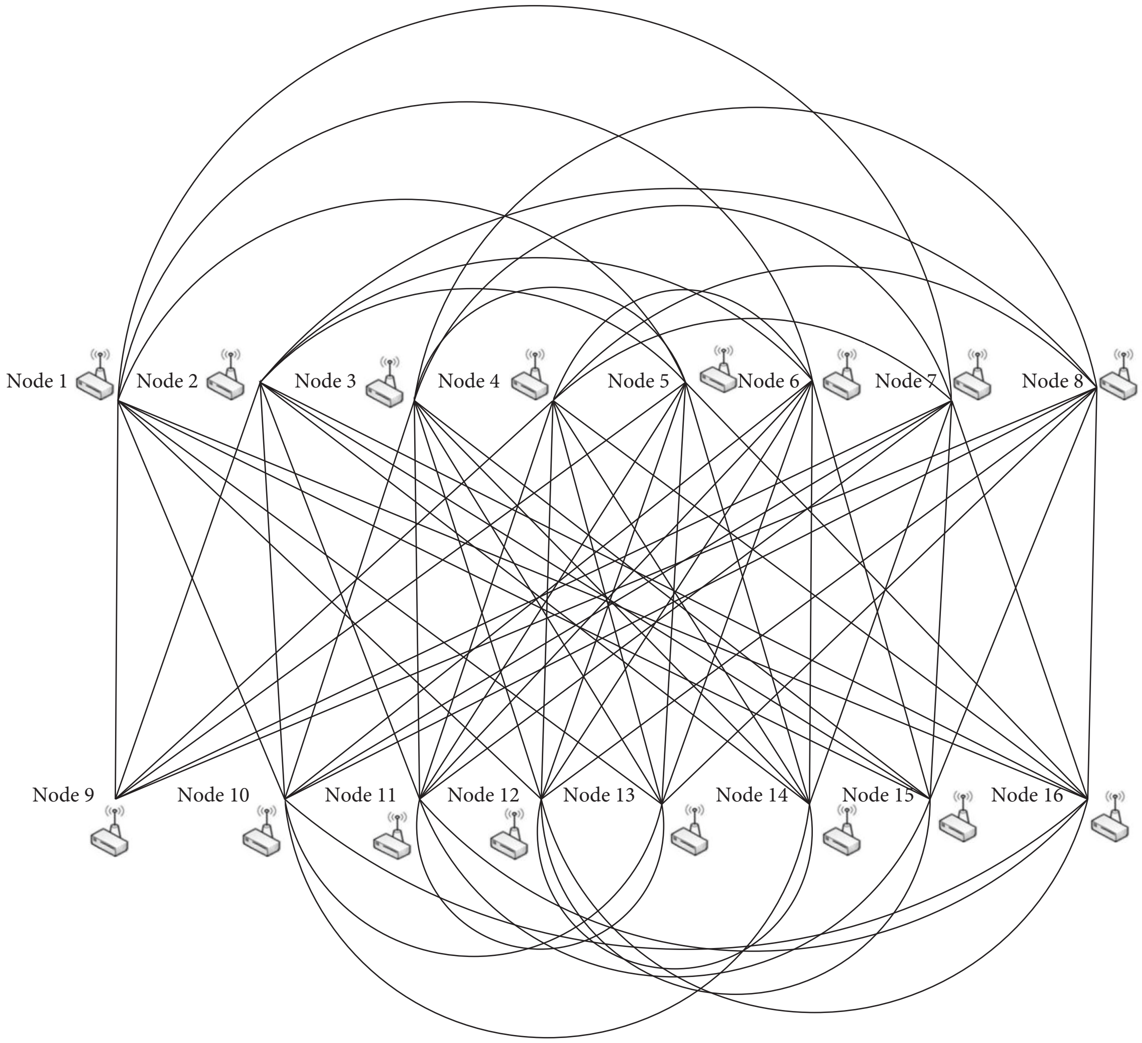


Figure 4: Wireless sensor network of 16 nodes corresponding to the $2S_2$ – $TD[3,\ 1;\ 4]$.

$$P_s = \frac{\left|\rho\left(s_i', t'\right) \cap \rho\left(s_i, t\right)\right|}{\left|\rho\left(s_i, t\right)\right|} = \frac{1}{n}. \tag{6}$$

□

Lemma 1. *There exists a* $C_4 - Ac(3,16,4)$ *with* $P_I = P_s = (1/4)$.

