Mathematics

AIMS Mathematics, 7(5): 7349–7373.
DOI: 10.3934/math.2022410
Received: 01 November 2021
Revised: 21 December 2021
Accepted: 23 December 2021
Published: 10 February 2022

http://www.aimspress.com/journal/Math

Research article

A novel application on mutually orthogonal graph squares and graph-orthogonal arrays

A. El-Mesady[1],*, Y. S. Hamed[2] and Khadijah M. Abualnaja[2]

[1] Department of Physics and Engineering Mathematics, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[2] Department of Mathematics and Statistics, College of Science, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

* **Correspondence:** Email: AHMED.IBRAHIEM81@el-eng.menofia.edu.eg.

Abstract: Security of personal information has become a major concern due to the increasing use of the Internet by individuals in the digital world. The main purpose here is to prevent an unauthorized person from gaining access to confidential information. The solution to such a problem is by authentication of users. Authentication has a very important role in achieving security. Mutually orthogonal graph squares (MOGS) are considered the generalization of mutually orthogonal Latin squares (MOLS). Also, MOGS are generated from edge decompositions of complete bipartite graphs by isomorphic graphs. Graph-orthogonal arrays can be constructed by MOGS. In this paper, graph-orthogonal arrays are used for constructing authentication codes. These arrays are the encoding matrices of authentication tags. We introduce the concepts and basic theorems of MOGS, graph-orthogonal arrays, and authentication codes. After constructing graph-orthogonal arrays by MOGS, then there is an established mapping between graph-orthogonal arrays and message set. This manages us to construct perfect non-splitting and splitting Cartesian authentication codes. In both cases, we calculate the probabilities of successful impersonation attacks and substitution attacks. Besides that, the performance of constructed non-splitting and splitting authentication codes is analyzed. In the end, optimal authentication codes and secure authentication codes are constructed.

Keywords: Latin squares; graph squares; graph-orthogonal arrays; Cartesian authentication codes; non-splitting authentication codes; splitting authentication codes; optimal authentication codes
Mathematics Subject Classification: 05B30, 05C70, 94A60, 94A62

Abbreviations: MOLS: Mutually orthogonal Latin squares; MOGS: Mutually orthogonal graph squares; BIBD: Balanced incomplete block designs; kF: k isolated copies of graph F; K_m: Complete graph with m vertices; $K_{m,n}$: Complete bipartite graph with size $m+n$ where vertices are classified into two sets with sizes m and n; P_m: Path graph on m vertices; $E(G)$: Edge set of graph G; $V(G)$: Vertex set of graph G; $G \cup H$: Disjoint union of graphs G and H; P_I or P_0: Probability of successful impersonation attacks; P_s or P_1: Probability of successful substitution attacks; X_n: The set $\{1,2,\ldots,n\}$; $L(x,y)$: Entry in row x and column y of square matrix L

1. Introduction

Nowadays, information technology is widely used in almost all disciplines around the world. Convenience to people's lives has been brought due to the unprecedented revolution of network technology. At the same time, a huge and tough problem also arises in front of human beings-information security issues, such as information leakage, viruses, tampering, and so on. Since ancient times, people have realized the importance of protecting the confidentiality of sensitive messages. Cryptology (secret writing) has been an established problem. This science was mainly concerned with diplomatic and military applications for a long period. In the modern era, storing and transmitting information has become cheap and simple based on strong techniques of information. There is a way by which a huge amount of information can be transferred, but almost anyone can access it. Security communications have several problems such as data integrity, confidentiality authentication, secret sharing, hidden information, and non-repudiation. Such problems can be solved by steganography and cryptography. Some means and methods are used to prevent information from being stolen or damaged to ensure information security. In this section, we just introduce a brief overview of previous works and a summary of our contributions. In 1948, a mathematical theory of communication was presented by Shannon [1]. This topic gave birth to information theory. In 1974, the authors of [2] proposed authentication codes. Simmons introduced the authentication code model described in [3–6]. Cryptology is associated with many new problems. For instance, an adversary can read transmitted messages and change them. Also, an adversary could intervene illegally to construct and send a fraudulent message to a receiver, and he or she hopes that the receiver takes a wrong decision.

A receiver may be worried about changing the content of a message by an adversary in transmission. Also, a receiver is worried about knowing a real sender. Authentication of messages takes care of these two major points. In modern times, the two important aspects of information security are authentication and secrecy problems. Authentication protection can be obtained by an authentication scheme, while secrecy protection can be obtained by a secrecy scheme. Authentication and secrecy are two independent aspects of information security. In some situations, secrecy may be essential, and in other situations, it is not essential. Moreover, secrecy may or may not be taken into account in the authentication scheme. Authentication is responsible for the protection of messages from tampering and impersonating by a deceptive adversary, and secrecy protects sensitive messages from eavesdropping.

An adversary can cheat a receiver. Before a transmitter sends any message to a receiver, an adversary can send a bogus message to a receiver, and a receiver will accept it as a genuine message. This may lead to a wrong decision taken by a receiver. What an adversary did, in this case, is called an impersonation attack. Also, an adversary can launch another kind of attack called a substitution attack. Also, an adversary can launch another kind of attack called a substitution attack. In a substitution attack, an adversary can change the content of an observed message. And a receiver also accepts it; this will lead to a different action from what a transmitter intended. Authentication code prevents these attacks. The probability of a successful impersonation attack is denoted by P_I or P_0, and the probability of a successful substitution attack is denoted by P_s or P_1.

There is a wide and considerable literature on authentication codes. The authors in [7] constructed authentication codes using groups. Some linear authentication codes were constructed in [8]. Bipartite graphs were used to construct authentication codes with secrecy [9]. From geometries over finite fields, several authors constructed Cartesian authentication codes, see, for example, [10–17]. Authentication codes without splitting were studied in several papers [18–26], while De Soete handled authentication codes with splitting in [27]. Optimal authentication codes also were intensively studied [5, 24, 28–30]. In authentication codes, "optimal" means that the number of keys (encoding rules) and deception probabilities are as small as possible. Combinatorial structures such as difference sets, BIBDs, external BIBDs (EBIBDs), splitting BIBDs, and external difference families (EDFs) were used for constructing optimal authentication codes. And also, in a reverse way, optimal authentication codes were used to construct some of the aforementioned combinatorial structures. In this paper, we propose a new combinatorial structure based on MOGS which correspond to mutually orthogonal edge decompositions of complete bipartite graphs by several graphs such as paths, stars, disjoint union of graphs, and so on. Additional background material for this field may be found in [31–36].

The main contributions made in this manuscript are the following: The decomposition of complete bipartite graph $K_{n,n}$ can be constructed by a large number of graphs such as stars, paths, cycles, and so forth. We tried to find mutually orthogonal decompositions of $K_{n,n}$. These decompositions can be converted to MOGS. Then these graph squares are used to construct graph-orthogonal arrays. By these graph-orthogonal arrays, we can construct a large number of authentication codes where there is a large number of graphs that can be used for decompositions of complete bipartite graph $K_{n,n}$. Hence, if an opponent knows the used code generated by a certain graph, then we can use another graph for the construction of an authentication code. Also, for each graph, we will get a code with new characteristics. Our work is considered a directed application for graph decompositions of $K_{n,n}$ in coding theory. This is a new proposal, and it will open a new horizon for research in this direction, and it will be the beginning of a lot of future work. This proposal leads to the construction of Cartesian authentication codes with splitting and non-splitting. In both cases, we prove that the constructed authentication codes are perfect. There is a special case of MOGS called mutually orthogonal Latin squares (MOLS) which are used for constructing optimal authentication codes. Also, we use Latin squares to construct secure authentication codes.

The remaining part of the paper is organized into the following six sections. Detailed definitions and basic results on graph-orthogonal arrays and MOGS are found in Subsection 2.1, while Subsection 2.2 describes basic theorems and definitions of authentication schemes and the probability of successful deceptions. Section 3 studies the construction of general perfect non-splitting Cartesian authentication codes based on MOGS. Section 4 studies the construction of general perfect splitting Cartesian authentication codes based on MOGS. The focus of Section 5 is on the construction of optimal authentication codes based on MOLS that are considered a special case of MOGS. Authentication codes with confidentiality based on graph squares are presented in Section 6. Finally, some concluding remarks are given in Section 7.

2. Preliminaries

2.1. Related definitions and theorems of graph-orthogonal arrays and MOGS

In this subsection, we present definitions of graph-orthogonal arrays and MOGS, along with a few basic results.

Definition 1 ([37]). *Assume that* G *is a subgraph of* $K_{n,n}$ *with size* n. *A square matrix* L *of order* n *is called a* G*-square if each element in* $X_n = \{1,2,..,n\}$*appears precisely* n *times in* L, *and all the graphs* G_i *where* $E(G_i) = \{(x_0, y_1): L(x_0, y_1) = i, i \in X_n\}$ *are isomorphic to* G. *The index set for the rows of* L *is the set* $X_n \times \{0\}$ *and the index set for the columns of* L *is the set* $X_n \times \{1\}$. *Each* G*-square of order* n *represents an edge decomposition of* $K_{n,n}$ *by the graph* G.

