Latin squares associated to principal autotopisms of long cycles. Application in Cryptography

Raúl M. Falcón Ganfornina

Abstract

Fixed a principal isotopism $\Theta = (\alpha, \beta, \epsilon) \in S_n^3$, where S_n is the symmetric group of the set $N = \{0, 1, ..., n-1\}$, we are going to study in this paper the number $\Delta(\Theta)$ of Latin squares which have Θ as a principal autotopism. As an application in Cryptography, we use it in the construction of secret sharing schemes based in $\mathfrak{F}$-critical sets of Latin squares.

Keyword: Latin square, Autotopism group, Critical set, Secret sharing scheme.

1 Introduction

A *quasigroup* [1] is a nonempty set G endowed with a product $\cdot$, such that if any two of the three symbols a, b, c in the equation $a \cdot b = c$ are given as elements of G, the third is uniquely determined as an element of G. It is equivalent to say that G is endowed with left / and right \ division. Two quasigroups $(G, \cdot)$ and $(H, \circ)$ are *isotopic* [4] if there are three bijections α, β, γ from H to G, such that:

$$\gamma(a \circ b) = \alpha(a) \cdot \beta(b), \text{ for all } a, b \in H.$$

The triple $\Theta = (\alpha, \beta, \gamma)$ is called an *isotopism* from $(G, \cdot)$ to $(H, \circ)$. If $G = H$ and $\alpha = \beta = \gamma$, the isotopism is indeed an *isomorphism*. If $\gamma = \epsilon$, the identity map on G, Θ is called a *principal isotopism*. If $G = H$ and $\cdot \equiv \circ$, Θ is called an *autotopism*. Finally, $\Theta = (\epsilon, \epsilon, \epsilon)$ is called the *trivial autotopism*.

If we consider the multiplication table of a quasigroup, we obtain a Latin square. A *Latin square*, L, of order n, is a $n \times n$ array with elements chosen from a set of n symbols $N = \{x_1, ..., x_n\}$, such that each symbol occurs precisely once in each row and each column. A *Latin subrectangle* of L is a rectangular subarray R of L such that exactly the same symbols occur in each row of R. The set of Latin squares of order n is denoted by $LS(n)$. A *partial Latin square*, P, of order n, is a $n \times n$ array with elements chosen from a set of n symbols, such that each symbol occurs at most once in each row and in each column. The set of partial Latin squares of order n is denoted as $PLS(n)$. It is said that a fixed $P \in PLS(n)$ can be *uniquely completed* to a Latin square $L \in LS(n)$ if L is the unique Latin square such that $P \subseteq L$ and it is denoted $P \in UC(L)$. If besides any proper subset of P can be completed to two distinct Latin squares it is said that P is a *critical set* of L and it is denoted $P \in CS(L)$. A critical set of L is said *minimal* if it has the smallest size of all possible critical sets of L. Critical sets were introduced in the last 70's of the past century [15], [6]. Applications of them in Cryptography were obtained by Seberry [18] in 1990. Later on, it has been proved that critical sets allow to construct secret sharing schemes [5]. In [10] it can be observed some of these applications to Cryptography.

The cardinality of $LS(n)$ for all $n \in \mathbb{N}$, $N(n,n)$, is still an open problem, although it is known that this cardinality grows exponentially. Studies of $N(n,n)$ with $n \leq 11$ can be found in [20], [2] or [14]. We will consider from now on $N = \{0, 1, ..., n-1\}$. So, if $L = (l_{ij})$, the *orthogonal array representation of* L is the set of n^2 triples $\{(i, j, l_{ij}) : 0 \leq i, j \leq n-1\}$. An *isotopism* of a Latin square L is a triple $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n = S_n \times S_n \times S_n$, where S_n is the symmetric group on N and so, α, β and γ are respectively, permutations of rows, columns and symbols of L. The resulting square L^Θ is also a Latin square and it is said to be *isotopic* to L. In particular, if $L = (l_{ij})$, then $L^\Theta = \{(i, j, \gamma^{-1}\left(l_{\alpha(i)\beta(j)}\right) : 0 \leq i, j \leq n-1\}$. The set of all Latin squares isotopic to L is called its *isotopy class*. An isotopism which maps L to itself is an *autotopism*. The stabilizer subgroup of L in $\mathcal{I}_n$ is its *autotopism group*, $\mathcal{U}(L) = \{\Theta \in \mathcal{I}_n : L^\Theta = L\}$. Given $P \in PLS(n)$, contained in L, and $\mathfrak{F} \subseteq \mathcal{U}(L)$, it is defined the *extended autotopy* $P^{\mathfrak{F}} = \bigcup_{\Theta \in \mathfrak{F}} P^\Theta \in PLS(n)$.