Proof. Let the 3 mutually orthogonal C_4-squares of the order 4 be M_i, $1 \leq i \leq 3$ listed in Table 4. Define an authentication code with three sources states s_1, s_2, s_3. The key set $K = \left\{\sigma_j\colon 1 \leq j \leq 16\right\}$. For each pair (σ_j, s_i), use formula (4) to set $\delta(\sigma_j, s_i)$. The induced graph of this reduction is shown in Figure 3. By straightforward application of Theorem 1, the code is constructed from mutually orthogonal C_4-squares of the order 4 has $P_I = P_s = (1/4)$. □

4. Applications of the Graph-Transversal Designs in Key Predistribution in Wireless Sensor Network

The balance of key content in different sensor nodes can be achieved by combinatorial design [19]; the maximum number of couples of nodes may communicate directly by a pairwise common key. The transversal design is a combinatorial design that can introduce a deterministic nature of key distribution [20]. In [21], the authors proposed the application of transversal design in key predistribution in wireless sensor networks. Now, we introduce an example to show the application of the graph-transversal designs. From Example 3, we can construct the $2S2 - TD[3,1;4]$ transversal design as shown in Table 5.

In Table 5, each block represents the key ids of a certain node in a sensor network. The numbers in the blocks represent the set of key ids. Here, the common key between blocks χ_4 and χ_6 is z_{11}. The maximum number of shared key between two nodes is 1 in the transversal design. Consequently, it may happen that there is no shared key between two nodes. For instance, nodes 1 and 2 have not any common key. Therefore, if they want to communicate, they need one or more intermediate nodes. In Table 5, the block χ_5 has a common key with both the blocks χ_1 and χ_2. Hence, blocks χ_1 and χ_2 can communicate through block χ_5 by key z_{33} and z_{32}, respectively.

Now, we can construct a wireless sensor network of 16 nodes corresponding to the $2S_2 - TD[3,1;4]$ as shown in Figure 4 such that there is a link between two nodes if there is a common key between them.

5. Conclusion

The importance of combinatorial design theory can be attributed in large degree to its continued deep interactions with algebra, geometry, and number theory and its applications in communications and coding theory. Combinatorial design theory is mature and rich in wide practical applications today. The paper you hold in your hands presents a seamless interaction of mutually orthogonal graph squares (MOGS), graph-transversal designs, and authentication codes. MOGS is the generalization of the mutually orthogonal Latin squares used for constructing the transversal designs; hence, the MOGS helps us to construct new interesting graph-transversal designs and authentication codes. The paper's novelty is demonstrated by the fact that it is the first to construct graph-transversal designs and graph-authentication codes based on MOGS concerned with complete bipartite graphs. We will strive to enhance the existing methods and propose new algorithms in the future to make them applicable for all classes of graphs that can be used to construct new graph-transversal designs and graph-authentication codes.

Nomenclature

$E(G)$:	Edge set of a graph G
lG:	l disjoint copies of a graph G
$G \cup H$:	Disjoint union of the graphs G and H
K_m:	Complete graph of size m
P_k:	Path graph with k vertices and K–1 edges
S_n:	Star graph with n edges
C_k:	Cycle graph with k vertices and k edges
$K_{m,n}$:	Complete bipartite graph with partite sets of sizes m and n
$N(n; G)$:	The maximum number of mutually orthogonal graphs squares of order n. Such that all these graphs are isomorphic to a graph G.

Data Availability

The data used to support the findings of this study are available from the corresponding author on request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, Chapman & Hall/CRC, Boca Raton, FL, USA, 2nd edition, 2007.