Example 1. *An edge decomposition of* $K_{3,3}$ *by* $K_{1,3}$ *is shown in Figure 1. There is a* G*-square* L *of order* 3 *corresponding to this decomposition, where* G *is isomorphic to* $K_{1,3}$. *Here* n=3, $X_3 = \{1,2,3\}$. *The* $K_{1,3}$*-square can be represented as sollows:*

$$L = \begin{array}{cccc} & 1_1 & 2_1 & 3_1 \\ 1_0 & 1 & 1 & 1 \\ 2_0 & 2 & 2 & 2 \\ 3_0 & 3 & 3 & 3 \end{array}$$

From L, *it is clear that the rows are indexed by* $X_3 \times \{0\} = \{1_0, 2_0, 3_0\}$, *the columns are indexed by* $X_3 \times \{1\} = \{1_1, 2_1, 3_1\}$, *and each element in* $X_3 = \{1,2,3\}$ *appears precisely* 3 *times in* L. *From Figure 1, the edge set and the vertex set for* G_1, G_2, *and* G_2 *are as follows:*

$$E(G_1) = \{(x_0, y_1): L(x_0, y_1) = 1\} = \{(1_0, 1_1), (1_0, 2_1), (1_0, 3_1)\}, V(G_1) = \{1_0, 1_1, 2_1, 3_1\},$$

$$E(G_2) = \{(x_0, y_1): L(x_0, y_1) = 2\} = \{(2_0, 1_1), (2_0, 2_1), (2_0, 3_1)\}, V(G_2) = \{2_0, 1_1, 2_1, 3_1\},$$

$$E(G_3) = \{(x_0, y_1): L(x_0, y_1) = 3\} = \{(3_0, 1_1), (3_0, 2_1), (3_0, 3_1), V(G_3) = \{3_0, 1_1, 2_1, 3_1\}.$$

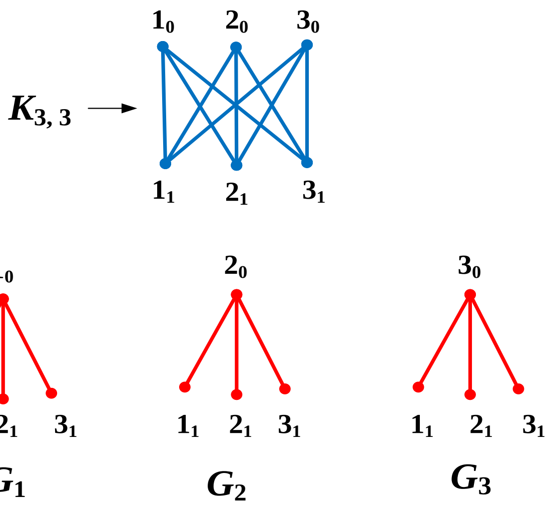


Figure 1. An edge decomposition of $K_{3,3}$ by $K_{1,3}$.

Definition 2 ([37])**.** *Let* L_1 *be a G-square of order* n *with entries from a set* A *and* M_2 *be a G-square of order* n *with entries from a set* B*. Then* L_1 *and* L_2 *are orthogonal if, for every* $a \in A$ *and for every* $b \in B$*, there is exactly one cell* (x_0, y_1) *such that* $L_1(x_0, y_1) = a$ *and* $L_2(x_0, y_1) = b$*. A set of* k *G-squares of order* n*, say* $L_1, \dots, L_k$*, are called mutually orthogonal (pairwise orthogonal) G-squares (MOGS) if* L_i *and* L_j *are orthogonal for all* $1 \le i < j \le k$*.*
Notice that in this paper, we consider $A = B = X_n$*.*

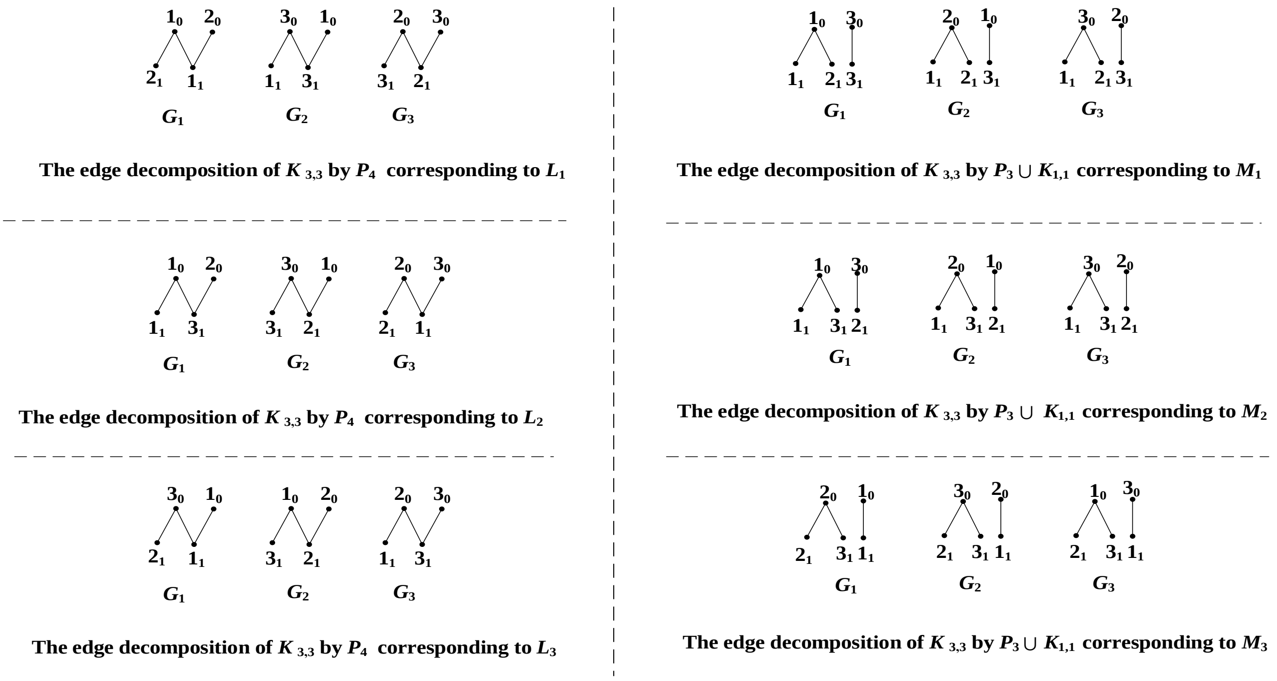
Example 2. *Three MOGS for the graph* P_4 *are represented by the squares* L_1*,* L_2*, and* L_3*. Also, three MOGS for the graph* $P_3 \cup K_{1,1}$ *are represented by the squares* M_1*,* M_2*, and* M_3*. See Figure 2 for more illustration.*

$$L_1 = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 3 & 3 \\ 2 & 3 & 2 \end{bmatrix} L_2 = \begin{bmatrix} 1 & 2 & 1 \\ 3 & 3 & 1 \\ 3 & 2 & 2 \end{bmatrix} L_3 = \begin{bmatrix} 1 & 2 & 2 \\ 3 & 2 & 3 \\ 1 & 1 & 3 \end{bmatrix}$$

$$M_1 = \begin{bmatrix} 1 & 1 & 2 \\ 2 & 2 & 3 \\ 3 & 3 & 1 \end{bmatrix} M_2 = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 3 & 2 \\ 3 & 1 & 3 \end{bmatrix} M_3 = \begin{bmatrix} 1 & 3 & 3 \\ 2 & 1 & 1 \\ 3 & 2 & 2 \end{bmatrix}$$

The superimposition of L_1 and L_2 is as follows:

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


1_0 2_0 2_1 1_1 G_1
3_0 1_0 1_1 3_1 G_2
2_0 3_0 3_1 2_1 G_3
1_0 3_0 1_1 2_1 3_1 G_1
2_0 1_0 1_1 2_1 3_1 G_2
3_0 2_0 1_1 2_1 3_1 G_3
1_0 2_0 1_1 3_1 G_1
3_0 1_0 3_1 2_1 G_2
2_0 3_0 2_1 1_1 G_3
1_0 3_0 1_1 3_1 2_1 G_1
2_0 1_0 1_1 3_1 2_1 G_2
3_0 2_0 1_1 3_1 2_1 G_3
3_0 1_0 2_1 1_1 G_1
1_0 2_0 3_1 2_1 G_2
2_0 3_0 1_1 3_1 G_3
2_0 1_0 2_1 3_1 1_1 G_1
3_0 2_0 2_1 3_1 1_1 G_2
1_0 3_0 2_1 3_1 1_1 G_3

The edge decomposition of $K_{3,3}$ by P_4 corresponding to L_1

The edge decomposition of $K_{3,3}$ by $P_3 \cup K_{1,1}$ corresponding to M_1

The edge decomposition of $K_{3,3}$ by P_4 corresponding to L_2

The edge decomposition of $K_{3,3}$ by $P_3 \cup K_{1,1}$ corresponding to M_2

The edge decomposition of $K_{3,3}$ by P_4 corresponding to L_3

The edge decomposition of $K_{3,3}$ by $P_3 \cup K_{1,1}$ corresponding to M_3

Figure 2. Three mutually orthogonal edge decompositions (MOEDs) of $K_{3,3}$ by P_4, and three MOEDs of $K_{3,3}$ by $P_3 \cup K_{1,1}$.

All the ordered pairs are different and equivalent to $X_3 \times X_3 = \{1,2,3\} \times \{1,2,3\}$. Hence, L_1 and L_2

are orthogonal. Similarly, the orthogonality between L_1 and L_3, L_2 and L_3, M_1 and M_2, M_1 and M_3, M_2 and M_3 can be shown.

Theorem 1 ([38])**.** *For every bipartite graph G with $n \geq 2$ edges, we have $N(n, G) \leq n$, where $N(n, G)$ refers to the maximal number of G-squares in the largest possible set of mutually orthogonal G-squares of order n.*

There are several results on MOGS in the literature. For a survey on MOGS, see [37−45].

Definition 3 ([46])**.** *Suppose B is a symbol set with cardinality $|B| = m \geq 1$, μ, and $\lambda \geq 2$ are integers. An orthogonal array A is an $\mu m^2 \times \lambda$ array with entries from B such that within any two columns from A, every ordered pair of symbols from B occurs in exactly μ rows of A, denoted as $OA(m, \lambda, \mu)$.*

Definition 4. *If we have λ mutually orthogonal $m \times m$ G-squares, then by converting each G-square to an $m^2 \times 1$ array by juxtaposing the m columns of the G-square, then we have λ arrays with $m^2 \times 1$ dimension, then by combining these arrays we get an $m^2 \times \lambda$ array which is called a graph-orthogonal array G-$OA(m, \lambda, 1)$.*

Proposition 1 ([40])**.** *If we have λ mutually orthogonal $m \times m$ G-squares based on m symbols, then, we can obtain a G-orthogonal array G-$OA(m, \lambda, 1)$.*

Proof. The construction technique is as follows. Convert each of the λ mutually orthogonal $m \times m$ G-squares to an $m^2 \times 1$ array by juxtaposing the m columns of the G-square. Then, these arrays are combined to construct an $m^2 \times \lambda$ array. Since there are λ mutually orthogonal G-squares based on m symbols, the number of the levels equals $m.$ Furthermore, since the λ G-squares are mutually orthogonal, then the superimposition of any two columns of the $m^2 \times \lambda$ array gives $X_m \times X_m$, $i.e.$, the $m^2 \times \lambda$ array has strength two. Every ordered pair of symbols from X_m occurs in exactly one row of G-$OA(m, \lambda, 1)$.