Cardinalities of isotopy classes and autotopism groups have been already studied, for example in [17], [7] or, more recently, in [13] and [14]. In these two last papers, authors have used autotopism group sizes (computed by B.D. McKay's *nauty* [11]) to give counts of Latin squares of order up to 11. Indeed, as a first step to obtain it, they have studied the possible autotopisms of a given Latin square. To do it, they have defined the *cycle structure of a permutation* γ as the sequence $(n_1, n_2, ...)$, where n_i is the number of cycles of length i in γ. So, they have proved the following:

Theorem 1.1. (McKay, Meynert and Myrvold [13]) *Let $L \in LS(n)$. Every non-trivial $\Theta = (\alpha, \beta, \gamma) \in \mathcal{U}(L)$ verifies one of the following assertions:*

a) α, β, γ have the same cycle structure with at least one and at most $\lfloor n/2 \rfloor$ fixed points,

b) One of α, β, γ has at least one fixed point and the other two have the same cycle structure without fixed points,

c) None of α, β, γ has fixed points. □

Also in these papers, they have studied the reciprocal question. That is, given an isotopism $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$, how many Latin squares there exist such that Θ is an autotopism of all of them. However, they are not interested in the number of Latin squares but in the number of isotopy classes. Besides, they only study [13] some concrete cases of autotopisms:

a) For some prime p, α, β and γ have order p with the same number m of fixed points, where $1 \leq m \leq \lfloor n/2 \rfloor$.

b) For some prime p dividing n, α and β have order p and no fixed points, and γ has order 1 or p. If $p = 2$ and $n \equiv 2$ $(mod\ 4)$, γ has at least two fixed points.

To obtain the previous number, they use computer programs which incorporate two methods of approach to generation: the orderly approach method [9], [16] and the canonical construction path method [12]. In particular, this last one allows to construct a Latin square one *row block* at a time, where a row block consists of the rows which correspond to a cycle of α.

Nevertheless, a study of the number of Latin squares associated to any autotopism is even necessary. Indeed, this question will allow to study better the problem of the smallest size of $\mathfrak{F}$-critical sets [8]: Fixed $L \in LS(n)$, $P \in PLS(n)$ contained in L and $\mathfrak{F} \subseteq \mathcal{U}(L)$, it is defined $\mathfrak{F}(P) = P^{<\mathfrak{F}>}$, where $< \mathfrak{F} >$ is the subgroup of $\mathcal{U}(L)$ generated by $\mathfrak{F}$. Then, P is *uniquely* $\mathfrak{F}$*-completable to* L, which is denoted as $P \in UC_{\mathfrak{F}}(L)$, if $\mathfrak{F}(P) \in UC(L)$. Furthermore, P is a $\mathfrak{F}$*-critical set* if $P \in UC_{\mathfrak{F}}(L)$ and $Q \notin UC_{\mathfrak{F}}(L)$ for all $Q \subset P$. Analogous to critical sets, it is expected that $\mathfrak{F}$-critical sets will have applications in Cryptography, specially as secret sharing schemes.

In this paper we will start this study with a particular case of autotopisms, the principal ones, which have been partially studied in [13], although only to get the number of isotopy class. The paper is structured as follows. In the next section, fixed a principal isotopism $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$, we will study the number $\Delta(\Theta)$ of Latin squares which have Θ as a principal autotopism. First, we will prove that α and β must have the same cycle structure with all their cycles of the same length and without fixed points. Then, we will study the cases in which this length is $\frac{n}{k}$, with $k \in \{1, 2, 3, 4\}$. We will use the canonical construction path to generate the associated Latin squares. So, in the general case, we will see that:

$$\Delta(\Theta) = n! \cdot \left(\frac{n}{k}!\right)^{k(k-1)} \cdot \Omega(\Theta),$$

where $\Omega(\Theta)$ is the number of different ways in which we can choose a determined set of row blocks. Finally, the paper finishes in the third section with a study in Cryptography about the possible use of a set $\mathfrak{F}$ of autotopisms of a Latin square L as shares of a secret sharing scheme. To get it, we will keep in mind the concept of $\mathfrak{F}$-critical set of L.