[2] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer, New York, NY, USA, 2004.

[3] R. El-Shanawany, *Orthogonal Double Covers of Complete Bipartite Graphs*, Ph.D. thesis, University of Rostock, Rostock, Germany, 2001.

[4] R. El-Shanawany and A. El-Mesady, "Mutually orthogonal graph squares for disjoint union of stars," *ARS Combinatoria*, vol. 149, pp. 83–91, 2020.

[5] R. C. Bose and S. S. Shrikhande, "On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler," *Transactions of American Mathematical Society*, vol. 95, no. 2, pp. 191–209, 1960.

[6] R. C. Bose, S. S. Shrikhande, and E. T. Parker, "Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture," *Canadian Journal of Mathematics*, vol. 12, pp. 189–203, 1960.

[7] R. M. Wilson, “Concerning the number of mutually orthogonal Latin squares,” *Discrete Mathematics*, vol. 9, no. 2, pp. 181–198, 1974.

[8] C. Colbourn and J. Dinitz, “Mutually orthogonal Latin squares: a brief survey of constructions,” *Journal of Statistical Planning and Inference*, vol. 95, no. 1-2, pp. 9–48, 2001.

[9] R. Sampathkumar and S. Srinivasan, “Mutually orthogonal graph squares,” *Journal of Combinatorial Designs*, vol. 17, no. 5, pp. 369–373, 2009.

[10] R. El-Shanawany, “On mutually orthogonal graph-path squares,” *Open Journal of Discrete Mathematics*, vol. 06, no. 01, pp. 7–12, 2016.

[11] R. El-Shanawany, “On mutually orthogonal disjoint copies of graph squares,” *Note di Matematica*, vol. 36, pp. 89–98, 2016.

[12] M. Higazy, “λ-mutually orthogonal covers of complete bipartite graphs,” *Advances and Applications in Discrete Mathematics*, vol. 17, pp. 151–167, 2016.

[13] R. El-Shanawany, A. El-Mesady, and S. M. Shaaban, “Mutually orthogonal graph squares for disjoint union of paths,” *Applied Mathematical Sciences*, vol. 12, no. 7, pp. 303–310, 2018.

[14] R. El-Shanawany and A. El-Mesady, “On mutually orthogonal certain graph squares,” *Online Journal of Analytic Combinatorics*, p. 14, 2020.

[15] R. Sampathkumar and S. Srinivasan, “More mutually orthogonal graph squares,” *Utilitas Mathematica*, vol. 91, pp. 345–354, 2013.

[16] A. El-Mesady, Y. S. Hamed, and M. Abualnaja Khadijah, “A novel application on mutually orthogonal graph squares and graph-orthogonal arrays,” *AIMS Mathematics*, vol. 7, no. 5, pp. 7349–7373, 2022.

[17] M. Higazy, A. El-Mesady, and M. S. Mohamed, “On graph-orthogonal arrays by mutually orthogonal graph squares,” *Symmetry*, vol. 12, no. 11, 2020.

[18] A. El-Mesady and S. M. Shaaban, “Generalization of MacNeish’s kronecker product theorem of mutually orthogonal Latin squares,” *AKCE International Journal of Graphs and Combinatorics*, vol. 18, no. 2, pp. 117–122, 2021.

[19] S. A. Camtepe and B. Yener, “Combinatorial design of key distribution mechanisms for wireless sensor networks,” in *ESORICS. Volume 3193 of Lecture Notes in Computer Science*, P. Samarati, P. Y. A. Ryan, D. Gollmann, and R. Molva, Eds., pp. 293–308, Springer, Berlin, Germany, 2004.

[20] J. Lee and D. R. Stinson, “Deterministic key pre distribution schemes for distributed sensor networks,” in *LNCS*vol. 3357, pp. 294–307, Proceeding of SAC, 2004.

[21] J. Lee and D. R. Stinson, “On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs,” *ACM Transactions on Information and System Security*, vol. 11, no. 2, pp. 1–35, 2008.