Example 3. *We have 3 MOGS A_1, A_2, and A_3 ($4K_2$-squares). Then, there is an $4K_2$-$OA(4,3,1)$ that can be represented by $\mathcal{A}$,*

$$A_1 = \begin{bmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 4 & 2 & 3 & 1 \\ 1 & 3 & 2 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 4 & 1 & 2 & 3 \\ 1 & 4 & 3 & 2 \\ 2 & 3 & 4 & 1 \\ 3 & 2 & 1 & 4 \end{bmatrix}$$

$$\mathcal{A} = \begin{bmatrix} 4 & 4 & 4 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \\ 3 & 2 & 1 \\ 2 & 3 & 4 \\ 1 & 4 & 3 \\ 4 & 1 & 2 \\ 1 & 3 & 2 \\ 4 & 2 & 3 \\ 3 & 1 & 4 \\ 2 & 4 & 1 \\ 2 & 1 & 3 \\ 3 & 4 & 2 \\ 4 & 3 & 1 \\ 1 & 2 & 4 \end{bmatrix}$$

In what follows, we assume that the probability distribution of sources and encoding rules is uniform.

2.2 Basic theorems and definitions of authentication codes

A transmitter, receiver, and adversary are three participants in the authentication model considered in this paper. A sequence of source states can be conveyed to a receiver by a transmitter. An adversary can deceive a receiver by impersonating a transmitter and sending fraudulent messages or tampering with messages sent to a receiver. Transmitter and receiver must cooperate to deal with a spoofing attack by an adversary. Both sender and receiver must trust each other in this model.

In what follows, the set of all sources states that a transmitter will send to a receiver will be denoted by $\mathcal{G}$. Source states are encoded based on one encoding rule for protecting source states from an adversary attack. The set of all encoding rules will be denoted by $\mathcal{H}.$ The set of all possible encoded messages will be denoted by $\mathcal{R}$. The one-to-one mapping $h \in \mathcal{H}$ is a mapping from $\mathcal{G}$ to $\mathcal{R}$. There is always an agreement between the transmitter and the receiver on an encoding rule h before the transmission process. The encoding rule h is considered a secret to an adversary. The source states are encoded using h by a transmitter. Then, through an insecure public channel, encoded messages are transferred. A receiver receives a message sent by a transmitter and checks whether it belongs to the range $h(\mathcal{G})$. Only messages belonging to the range $h(\mathcal{G})$ will be accepted as authentic. It is assumed that the adversary is fully familiar with the system, including all encoding rules. But, the particular encoding rule known by a transmitter and a receiver is unknown to an adversary. If the fraudulent message of the adversary is compatible with the used encoding rule, then the adversary is successful in his attack. The possibility of successful deception by an adversary can be decreased by repeatedly alternating the used encoding rule. Formally, the authentication code can be defined as follows.

Definition 5 ([47]). *Suppose $\mathcal{G}$, $\mathcal{H}$, and $\mathcal{R}$ are three non-empty finite sets, where $\mathcal{G}$ is the set of source states, $\mathcal{H}$ the set of encoding rules, and $\mathcal{R}$ the set of encoded messages. Suppose $\varphi : \mathcal{G} \times \mathcal{H} \to \mathcal{R}$ is a map, then the four tuple $(\mathcal{G}, \mathcal{H}, \mathcal{R}; \varphi)$ is called an authentication code, if*
(i) the map φ is surjective and
(ii) for any $r \in \mathcal{R}$ and $h \in \mathcal{H}$, if there is an element $g \in \mathcal{G}$ satisfying $\varphi(g,h) = r$, then such an element g is uniquely determined by the given r and h.

Now, we show the parameters of an authentication code as follows: $|\mathcal{G}| = \alpha$, $|\mathcal{H}| = \beta$, and $|\mathcal{R}| = \gamma$. Hence, the authentication code can be denoted by $AC(\alpha, \beta, \gamma)$. For the authentication code, we can construct a $\beta \times \alpha$ encoding matrix (A). Rows of A correspond to the encoding rule of an authentication code, and columns of A correspond to the source of an authentication code.

Definition 6 ([47]). *Let $g \in \mathcal{G}$, put $\mathcal{R}(g) = \{r \in \mathcal{R} | r = h(g)$ for some $h \in \mathcal{H}\}$. The set $\mathcal{R}$ represents messages that can be used to transmit the source state g. If $\mathcal{R}(g_1)$ and $\mathcal{R}(g_2)$ are disjointed, for any two source states g_1 and g_2, the authentication codes, in this case, are called Cartesian codes. Cartesian codes have no secrecy since one may know the source state once the transmitted message is observed.*

In a simplified way, Cartesian authentication codes can be redefined as follows: regardless of the used encoding rule, if you know the message r, you can know the corresponding source g, so the Cartesian authentication codes are without secrecy.

Definition 7 ([47])**.** *Let* $(\mathcal{G},\mathcal{H},\mathcal{R};\varphi)$ *be an authentication code. This authentication code is called non-Cartesian if for any* $r\in\mathcal{R}$ *and* $h\in\mathcal{H}$*, there is a unique* $g\in\mathcal{G}$ *such that* $\varphi(g,h)=r$*. Non-Cartesian authentication codes are with secrecy.*

Definition 8 ([46])**.** *Let* $(\mathcal{G},\mathcal{H},\mathcal{R};\varphi)$ *be an authentication code. This authentication code is said to have splitting if, under the same encoding rule* $h\in\mathcal{H}$*, more than one message corresponds to a source state* $g\in\mathcal{G}$*.*

Definition 9 ([47])**.** *Let* $(\mathcal{G},\mathcal{H},\mathcal{R};\varphi)$ *be an authentication code. This authentication code is said to have no splitting if* g *can only correspond to one message* r *under the action of* h*.*

Definition 10 ([47])**.** *The Cartesian authentication code* $(\mathcal{G},\mathcal{H},\mathcal{R};\varphi)$ *is called an optimal Cartesian authentication code if* $|\mathcal{G}|=\alpha+1$*,* $|\mathcal{H}|=\alpha^2$*,* $|\mathcal{R}|=\alpha(\alpha+1)$ *and* $P_0=P_1=\frac{1}{\alpha}$*.*

Definition 11 ([47])**.** *For the authentication code* $(\mathcal{G},\mathcal{H},\mathcal{R};\varphi)$*, if* $\log_2 P_0=\log_2 P_1=-I(\mathcal{R};\mathcal{H})$*, then the authentication code, in this case, is perfect, where*

$$I(\mathcal{R};\mathcal{H})=H(\mathcal{R})-H(\mathcal{R}|\mathcal{H})=\sum_r P(r)\log_2\frac{1}{P(r)}-\sum_{r,h_x}P(r,h_x)\log_2\frac{1}{P(r|h_x)}, \tag{1}$$

where $H(\mathcal{R})$ is the entropy of $\mathcal{R}$, $H(\mathcal{R}|\mathcal{H})$ is the entropy of $\mathcal{R}|\mathcal{H}$, and P refers to the probability.

In perfect authentication codes, it can be seen that P_0 and P_1 are the minimum. For the probability of a successful impersonation attack P_0, there is an agreement between a sender and a receiver about the encoding rule h in advance.

In impersonation attacks, an adversary does not know which authentication tag each source corresponds to under this encoding rule h. Hence, an adversary arbitrarily selects a source g and an authenticator $a\in T$ (T refers to the set of authentication tags). Impersonation attacks succeed if the message (g,a) satisfies $h(g)=a$, and P_0 can be expressed as follows:

$$P_0=\frac{\max_{g\in\mathcal{G},a\in T}\left|\left\{h\in\mathcal{H}\middle|h(g)=a\right\}\right|}{|\mathcal{H}|}. \tag{2}$$

For the probability of a successful substitution attack P_1, there is an agreement between a sender and a receiver about the encoding rule h that acts on the message r. A message $r=(g,a)$ is transmitted by a transmitter to a receiver, where $h(g)=a\in T$. Then, a message $\acute{r}=(\acute{g},\acute{a})$ is sent by an adversary to replace the message $r=(g,a)$, where $h(\acute{g})=\acute{a}\in T,\ \acute{g}\neq g$. That is, h is in the set $\{h\in\mathcal{H}|h(g)=a,h(\acute{g})=\acute{a}\}$, and the substitution attack is successful. The probability of substitution attack P_1 can be expressed as follows:

$$P_1=\frac{\max_{\acute{g}\neq g\in\mathcal{G};\ a,\acute{a}\in T}\left|\left\{h\in\mathcal{H}\middle|h(g)=a,h(\acute{g})=\acute{a}\right\}\right|}{\left|\left\{h\in\mathcal{H}\middle|h(g)=a\right\}\right|}. \tag{3}$$

An authentication code enables a sender to encode a message using a secret key. Then, by the same key, a designated receiver can decode the message. Flow diagrams for the encoding and decoding for authentication codes are shown in Figures 3 and 4, respectively [48].

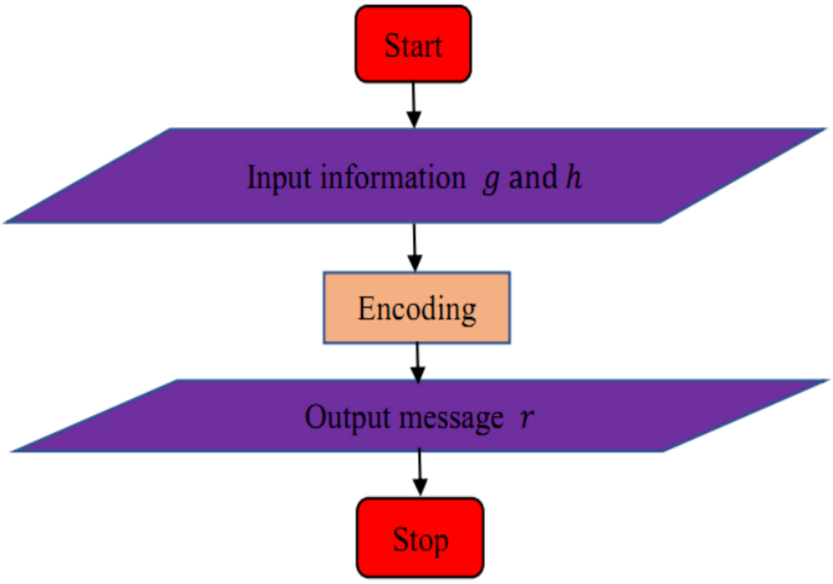


Figure 3. A flow diagram for the encoding of authentication code.