2 Principal autotopisms of Latin squares

Fixed $n \in \mathbb{N}$ and $\Theta \in \mathcal{I}_n$, we will denote by $\Delta(\Theta)$ the number of Latin squares of order n such that Θ is an autotopism of all of them, and by $LS(\Theta)$ the set of such Latin squares. That is, $\Delta(\Theta) = |LS(\Theta)|$ and $L \in LS(\Theta)$ if and only if $\Theta \in \mathcal{U}(L)$. In this paper, we are interested in the value of $\Delta(\Theta)$ if Θ is a principal isotopism, that is, if $\Theta = (\alpha, \beta, \epsilon)$, where ϵ is the identity map in $N = \{0, 1, ..., n-1\}$. It is clear that $(\epsilon, \epsilon, \epsilon) \in \mathcal{U}(L)$ for all $L \in LS(n)$. So, $\Delta((\epsilon, \epsilon, \epsilon)) = N(n, n)$, the number of Latin squares of orden n. Therefore, we must study when Θ is a non-trivial principal autotopism of a Latin square.

Let us see a result which allows to fix the structure of Θ in the more general case in which ϵ is one of the permutations of Θ:

Proposition 2.1. *Let $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be a non-trivial isotopism. If one of the permutations α, β or γ is equal to ϵ, then $\Delta(\Theta) > 0$ only if the other two permutations have the same cycle structure with all their cycles of the same length and without fixed points.*

Proof.

We are in the case (b) of Theorem 1.1. So, if the other two permutations have not the same cycle structure or have fixed points, then $\Delta(\Theta) = 0$. Let us study the different possibilities:

a) If $\alpha = \epsilon$, let us consider that β and γ have the same cycle structure without fixed points. Let us take $b, c \in N = \{0, 1, ..., n-1\}$ such that b appears in a cycle of length λ_β of β, $(bx_2x_3...x_{\lambda_\beta})$, and c appears in a cycle of length λ_γ of γ, $(cy_2y_3...y_{\lambda_\gamma})$. We can suppose that $\lambda_\beta > \lambda_\gamma$. If $L = (l_{ij}) \in LS(n)$ is such that $\Theta \in \mathcal{U}(L)$, there must exist $a \in N$ such that $l_{ab} = c$. So, $l_{ab} = c = l_{ax_{\lambda_\gamma+1}}$, which is a contradiction with being $L \in LS(n)$.

b) If $\beta = \epsilon$, we reason analogously to (a).

c) If $\gamma = \epsilon$, let us consider that α and β have the same cycle structure without fixed points. Let us take $a, b \in N$ such that a appears in a cycle of length λ_α of α, $(ax_2x_3...x_{\lambda_\alpha})$, and b appears in a cycle of length λ_β of β, $(by_2y_3...y_{\lambda_\beta})$. We can suppose that $\lambda_\alpha < \lambda_\beta$. If $L = (l_{ij}) \in LS(n)$ is such that $\Theta \in \mathcal{U}(L)$, then $l_{ab} = l_{ay_{\lambda_\alpha+1}}$, which is a contradiction with being $L \in LS(n)$.

□

Keeping in mind the previous proposition, we will be interested from now on in principal autotopisms $\Theta = (\alpha, \beta, \epsilon)$, such that α and β have the same cycle structure with all their cycles of the same length and without fixed points. Given such a Θ, we are interested in the exact value of $\Delta(\Theta)$. To see it, we start with cycles of length n and later on, we will decrease this length.

2.1 Cycles of length n

If α and β are both cycles of length n, we obtain the following result:

Proposition 2.2. *Let $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$ be such that α and β are both cycles of length n. Then, $\Delta(\Theta) = n!$.*

Proof.

Let $\alpha = (a_0a_1...a_{n-1})$ and $\beta = (b_0b_1...b_{n-1})$ be two cycles of length n of N. We can obtain a Latin square $L = (l_{ij})$ such that $\Theta \in \mathcal{U}(L)$. To do it, for all $i \in N$, let us take $l_{0i} \in N$, such that $l_{0j} \neq l_{0k}$ for all $j \neq k$. We can supppose that $a_0 = 0$. Now, fixed $i \in N$, we take $t_i \in N$ such that $b_{t_i} = i$. So, $l_{a_jb_{t_i+j \ (mod \ n)}} = l_{0i}$, for all $j \in N$. In this way, we can define the Latin square L. Furthermore, by swapping the elements l_{0i} in N, we can obtain $n!$ distinct Latin squares and it cannot exist other one such that has Θ as an autotopism.

□

Let us see an example:

Example 2.3. Let us consider $n = 3$ and $N = \{0, 1, 2\}$. There are 36 elements of $\mathcal{I}_3$ with the form $(\alpha, \beta, \epsilon)$. However, from Proposition 2.1, only five of them are autotopisms of some Latin square of order 3. They are:

$$\Theta_1 = (\epsilon, \epsilon, \epsilon), \quad \Theta_2 = ((012), (012), \epsilon), \quad \Theta_3 = ((012), (021), \epsilon)$$
$$\Theta_4 = ((021), (012), \epsilon), \quad \Theta_5 = ((021), (021), \epsilon)$$

Besides, it can be seen that:

$$LS(\Theta_1) = LS(3)$$
$$LS(\Theta_2) = LS(\Theta_5) = \left\{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \in LS(3) : a, b, c \in N \right\}$$
$$LS(\Theta_3) = LS(\Theta_4) = \left\{ \begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix} \in LS(3) : a, b, c \in N \right\}$$

So, $\Delta(\Theta_1) = 12$ and $\Delta(\Theta_i) = 6$, if $i \in \{2, 3, 4, 5\}$. Let us observe that $LS(\Theta_2) \cap LS(\Theta_3) = \emptyset$ and that $LS(\Theta_2) \cup LS(\Theta_3) = LS(3)$. $\lhd$

2.2 Cycles of length $\frac{n}{2}$

Now, if $n > 2$ is even and if α and β are both cycles of length $\frac{n}{2}$, we obtain the following result:

Proposition 2.4. *Let $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$, where $n > 2$ is even, be such that α and β are both the composition of two cycles of length $\frac{n}{2}$. Then, $\Delta(\Theta) = n! \cdot \left(\frac{n}{2}!\right)^2$.*

Proof.
Let us suppose that:

$$\alpha = (a_0 a_1 ... a_{\frac{n}{2}-1})(a_{\frac{n}{2}} a_{\frac{n}{2}+1} ... a_{n-1}), \qquad \beta = (b_0 b_1 ... b_{\frac{n}{2}-1})(b_{\frac{n}{2}} b_{\frac{n}{2}+1} ... b_{n-1}).$$

By using the canonical construction path [12], we can obtain a Latin square $L = (l_{ij})$ such that $\Theta \in \mathcal{U}(L)$. To do it, similarly to Proposition 2.2, we take $l_{a_0 i} \in N$ for all $i \in N$, such that $l_{a_0 j} \neq l_{a_0 k}$ for all $j \neq k$. Now, fixed $i \in N$, we take $t_i \in N$ such that $b_{t_i} = i$. So, $l_{a_j b_{t_i+j \ (mod \ \frac{n}{2})}} = l_{a_0 i}$, for all $j \in \{0, 1, ..., \frac{n}{2} - 1\}$. In this way, we can define a Latin subrectangle R of L of $\frac{n}{2}$ rows and n columns. Indeed, R is a row block, because its rows correspond to the cycle $(a_0 a_1 ... a_{\frac{n}{2}-1})$. Besides, by swapping the elements l_{0i} in N, we can obtain $n!$ different Latin subrectangles of L, all of them associated by construction to the same rows.