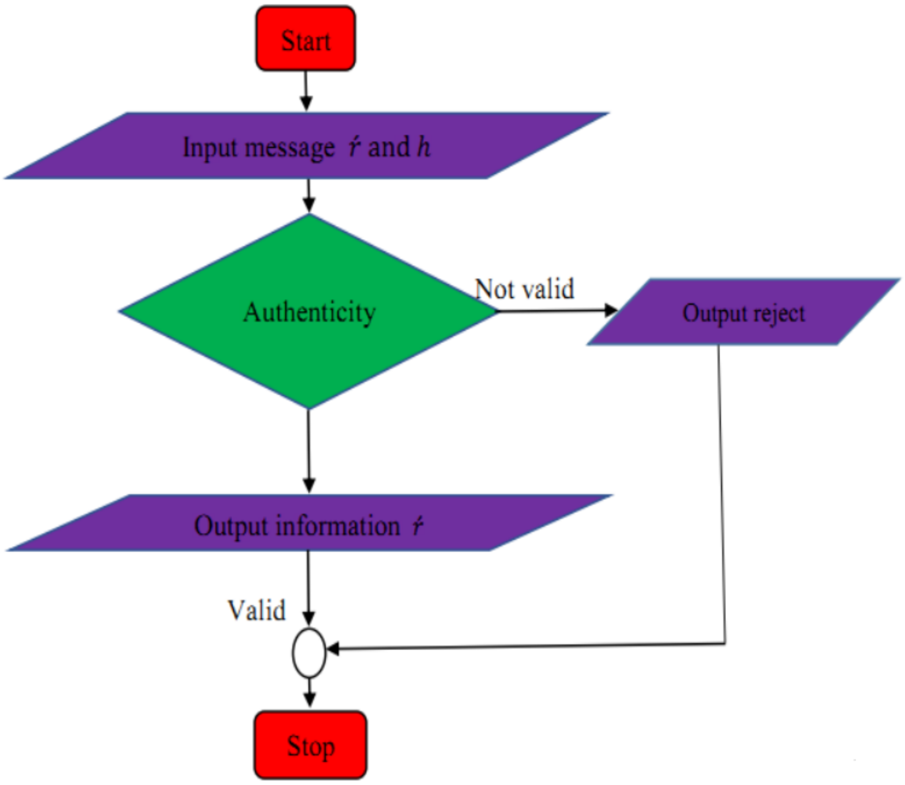

Start
Input message $\acute{r}$ and h
Authenticity
Not valid
Output reject
Output information $\acute{r}$
Valid
Stop

Figure 4. A flow diagram for the decoding of authentication code.

3. MOGS and general non-splitting Cartesian authentication codes

In this section, we will use MOGS and graph-orthogonal arrays to construct general non-splitting Cartesian authentication codes. We first construct a graph-orthogonal array by k MOGS of order n.

Then there is a mapping between the graph-orthogonal array and the message set by using the property of the graph-orthogonal array. And an encoding matrix for the Cartesian authentication code is obtained. Secondly, we get a perfect Cartesian authentication code when we obtain an encoding matrix by a graph-orthogonal array. Besides that, in this paper, some new Cartesian authentication codes can also be obtained by transforming a graph-orthogonal array in column order, or partition of a message set or changing the mapping between a message set and an authentication tag. Thus, it can be said that the used construction method has global significance from a theoretical point of view. For more illustration, see Figure 5 that shows a flow chart for the proposed algorithm in this paper. Also, a pseudo code for the proposed algorithm can be described as follows:

```
Input: Complete bipartite graph $K_{n,n}$.
Output: Authentication code.
1. Constructing $k$ mutually orthogonal edge decompositions of $K_{n,n}$ by $G$.
2. Generating $k$ mutually orthogonal $G$ squares of order $n$.
3. Constructing a $G$-orthogonal array $OA(n,k,1)$.
4. Generating an authentication code using the $OA(n,k,1)$.
5. End.
```

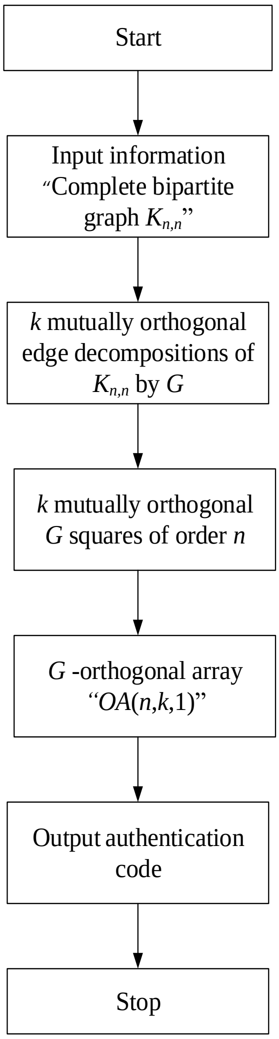

Start
Input information "Complete bipartite graph $K_{n,n}$"
k mutually orthogonal edge decompositions of $K_{n,n}$ by G
k mutually orthogonal G squares of order n
G -orthogonal array "$OA(n,k,1)$"
Output authentication code
Stop

Figure 5. Flow chart for the proposed algorithm in this paper.

Suppose we have k MOGS of order n : $M_1, M_2, \dots, M_k$. From Theorem 1, $k \leq n$. Suppose M_α^ω refer to the ωth column of M_α. Based on Proposition 1, the following graph-orthogonal array can be constructed.

$$Z = \begin{bmatrix} M_1^1 & M_2^1 & \dots & M_k^1 \\ M_1^2 & M_2^2 & \dots & M_k^2 \\ \vdots & \vdots & \vdots & \vdots \\ M_1^n & M_2^n & \dots & M_k^n \end{bmatrix}_{n^2 \times k}$$

The graph-orthogonal array Z is an orthogonal array $OA(n, k, 1)$. The matrix Z will be used as an encoding matrix for the authentication tag.

Let $Z = (A_1, A_2, \dots, A_k)$, where A_α $(1 \leq \alpha \leq k)$ is the αth column of Z. Now, n different symbols inside A_α can be represented by $A_\alpha(1), A_\alpha(2), \dots, A_\alpha(n)$. In the matrix Z, $1, 2, \dots, n$ are n different authentication tags, and the messages set $\mathcal{R}$ consists of nk ordered pairs (g, a), where $g \in \mathcal{G}$. Hence, the number of messages is $|\mathcal{R}| = nk$. Then, $\mathcal{R}$ can be divided into $\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_k$, and

$$\cup_{\alpha=1}^{k} \mathcal{R}_\alpha = \mathcal{R}, \cap_{\alpha=1}^{k} \mathcal{R}_\alpha = \emptyset, |\mathcal{R}_\alpha| = n. \tag{4}$$

The n different messages in $\mathcal{R}_\alpha$ $(1 \leq \alpha \leq k)$ can be represented by $\mathcal{R}_\alpha(1), \mathcal{R}_\alpha(2), \dots, \mathcal{R}_\alpha(n)$ respectively. Define the mapping

$$\psi_i : A_\alpha \mapsto \mathcal{R}_\alpha$$

$$A_\alpha(\sigma) \to \mathcal{R}_\alpha(\sigma),\ 1 \leq \alpha \leq k, 1 \leq \sigma \leq n. \tag{5}$$

Therefore, $(Z, \mathcal{R}, (\psi_1, \psi_2, \dots, \psi_k))$ is a non-splitting Cartesian authentication code if the probability distribution of encoding rules and sources is uniform.

Example 4. *We have three mutually orthogonal* $(P_4 \cup 2P_2)$*-squares* M_1, M_2*, and* M_3 *which are defined as follows:*

$$M_1 = \begin{bmatrix} 5 & 5 & 2 & 4 & 1 \\ 2 & 1 & 1 & 3 & 5 \\ 1 & 3 & 2 & 2 & 4 \\ 5 & 2 & 4 & 3 & 3 \\ 4 & 1 & 3 & 5 & 4 \end{bmatrix} M_2 = \begin{bmatrix} 5 & 2 & 1 & 5 & 4 \\ 5 & 1 & 3 & 2 & 1 \\ 2 & 1 & 2 & 4 & 3 \\ 4 & 3 & 2 & 3 & 5 \\ 1 & 5 & 4 & 3 & 4 \end{bmatrix} M_3 = \begin{bmatrix} 5 & 1 & 4 & 2 & 5 \\ 1 & 1 & 2 & 5 & 3 \\ 4 & 2 & 2 & 3 & 1 \\ 2 & 5 & 3 & 3 & 4 \\ 5 & 3 & 1 & 4 & 4 \end{bmatrix}$$

Hence,

$$Z=\begin{bmatrix} M_1^1 & M_2^1 & M_3^1 \\ M_1^2 & M_2^2 & M_3^2 \\ M_1^3 & M_2^3 & M_3^3 \\ M_1^4 & M_2^4 & M_3^4 \\ M_1^5 & M_2^5 & M_3^5 \end{bmatrix}_{25\times 3}=\begin{bmatrix} 5 & 5 & 5 \\ 2 & 5 & 1 \\ 1 & 2 & 4 \\ 5 & 4 & 2 \\ 4 & 1 & 5 \\ 5 & 2 & 1 \\ 1 & 1 & 1 \\ 3 & 1 & 2 \\ 2 & 3 & 5 \\ 1 & 5 & 3 \\ 2 & 1 & 4 \\ 1 & 3 & 2 \\ 2 & 2 & 2 \\ 4 & 2 & 3 \\ 3 & 4 & 1 \\ 4 & 5 & 2 \\ 3 & 2 & 5 \\ 2 & 4 & 3 \\ 3 & 3 & 3 \\ 5 & 3 & 4 \\ 1 & 4 & 5 \\ 5 & 1 & 3 \\ 4 & 3 & 1 \\ 3 & 5 & 4 \\ 4 & 4 & 4 \end{bmatrix}$$

It is clear that Z *is a* $(P_4 \cup 2P_2)$*-orthogonal array* $(P_4 \cup 2P_2)$*-*$OA(5,3,1)$*. Let* $Z=(A_1,A_2,A_3)$*, where* A_α $(1 \le \alpha \le 3)$ *is the* α*th column of* Z*. Now,* 5 *different symbols inside* A_α *can be represented by* $A_\alpha(1), A_\alpha(2), \dots, A_\alpha(5)$*. In the matrix* Z*, symbols* $1,2,\dots,5$ *are* 5 *different authentication tags, and the messages set* $\mathcal{R}$ *consists of* 15 *ordered pairs* (g,a)*, where* $g \in \mathcal{G}$*. Hence, the number of messages is* $|\mathcal{R}|=15$*. Then,* $\mathcal{R}$ *can be divided into* $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$*, and*

$$\cup_{\alpha=1}^{3}\mathcal{R}_\alpha=\mathcal{R}\,,\cap_{\alpha=1}^{3}\mathcal{R}_\alpha=\emptyset, |\mathcal{R}_\alpha|=5. \tag{6}$$

The 5 *different messages in* $\mathcal{R}_\alpha(1 \le \alpha \le 3)$ *can be represented by* $\mathcal{R}_\alpha(1), \mathcal{R}_\alpha(2), \dots, \mathcal{R}_\alpha(5)$ *respectively. Define the mapping*

$$\psi_\alpha : A_\alpha \to \mathcal{R}_\alpha$$

$$A_\alpha(\sigma) \mapsto \mathcal{R}_\alpha(\sigma),\ 1 \le \alpha \le 3, 1 \le \sigma \le 5. \tag{7}$$

Therefore, $(Z, \mathcal{R}, (\psi_1, \psi_2, \psi_3))$ *is a non-splitting Cartesian authentication code if the probability distribution of encoding rules and sources is uniform.*

For more illustration, let the set of source states be $\mathcal{G}=\{i,j,k\}$*, then the set of encoded messages*

$$\mathcal{R}=\{(g,a)|g \in \mathcal{G}, a \in \{1,2,3,4,5\}\},$$

$$\mathcal{R}=\{(i,1),(i,2),(i,3),(i,4),(i,5),(j,1),(j,2),(j,3),(j,4),$$

$$(j,5),(k,1),(k,2),(k,3),(k,4),(k,5)\},$$

for example, if a receiver receives $(i,1)$*, then he or she can deduce that the original message is* i *because* 1 *belongs to the set of authentication tags* $\{1,2,3,4,5\}$.

Theorem 2. *The above constructed Cartesian authentication code is a non-splitting authentication code and has the following parameters* $|\mathcal{G}|=k, |\mathcal{H}|=n^2, |\mathcal{R}|=nk$. *Also,* $P_0=P_1=\frac{1}{n}$.

Proof. As shown above, the graph-orthogonal array Z is used as an encoding matrix of an authentication tag. Encoding rules are represented by rows of Z, and sources are represented by columns of Z. The graph-orthogonal array Z is an $n^2\times k$ matrix. Hence, the number of sources is k, the number of encoding rules is n^2, and the number of messages is $|\mathcal{R}|=nk$.

(i) For the impersonation attack, from the graph-orthogonal array Z, we can see that each encoding rule corresponds to k different messages. Suppose a sender uses the encoding rule h_0 to send a message to a receiver. It is known that by the encoding rule h_0, k messages can be obtained. Now, if one of these k messages is used by an adversary, then the adversary succeeds in his impersonation attack. In this code, the number of all messages is nk. Therefore, the probability of a successful impersonation attack is:

$$P_0=\frac{k}{|\mathcal{R}|}=\frac{k}{nk}=\frac{1}{n}. \tag{8}$$

(ii) For the substitution attack, suppose a message $r=(g,a)$ is sent by a sender to a receiver, because the graph-orthogonal array $OA(n,k,1)$ is used as an encoding matrix of an authentication tag, so by the superimposition of any two columns of this matrix, we conclude that every ordered pair of n^2 ordered pairs appears exactly once. Therefore, in the column of the source g, the authentication tag a appears exactly n times and corresponds to n different encoding rules, so we obtain

$$|\{h\in\mathcal{H}|h(g)=a\}|=n. \tag{9}$$

Suppose that an adversary sends a message $\acute{r}=(\acute{g},\acute{a})$ $(\acute{g}\neq g)$ to a receiver. We know from the used encoding matrix that the authentication tags a and $\acute{a}$ can only appear in one row simultaneously in the two columns of the sources g and $\acute{g}$, so we get

$$|\{h\in\mathcal{H}|h(g)=a,h(\acute{g})=\acute{a}\}|=1. \tag{10}$$

Hence

$$P_1=\frac{\max_{\acute{g}\neq g\in\mathcal{G};\,a,\acute{a}\in T}\left|\left\{h\in\mathcal{H}\middle|h(g)=a,h(\acute{g})=\acute{a}\right\}\right|}{\left|\left\{h\in\mathcal{H}\middle|h(g)=a\right\}\right|}=\frac{1}{n}. \tag{11}$$

Now, we want to prove that the constructed Cartesian authentication code, in this case, is a non-splitting authentication code. It is clear from the above construction that if we have the encoding rule h and the source g, then g and h can be mapped to only one message r, so we obtain a non-splitting authentication code.

Theorem 3. *The Cartesian authentication code* $(Z,\mathcal{R},(\psi_1,\psi_2,\dots,\psi_k))$*, which is constructed by* k *mutually orthogonal* $n\times n$ *G-squares, is a perfect Cartesian authentication code.*

Proof. For the authentication code $(Z,\mathcal{R},(\psi_1,\psi_2,\dots,\psi_k))$, let $Z_{n^2\times k}$ be an encoding matrix. The row of Z represents the encoding rule and the column of Z represents the source. An element $z_{x,y}$

is in the position (x,y) of Z. The element $z_{x,y}$ shows that the source g_y is encoded into the messages $r = z_{x,y}$ with the encoding rules h_x, where $1 \leq x \leq n^2;\ 1 \leq y \leq k.$
(i) We have

$$P(h_x) = \frac{1}{n^2}, P(g_y) = \frac{1}{k}. \tag{12}$$

(ii) The elements g_y and h_x are used to determine the element $z_{x,y}$ in the encoding matrix $Z_{n^2\times k}$. It is clear that an encoding rule can encode k sources $(g_y, 1 \leq y \leq k)$ and a source can be affected by n^2 encoding rules $(h_x, 1 \leq x \leq n^2)$, so after determining g_y, the distribution probability of h_x is

$$P(h_x|g_y) = \frac{1}{n^2}. \tag{13}$$

If h_x is determined, then the distribution probability of g_y is

$$P(g_y|h_x) = \frac{1}{k}. \tag{14}$$

Now, the distribution probability of every element $z_{x,y}$ in the encoding matrix $Z_{n^2\times k}$ can be obtained as follows:

$$P(z_{x,y}) = P(h_x, g_y) = P(g_y)P(h_x|g_y) = P(h_x)P(g_y|h_x) = \frac{1}{kn^2}. \tag{15}$$

(iii) For the encoding matrix $Z_{n^2\times k}$, the same authentication tag occurs n times in any column. Also, in each column, the same authentication tag is mapped into a message. Therefore, every message r occurs n times. We now can obtain

$$P(r) = n\,.\,P(z_{x,y}) = n\,.\frac{1}{kn^2} = \frac{1}{kn}. \tag{16}$$

(iv) We know from $Z_{n^2\times k}$ that each encoding rule corresponds to k messages. Hence, the distribution probability of the message r given an encoding rule h_x is

$$P(r|h_x) = \frac{1}{k}. \tag{17}$$

And

$$P(h_x, r) = P(h_x).P(r|h_x) = \frac{1}{n^2}.\frac{1}{k} = \frac{1}{kn^2}. \tag{18}$$

Also,

$$I(\mathcal{R};\mathcal{H}) = H(\mathcal{R}) - H(\mathcal{R}|\mathcal{H}) = H(\mathcal{R}) + H(\mathcal{H}) - H(\mathcal{R},\mathcal{H})$$

$$= \sum_{r} P(r)\log_2\frac{1}{P(r)} + \sum_{h_x} P(h_x)\log_2\frac{1}{P(h_x)} - \sum_{r,h_x} P(r,h_x)\log_2\frac{1}{P(r,h_x)}$$

$$I(\mathcal{R};\mathcal{H})= nk.\frac{1}{nk}log_2\, nk + n^2.\frac{1}{n^2}log_2\, n^2 - n^2k.\frac{1}{n^2k}log_2\, n^2k = log_2\, n. \tag{19}$$

Since $P_0 = P_1 = \frac{1}{n}$, then $\log_2 P_0 = \log_2 P_1 = -\log_2 n$.

Finally, we can deduce that $\log_2 P_0 = \log_2 P_1 = -I(\mathcal{R};\ \mathcal{H}) = -\log_2 n$. From Definition 11, the Cartesian authentication code $(Z,\mathcal{R},(\psi_1,\psi_2,\dots,\psi_k))$, which is constructed by k mutually orthogonal $n \times n$ G-squares, is a perfect Cartesian authentication code.

4. MOGS and general splitting Cartesian authentication codes

In this section, we will construct a general splitting Cartesian authentication code based on graph-orthogonal arrays which are constructed by MOGS. There is a difference in this section from the previous section because, in this section, we divide the message set twice. If some or all sources and encoding rules are determined, then this message set can correspond to multiple messages. Thus this construction has the characteristic of splitting.

Let $Z = (A_1, A_2, \dots, A_k)$, where A_α $(1 \le \alpha \le k)$ is the αth column of Z. Now, the n different symbols inside A_α can be represented by $A_\alpha(1), A_\alpha(2), \dots, A_\alpha(n)$. Here, we divide the message set $\mathcal{R}$ into $\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_k$, where the following conditions are satisfied:

$$\cup_{\alpha=1}^{k}\mathcal{R}_\alpha = \mathcal{R}\,, \cap_{\alpha=1}^{k}\mathcal{R}_\alpha = \Phi, |\mathcal{R}_\alpha| = t_\alpha n, 1 \le \alpha \le k, t_\alpha \ge 1. \tag{20}$$

It is clear that

$$|\mathcal{R}| = \sum_{\alpha=1}^{k} t_\alpha n = tn, t \ge k. \tag{21}$$

Now, we apply another division on each $\mathcal{R}_\alpha$ such that $\mathcal{R}_\alpha = \{\mathcal{R}_\alpha^1, \mathcal{R}_\alpha^2, \dots, \mathcal{R}_\alpha^n\}$ and

$$\cup_{y=1}^{n}\mathcal{R}_\alpha^y = \mathcal{R}_\alpha\,, \cap_{y=1}^{n}\mathcal{R}_\alpha^y = \emptyset, \left|\mathcal{R}_\alpha^y\right| = t_\alpha, 1 \le y \le k. \tag{22}$$

Define the mapping

$$\psi_\alpha : A_\alpha \to \mathcal{R}_\alpha$$
$$A_\alpha(y) \mapsto \mathcal{R}_\alpha^y,\ \ 1 \le \alpha \le k, 1 \le y \le n. \tag{23}$$

Therefore, $(Z,\mathcal{R},(\psi_1,\psi_2,\dots,\psi_k))$ is a splitting Cartesian authentication code if the probability distribution of encoding rules and sources is uniform.

Example 5. *We have three mutually orthogonal* $(P_4 \cup 2P_2)$*-squares* $M_1, M_2,$ *and* M_3 *which are defined in Example 4. Hence,*

$$Z = \begin{bmatrix} M_1^1 & M_2^1 & M_3^1 \\ M_1^2 & M_2^2 & M_3^2 \\ M_1^3 & M_2^3 & M_3^3 \\ M_1^4 & M_2^4 & M_3^4 \\ M_1^5 & M_2^5 & M_3^5 \end{bmatrix}_{25\times 3}$$

Let $Z = (A_1, A_2, A_3)$, *where* A_α $(1 \le \alpha \le 3)$ *is the* αth *column of* Z. *Now, the* 5 *different symbols* *inside* A_α *can be represented by* $A_\alpha(1), A_\alpha(2), \ldots, A_\alpha(5)$. *Here, we divide the message set* $\mathcal{R}$ *into* $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$, *where the following conditions are satisfied:*

$$\bigcup_{\alpha=1}^{3} \mathcal{R}_\alpha = \mathcal{R}, \bigcap_{\alpha=1}^{3} \mathcal{R}_\alpha = \emptyset, |\mathcal{R}_\alpha| = 5t_\alpha, 1 \leq \alpha \leq 3, t_\alpha \geq 1. \tag{24}$$

It is clear that

$$|\mathcal{R}| = \sum_{\alpha=1}^{3} 5t_\alpha = 5t, t \geq 3. \tag{25}$$

Now, we apply another division on each $\mathcal{R}_\alpha$ *such that* $\mathcal{R}_\alpha = \{\mathcal{R}_\alpha^1, \mathcal{R}_\alpha^2, \ldots, \mathcal{R}_\alpha^5\}$ *and*

$$\bigcup_{y=1}^{5} \mathcal{R}_\alpha^y = \mathcal{R}_\alpha, \bigcap_{y=1}^{5} \mathcal{R}_\alpha^y = \emptyset, |\mathcal{R}_\alpha^y| = t_\alpha, 1 \leq y \leq 5. \tag{26}$$

Define the mapping

$$\begin{gathered} \psi_\alpha : A_\alpha \rightarrow \mathcal{R}_\alpha \\ A_\alpha(y) \mapsto \mathcal{R}_\alpha^y, \ 1 \leq \alpha \leq 3, 1 \leq y \leq 5. \end{gathered} \tag{27}$$

Therefore, $(Z, \mathcal{R}, (\psi_1, \psi_2, \psi_3))$ *is a splitting Cartesian authentication code if the probability distribution of encoding rules and sources is uniform.*

Theorem 4. *The above constructed Cartesian authentication code is a splitting authentication code and has the following parameters* $|\mathcal{G}| = k, |\mathcal{H}| = n^2, |\mathcal{R}| = tn, \ t \geq k$. *Also,* $P_0 = P_1 = \frac{1}{n}$.

Proof. As shown above, the graph-orthogonal array Z is used as an encoding matrix of an authentication tag. Encoding rules are represented by the rows of Z, sources are represented by the columns of Z. The graph-orthogonal array Z is a $n^2 \times k$ matrix. Hence, the number of sources is k, the number of encoding rules is n^2, and the number of messages is $|\mathcal{R}| = tn, \ t \geq k$.
(i) For the impersonation attack, from the graph-orthogonal array Z, we can see that each encoding rule corresponds to t messages. This is because of the division of the messages into k parts in the beginning, where each source corresponds to $t_\alpha n$ messages, in the second division the messages are divided into the subsets $\mathcal{R}_\alpha^1, \mathcal{R}_\alpha^2, \ldots, \mathcal{R}_\alpha^n$. Therefore, for a given one source and one encoding rule, we can obtain t_α messages, where $\sum_{\alpha=1}^{k} t_\alpha = t$. And the previous is the result of the construction of one-to-one mapping of $\mathcal{R}_\alpha^y$ and each source corresponding to an authentication tag. Suppose a sender uses the encoding rule h_0 to send a message to a receiver. It is known that by the encoding rule h_0, t messages can be obtained. Now, if one of these t messages is used by an adversary, then the adversary succeeds in his impersonation attack. In this code, the number of all messages is tn. Therefore, the probability of a successful impersonation attack is:

$$P_0 = \frac{t}{|\mathcal{R}|} = \frac{t}{tn} = \frac{1}{n}. \tag{28}$$

(ii) For the substitution attack, suppose a message $r = (g, a)$ is sent by a sender to a receiver, because the graph-orthogonal array $OA(n, k, 1)$ is used as an encoding matrix of an authentication tag, so by the superimposition of any two columns of this matrix, we conclude that every ordered pair of n^2 ordered pairs appears exactly once. Therefore, in the column of the source g, the authentication tag a appears exactly n times and corresponds to n different encoding rules, so we obtain

$$|\{h \in \mathcal{H} | h(g) = a\}| = n. \tag{29}$$

Suppose that an adversary sends a message $\acute{r} = (\acute{g}, \acute{a})$ $(\acute{g} \neq g)$ to a receiver. We know from the used encoding matrix that the authentication tags a and $\acute{a}$ can only appear in one row simultaneously in the two columns of the sources g and $\acute{g}$, so we get

$$|\{h \in \mathcal{H} | h(g) = a, h(\acute{g}) = \acute{a}\}| = 1. \tag{30}$$

Hence,

$$P_1 = \frac{\max_{\acute{g} \neq g \in \mathcal{G};\, a, \acute{a} \in T} \left|\{h \in \mathcal{H} \middle| h(g) = a, h(\acute{g}) = \acute{a}\}\right|}{\left|\{h \in \mathcal{H} \middle| h(g) = a\}\right|} = \frac{1}{n}. \tag{31}$$

Now, we want to prove that the constructed Cartesian authentication code, in this case, is a splitting authentication code. It is clear from the above construction that if we have the encoding rule h and the source g, then the authentication tag corresponded to g and h is $A_\alpha(y)$. From the mapping, we have $A_\alpha(y) \mapsto \mathcal{R}_\alpha^y$, g is mapped under h into a subset $\mathcal{R}_\alpha^y$, $|\mathcal{R}_\alpha^y| = t_\alpha$ and $t_\alpha \geq 1$. Thus, there is a possibility to encode one or more messages, so the code is a splitting Cartesian authentication code.

Theorem 5. *The splitting Cartesian authentication code* $(Z, \mathcal{R}, (\psi_1, \psi_2, \dots, \psi_k))$, *which is constructed by* k *mutually orthogonal* $n \times n$ G*-squares, is a perfect Cartesian authentication code.*

Proof. For the authentication code $(Z, \mathcal{R}, (\psi_1, \psi_2, \dots, \psi_k))$, let $Z_{n^2 \times k}$ be the encoding matrix. The row of Z represents encoding rules and the column of Z represents sources. Let the source g_y be encoded by the message $r_{x,y}$ with the encoding rule h_x, and $|r_{(x,y)}| = t_y$; $r_{(x,y,m)}$ represents the mth message of message set, and $1 \leq x \leq n^2$; $1 \leq y \leq k$; m=1,2,…, t_y.
(i) We have

$$P(h_x) = \frac{1}{n^2}, P(g_y) = \frac{1}{k}. \tag{32}$$

(ii) It is clear that an encoding rule can encode k sources $(g_y, 1 \leq y \leq k)$ and a source can be affected by n^2 encoding rules $(h_x, 1 \leq x \leq n^2)$, so after determining g_y, the distribution probability of h_x is

$$P(h_x | g_y) = \frac{1}{n^2}. \tag{33}$$

If h_x is determined, then the distribution probability of g_y is

$$P(g_y | h_x) = \frac{1}{k}. \tag{34}$$

(iii) After determining h_x and g_y, the probability distribution of the message $r_{(x,y,m)}$ is

$$P(r_{(x,y,m)} | h_x, g_y) = \frac{1}{t_y}. \tag{35}$$

And

$$P(r_{(x,y,m)}, h_x|g_y) = P(r_{(x,y,m)}|h_x, g_y). P(g_y|h_x) = \frac{1}{kt_y}. \tag{36}$$

Also,

$$P(r_{(x,y,m)}|h_x) = \sum_{g_y} P\left(r_{(x,y,m)}, g_y\middle|h_x\right) = \frac{1}{kt_y}. \tag{37}$$

Now, we can obtain

$$P\left(r_{(x,y,m)}, h_x\right) = P(r_{(x,y,m)}|h_x)P(h_x) = \frac{1}{kt_y n^2}. \tag{38}$$

$$H(\mathcal{R}|\mathcal{H}) = \sum_{x=1}^{n^2} H(\mathcal{R}|h_x) = \sum_{x=1}^{n^2} \sum_{r_{(x,y,m)}} P\left(r_{(x,y,m)}, h_x\right) \log_2 \frac{1}{P\left(r_{(x,y,m)}|h_x\right)}$$

$$= n^2 \times \sum_{y=1}^{k} t_y \cdot \frac{1}{kt_y n^2} . \log_2\left(kt_y\right)$$

$$H(\mathcal{R}|\mathcal{H}) = \frac{1}{k} \sum_{y=1}^{k} log_2\left(kt_y\right). \tag{39}$$

(iv) Let the message set corresponding to the source g_y be $\mathcal{R}_y$, $\mathcal{R}_{y,v}$ is the vth message of $\mathcal{R}_y$, then and the probability of $\mathcal{R}_{y,v}$ is

$$P\left(\mathcal{R}_{y,v}\right) = \frac{1}{nkt_y}. \tag{40}$$

$$H(\mathcal{R}) = \sum_{y=1}^{k} (t_y n). P(\mathcal{R}_{y,v})\, log_2 \frac{1}{P(\mathcal{R}_{y,v})} \tag{41}$$

$$= \sum_{y=1}^{k} (t_y n). \frac{1}{nkt_y} log_2\left(nkt_y\right)$$

$$= \frac{1}{k} \sum_{y=1}^{k} log_2\left(nkt_y\right).$$

Now, we can deduce that

$$I(\mathcal{R};\mathcal{H}) = H(\mathcal{R}) - H(\mathcal{R}|\mathcal{H}) = \frac{1}{k}\sum_{y=1}^{k} log_2\left(nkt_y\right) - \frac{1}{k}\sum_{y=1}^{k} log_2\left(kt_y\right) = \frac{1}{k}\sum_{y=1}^{k} log_2\left(\frac{nkt_y}{kt_y}\right)$$

$$= log_2 n\left(\frac{1}{k}\sum_{y=1}^{k} 1\right) = log_2 n. \tag{42}$$

Since $P_0 = P_1 = \frac{1}{n}$, then $\log_2 P_0 = \log_2 P_1 = -\log_2 n$.

Finally, we can deduce that $\log_2 P_0 = \log_2 P_1 = -I(\mathcal{R};\, \mathcal{H}) = -\log_2 n$. From Definition 11, the splitting Cartesian authentication code $(Z, \mathcal{R}, (\psi_1, \psi_2, \ldots, \psi_k))$, which is constructed by k mutually orthogonal $n \times n$ G-squares, is a perfect Cartesian authentication code.

5. Optimal Cartesian authentication codes based on MOGS

In this section, we will handle a special case of MOGS which is called MOLS. If we have a set of mutually orthogonal G-squares of order n, where $G \cong nK_2$, then this set is called a set of MOLS. It is known that for any prime power n, there exist $(n-1)$ MOLS of order n[46]. Suppose we have $(n-1)$ MOLS of order n: $M_1, M_2, \ldots, M_{n-1}$. The entries in $M_\alpha (\alpha = 1,2, \ldots, n-1)$ belong to the set $\{1,2, \ldots, n\}$. Suppose M_α^ω refer to the column of M_α, $Z_0 = (1,2, \ldots, n)^T$, $Z_x = (x, x, \ldots, x)^T$ and $x = 1,2, \ldots., n$.

Theorem 6 ([47]). *A set of $(n-1)$ MOLS of order n is equivalent to an $OA(n, n+1, 1)$.*
Hence, the following graph-orthogonal array can be constructed based on Theorem 6.

$$Z = \begin{bmatrix} Z_0 & Z_1 & M_1^1 & M_2^1 & \ldots & M_{n-1}^1 \\ Z_0 & Z_2 & M_1^2 & M_2^2 & \ldots & M_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ Z_0 & Z_n & M_1^n & M_2^n & \ldots & M_{n-1}^n \end{bmatrix}_{n^2 \times (n+1)}$$

The graph-orthogonal array Z is an orthogonal array $OA(n, n+1, 1)$. The matrix Z will be used as an encoding matrix for an authentication tag.

Theorem 7. *If the non-splitting Cartesian authentication code $(Z, \mathcal{R}, (\psi_1, \psi_2, \ldots, \psi_k))$, constructed in Section 3, is constructed by $(n-1)$ MOLS of order n, that is $k = n+1$, then the code is an optimal Cartesian authentication code.*

Proof. From Theorem 2, the parameters of this authentication code are $|\mathcal{G}| = k = n+1$, $|\mathcal{H}| = n^2, |\mathcal{R}| = n(n+1)$. Also, $P_0 = P_1 = \frac{1}{n}$. Hence, the authentication code is an optimal Cartesian authentication code from Definition 10.

Theorem 8. *If the splitting Cartesian authentication code $(Z, \mathcal{R}, (\psi_1, \psi_2, \ldots, \psi_k))$, constructed in Section 4, is constructed by $(n-1)$ MOLS of order n, that is $k = n+1$, then the code is an optimal Cartesian authentication code.*

Proof. From Theorem 4, the parameters of this authentication code are $|\mathcal{G}| = k = n+1$, $|\mathcal{H}| = n^2, |\mathcal{R}| = nt = n(n+1)$. Also, $P_0 = P_1 = \frac{1}{n}$. Hence, the authentication code is an optimal Cartesian authentication code from Definition 10.

6. Authentication codes with confidentiality based on graph squares

An authentication code can be kept secret if an adversary finds a message transmitted through a channel, but this adversary cannot get any information about the source. Here, we will construct a security authentication code by using Latin squares that are considered as a special case of graph squares (G-squares) as mentioned above. The constructed authentication codes in Section 3 and Section 4 are without confidentiality. Suppose C is the orthogonal array $OA(n, kn, k)$, where C can be represented as $C = (c_{i,j})_{kn^2 \times kn}$, where $i = 1,2, \ldots, kn^2, j = 1,2, \ldots, kn$. From Section 3, the parameters of the constructed authentication code by the orthogonal array C are $|\mathcal{G}| = kn$, $|\mathcal{H}| = kn^2$, $|\mathcal{R}| = n|\mathcal{G}| = kn^2$. Then, suppose that it is possible to construct the Cartesian authentication code $(C, \mathcal{R}, (\psi_1, \psi_2, \dots, \psi_{kn}))$, where C is the encoding matrix.

Now, we will use a Latin square to convert the constructed Cartesian authentication code to an authentication code with confidentiality. Suppose that the encoding matrix for the authentication code is $D = \left(d_{i,j}\right)_{kn^2 \times kn}$, $i = 1, 2, \dots, kn^2, j = 1, 2, \dots, kn$.

We make a partitioning to D into the following blocks,

$$D = \begin{bmatrix} D_{1,1} & D_{1,2} & \cdots & D_{1,kn} \\ D_{2,1} & D_{2,2} & \cdots & D_{2,kn} \\ \vdots & \vdots & \vdots & \vdots \\ D_{kn,1} & D_{kn,2} & \cdots & D_{kn,kn} \end{bmatrix}; \ D_{x,y} = \begin{bmatrix} d_{n(x-1)+1,y} \\ d_{n(x-1)+2,y} \\ \vdots \\ d_{n(x-1)+n,y} \end{bmatrix}; \ x = y = 1, 2, \dots, kn.$$

Suppose that we have any Latin square S of order kn;

$$S = \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,kn} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,kn} \\ \vdots & \vdots & \vdots & \vdots \\ s_{kn,1} & s_{kn,2} & \cdots & s_{kn,kn} \end{bmatrix}; \ s_{x,y} \in \{1, 2, \dots, kn\}, \ x = y = 1, 2, \dots, kn.$$

For the element in row x and column y of the matrix D, the second subscript is replaced with the element in row x and column $s_{x,y}$ of the Latin square S. Hence, for the matrix D, the element in row x and column y is put in the position in row x and column $s_{x,y}$, so the subblocks in rows of D are rearranged and we get a matrix $\acute{D}$. Finally, we obtain an authentication code with confidentiality $(\acute{D}, C, \mathcal{R}, D, S, (\psi_1, \psi_2, \dots, \psi_{kn}))$, where $\acute{D}$ is its encoding matrix. It seems that the strength of the proposal is the huge growth in the number of Latin squares of a given order.

Theorem 9. *The authentication code* $(\acute{D}, C, \mathcal{R}, D, S, (\psi_1, \psi_2, \dots, \psi_{kn}))$ *is a secure authentication code or with confidentiality.*

Proof. It is clear that

$$P(g) = \frac{1}{|\mathcal{G}|} = \frac{1}{kn}. \tag{43}$$

Each column in $\acute{D}$ contains all messages, and each message occurs precisely once in this column. Hence, the conditional distribution probability of source under the message is

$$P(g|r) = \frac{1}{kn}. \tag{44}$$

Hence,

$$P(g) = P(g|r) = \frac{1}{kn}. \tag{45}$$

Consequently, the authentication code $(\acute{D}, C, \mathcal{R}, D, S, (\psi_1, \psi_2, \dots, \psi_{kn}))$ is secure.

Example 6. *Let the matrices* $C, D,$ *and* S *be represented by*

$$C=\begin{bmatrix}1&6&11&16\\2&5&12&15\\3&8&9&14\\4&7&10&13\\1&7&12&14\\2&8&11&13\\3&5&10&16\\4&6&9&15\\1&8&10&15\\2&7&9&16\\3&5&12&13\\4&6&11&14\\1&5&9&13\\2&6&10&14\\3&7&11&15\\4&8&12&16\end{bmatrix},\ D=C=\begin{bmatrix}D_{1,1}&D_{1,2}&D_{1,3}&D_{1,4}\\D_{2,1}&D_{2,2}&D_{2,3}&D_{2,4}\\D_{3,1}&D_{3,2}&D_{3,3}&D_{3,4}\\D_{4,1}&D_{4,2}&D_{4,3}&D_{4,4}\end{bmatrix},\ S=\begin{bmatrix}1&2&3&4\\2&3&4&1\\3&4&1&2\\4&1&2&3\end{bmatrix}$$

Then, the matrix $\acute{D}$ *can be represented as follows:*

$$\acute{D}=\begin{bmatrix}1&6&11&16\\2&5&12&15\\3&8&9&14\\4&7&10&13\\14&1&7&12\\13&2&8&10\\16&3&5&11\\15&4&6&9\\10&15&1&8\\9&16&2&7\\12&13&3&5\\11&14&4&6\\5&9&13&1\\6&10&14&2\\7&11&15&3\\8&12&16&4\end{bmatrix}.$$

For more illustration, if we choose the following Latin square

$$S=\begin{bmatrix}1&2&3&4\\2&1&4&3\\3&4&1&2\\4&3&2&3\end{bmatrix}$$

Then

$$\acute{D}=\begin{bmatrix}1&6&11&16\\2&5&12&15\\3&8&9&14\\4&7&10&13\\7&1&14&12\\8&2&13&11\\5&3&16&10\\6&4&15&9\\10&15&1&8\\9&16&2&7\\12&13&3&5\\11&14&4&6\\13&9&5&1\\14&10&6&2\\15&11&7&3\\16&12&8&4\end{bmatrix}.$$

It is clear that $|\mathcal{G}|=4,\ |\mathcal{H}|=16,\ |\mathcal{R}|=16,$ *and* $P(g)=P(g|r)=\frac{1}{4}.$

7. Conclusions

This paper mainly studies how to use graph-orthogonal arrays and MOGS to construct non-splitting Cartesian authentication codes and splitting Cartesian authentication codes where the probability distribution of encoding rules and sources is uniform. We have calculated the probability of successful impersonation attack and substitution attack of the constructed non-splitting and splitting Cartesian authentication codes and have analyzed their performance. These codes are proved to be perfect and optimal Cartesian authentication codes with good performance. Our goal in this paper has been to develop message authentication schemes to provide a guarantee of integrity: that is, the assurance that a message was sent by its purported sender. By the way, this paper is the first one that deals with the construction of authentication codes by MOGS. In future work, we will try to study the properties of the authentication codes constructed by MOGS as the *G*-squares are different according to graph *G*. The graph *G* may be a path graph, cycle graph, tree graph, and so forth.

Acknowledgments

This Research was supported by Taif University Researchers Supporting Project Number (TURSP-2020/217), Taif University, Taif, Saudi Arabia.

Conflict of interest

The authors declare no conflict of interest.

References

1. C. Shannon, A mathematical theory of communication, *Bell System Technical Journal*, **27** (1948), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x
2. E. Gilbert, F. MacWilliams, N. Sloane, Codes which detect deception, *Bell System Technical Journal*, **53** (1974), 405–424. https://doi.org/10.1002/j.1538-7305.1974.tb02751.x
3. G. Simmons, A game theory model of digital message authentication, *Congressus Neumerantium*, **34** (1982), 413–424.
4. G. Simmons, Message authentication: a game on hypergraphs, *Congressus Neumerantium*, **45** (1984), 161–192.
5. G. Simmons, Authentication theory / coding theory, In: *Lecture Notes in Computer Science*, Berlin: Springer, 1985, 411–431. https://doi.org/10.1007/3-540-39568-7_32
6. G. Simmons, A survey of information authentication. *Proceedings of the IEEE*, 1992, 379–419. https://doi.org/10.1109/5.4445
7. T. Sze, S. Chanson, C. Ding, T. Helleseth, M. Parker, Logarithm Cartesian authentication codes, *Inform. Comput.*, **184** (2003), 93–108. https://doi.org/10.1016/S0890-5401(03)00053-1
8. H. Wang, C. Xing, R. Safavi-Naini, Linear authentication codes: bounds and constructions, *IEEE T. Inform. Theory*, **49 (**2003), 866–872. https://doi.org/10.1109/TIT.2003.809567
9. R. Feng, L. Hu, J. Kwak, Authentication codes and bipartite graph, *Eur. J. Combin.*, **29** (2008), 1473–1482. https://doi.org/10.1016/j.ejc.2007.06.013
10. S. Chen, D. Zhao, Two constructions of optimal Cartesian authentication codes from unitary geometry over finite fields, *Acta Math. Appl. Sin. Engl. Ser.*, **29** (2013), 829–836. https://doi.org/10.1007/s10255-013-0259-6
11. R. Feng, Another construction of Cartesian authentication codes from geometry of classical groups, *Northeast Math. J.*, **15** (1999), 103–114.
12. R. Feng, Z. Wan, A construction of Cartesian authentication codes from geometry of classical groups, *J. Comb. Inf. Syst. Sci.*, **20** (1995), 197–210.
13. S. Gao, Two constructions of Cartesian authentication codes from unitary geometry, *Appl. Math. J. Chinese Univ. Ser. A.*, **11** (1996), 343–354.
14. Y. Gao, Z. Zou, Two new constructions of Cartesian authentication codes from symplectic geometry, *Appl. Math.*, **10** (1995), 345–356. https://doi.org/10.1007/BF02662876
15. H. You, Y. Gao, Some new constructions of Cartesian authentication codes from symplectic geometry, *J. Syst. Sci. Complex.*, **7** (1994), 317–327.
16. Z. Li, S. Gao, Z. Wang, B. Thuraisingham, W. Wu, A construction of Cartesian authentication code from orthogonal spaces over a finite field of odd characteristic, *Discret. Math. Algorit.*, **1** (2009), 105–114. https://doi.org/10.1142/S1793830909000075
17. J. Ma, J. Guo, F. Li, K. Wang, A generalization of the formulas for intersection numbers of dual polar association schemes and their applications, *Linear Algebra Appl.*, **434** (2011), 1272–1284. https://doi.org/10.1016/j.laa.2010.11.007
18. L. Casse, K. Martin, P. Wild, Bounds and characterizations of authentication / secrecy schemes, *Des. Codes Cryptogr.*, **13** (1998), 107–129. https://doi.org/10.1023/A:1008270111149
19. C. Ding, A. Salomaa, P. Solé, X. Tian, Three constructions of authentication/secrecy codes, *J. Pure Appl. Algebra*, **196** (2005), 149–168. https://doi.org/10.1016/j.jpaa.2004.08.008

20. G. Ge, L. Zhu, Authentication perpendicular arrays APA1 (2, 5, v), *J. Comb. Des.*, **4** (1996), 365–375. https://doi.org/10.1002/(SICI)1520-6610(1996)4:5%3C365::AID-JCD5%3E3.0.CO;2-D
21. G. Ge, L. Zhu, Authentication perpendicular arrays APA1 (2, 7, v), *J. Comb. Des.*, **5** (1997), 111–124. https://doi.org/10.1002/(SICI)1520-6610(1997)5:2%3C111::AID-JCD3%3E3.0.CO;2-I
22. D. Stinson, Some constructions and bounds for authentication codes, *J. Cryptology*, **1** (1988), 37–51. https://doi.org/10.1007/BF00206324
23. D. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, In: *Lecture Notes in Computer Science*, Berlin: Springer, 1988, 119–127. https://doi.org/10.1007/3-540-48184-2_31
24. D. Stinson, The combinatorics of authentication and secrecy codes, *J. Cryptology*, **2** (1990), 23–49. https://doi.org/10.1007/BF02252868
25. D. Stinson, L. Teirlink, A construction for authentication/secrecy codes from 3-homogeneous permutation groups, *Eur. J. Combin.*, **11** (1990), 73–79. https://doi.org/10.1016/S0195-6698(13)80058-3
26. T. Van Tran, On the construction of authentication and secrecy codes, *Des. Codes Crypt.*, **5** (1995), 269–280. https://doi.org/10.1007/BF01388389
27. M. De Soete, New bounds and constructions for authentication/secrecy codes with splitting, *J. Cryptology*, **3** (1991), 173–186. https://doi.org/10.1007/BF00196910
28. W. Ogata, K. Kurowawa, D. Stinson, H. Saido, New combinatorial designs and their applications to authentication codes and secret sharing schemes, *Discrete Math.*, **279** (2004), 383–405. https://doi.org/10.1016/S0012-365X(03)00283-8
29. J. Massey, Cryptography–a selective survey, In: *Digital Communications*, North-Holland: Elsevier Science Publisher, 1985, 4–11.
30. R. Rees, D. Stinson, Combinatorial characterizations of authentication codes II, *Des. Codes Crypt.*, **7** (1996), 239–259. https://doi.org/10.1023/A:1018094824862
31. T. Bolton, T. Dargahi, S. Belguith, M. Al-Rakhami, A. Sodhro, On the security and privacy challenges of virtual assistants, *Sensors*, **21** (2021), 2312. https://doi.org/10.3390/s21072312
32. C. Nykvist, M. Larsson, A. Sodhro, A. Gurtov, A lightweight portable intrusion detection communication system for auditing applications, *Int. J. Commun. Syst.*, **33** (2020), 4327. https://doi.org/10.1002/dac.4327
33. S. Bakhtiari, R. Safavi-Naini, J. Pieprzyk, A message authentication code based on latin squares, In: *Lecture Notes in Computer Science*, Berlin: Springer, 1997. https://doi.org/10.1007/BFb0027926
34. D. Stinson, Combinatorial characterizations of authentication codes, *Des. Codes Crypt.*, **2** (1992), 175–187. https://doi.org/10.1007/BF00124896
35. S. Pal, D. Bhardwaj, R. Kumar, V. Bhatia, A new cryptographic Hash function based on Latin squares and non-linear transformations, *Proceeding of 2009 IEEE International Advance Computing Conference*, 2009, 862–867. https://doi.org/10.1109/IADCC.2009.4809128
36. S. Golomb, E. Posner, Rook domains, Latin squares, affine planes, and error-distributing codes, *IEEE T. Inform. Theory*, **10** (1964), 196–208. https://doi.org/10.1109/TIT.1964.1053680
37. R. El-Shanawany, A. El-Mesady, Mutually orthogonal graph squares for disjoint union of stars, *Ars Combinatoria*, **149** (2020), 83–91.
38. R. Sampathkumar, S. Srinivasan, Mutually orthogonal graph squares, *J. Comb. Des.*, **17** (2009), 369–373. https://doi.org/10.1002/jcd.20216

39. R. El-Shanawany, A. El-Mesady, On mutually orthogonal certain graph squares, *Online J. Anal. Comb*, **14** (2020), 1–20.
40. M. Higazy, A. El-Mesady, M. Mohamed, On graph-orthogonal arrays by mutually orthogonal graph squares, *Symmetry*, **12** (2020), 1895. https://doi.org/10.3390/sym12111895
41. A. El-Mesady, S. Shaaban, Generalization of MacNeish's Kronecker product theorem of mutually orthogonal, *AKCE Int. J. Graphs Co.*, **18** (2021), 117–122. https://doi.org/10.1080/09728600.2021.1966349
42. R. El-Shanawany, On mutually orthogonal graph-path squares, *Open Journal of Discrete Mathematics*, **6** (2016), 7–12. https://doi.org/10.4236/ojdm.2016.61002
43. R. El-Shanawany, A. El-Mesady, S. Shaaban, Mutually orthogonal graph squares for disjoint union of paths, *Applied Mathematical Sciences*, **12** (2018), 303–310. https://doi.org/10.12988/ams.2018.8112
44. R. El-Shanawany, On mutually orthogonal disjoint copies of graph squares, *Note Mat.*, **36** (2016), 89–98.
45. M. Higazy, λ-Mutually orthogonal covers of complete bipartite graphs, *Adv. Appl. Discret. Mat.*, **17** (2016), 151–167. https://doi.org/10.17654/DM017020151
46. Z. Wan, *Design theory*. Beijing: Higher Education Press, 2009.
47. J. Liu, Z. Xu, On the Theory and Construction of CARTESIAN Authentication Codes, *J. Electron. Inf. Techn.*, **30** (2008), 93–95. https://doi.org/10.3724/SP.J.1146.2006.00838
48. W. Jirakitpuwapat, P. Chaipunya, P. Kumam, S. Dhompongsa, P. Thounthong, New methods of construction of Cartesian authentication codes from geometries over finite commutative rings, *J. Math. Cryptol.*, **12** (2018), 119–136. https://doi.org/10.1515/jmc-2017-0057