Now, we do the same process with $a_{\frac{n}{2}}$ in the place of a_0, although when we choose the elements $l_{a_{\frac{n}{2}} i} \in N$, we must keep in mind R, as L must be a Latin square. That is, it must be $l_{a_{\frac{n}{2}} i} \in \{l_{a_0 \frac{n}{2}}, l_{a_0 \left(\frac{n}{2}+1\right)}, ..., l_{a_0 n}\}$ for all $i \in \{0, 1, ..., \frac{n}{2} - 1\}$ and $l_{a_{\frac{n}{2}} i} \in \{l_{a_0 1}, l_{a_0 2}, ..., l_{a_0 \left(\frac{n}{2}-1\right)}\}$

for all $i \in \{\frac{n}{2}, \frac{n}{2}+1, ..., n\}$. Therefore, in this way we can obtain finally $n! \cdot \left(\frac{n}{2}!\right)^2$ different Latin squares which have Θ as an autotopism. □

Let us see an example:

Example 2.5. Let us consider $n = 4$ and $N = \{0, 1, 2, 3\}$. If $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_4$ is a principal isotopy such that α and β are both products of two cycles of length 2, Θ must be one of the followings:

$$\begin{array}{ll}
\Theta_1 = ((01)(23), (01)(23), \epsilon); & \Theta_2 = ((01)(23), (02)(13), \epsilon);\\
\Theta_3 = ((01)(23), (03)(12), \epsilon); & \Theta_4 = ((02)(13), (01)(23), \epsilon);\\
\Theta_5 = ((02)(13), (02)(13), \epsilon); & \Theta_6 = ((02)(13), (03)(12), \epsilon);\\
\Theta_7 = ((03)(12), (01)(23), \epsilon); & \Theta_8 = ((03)(12), (02)(13), \epsilon);
\end{array}$$
$$\Theta_9 = ((03)(12), (03)(12), \epsilon).$$

By swapping the values of a, b, c, d, e, f, g in N, we have that:

$LS(\Theta_1) = \left\{ \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ e & f & g & h \\ f & e & h & g \end{pmatrix} \in LS(4) \right\}$	$LS(\Theta_2) = \left\{ \begin{pmatrix} a & b & c & d \\ c & d & a & b \\ e & f & g & h \\ g & h & e & f \end{pmatrix} \in LS(4) \right\}$
$LS(\Theta_3) = \left\{ \begin{pmatrix} a & b & c & d \\ d & c & b & a \\ e & f & g & h \\ h & g & f & e \end{pmatrix} \in LS(4) \right\}$	$LS(\Theta_4) = \left\{ \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ b & a & d & c \\ f & e & h & g \end{pmatrix} \in LS(4) \right\}$
$LS(\Theta_5) = \left\{ \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ c & d & a & b \\ g & h & e & f \end{pmatrix} \in LS(4) \right\}$	$LS(\Theta_6) = \left\{ \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ d & c & b & a \\ h & g & f & e \end{pmatrix} \in LS(4) \right\}$
$LS(\Theta_7) = \left\{ \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ f & e & h & g \\ b & a & d & c \end{pmatrix} \in LS(4) \right\}$	$LS(\Theta_8) = \left\{ \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ g & h & e & f \\ c & d & a & b \end{pmatrix} \in LS(4) \right\}$
$LS(\Theta_9) = \left\{ \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ h & g & f & e \\ d & c & b & a \end{pmatrix} \in LS(4) \right\}$	

So, $|LS(\Theta_i)| = \Delta(\Theta_i) = 4! \cdot (2!)^2 = 96$. By the other way, let us observe that $LS(\Theta_i) \cap LS(\Theta_j) = \emptyset$, except for:

(i,j)	$LS(\Theta_i)\cap LS(\Theta_j)$	(i,j)	$LS(\Theta_i)\cap LS(\Theta_j)$
$(1,5)$ $(1,9)$ $(5,9)$	$\left\{\begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix} \in LS(4)\right\}$	$(1,6)$ $(1,8)$ $(6,8)$	$\left\{\begin{pmatrix} a & b & c & d \\ b & a & d & c \\ d & c & b & a \\ c & d & a & b \end{pmatrix} \in LS(4)\right\}$
$(2,4)$ $(2,9)$ $(4,9)$	$\left\{\begin{pmatrix} a & b & c & d \\ c & d & a & b \\ b & a & d & c \\ d & c & b & a \end{pmatrix} \in LS(4)\right\}$	$(2,6)$ $(2,7)$ $(6,7)$	$\left\{\begin{pmatrix} a & b & c & d \\ c & d & a & b \\ d & c & b & a \\ b & a & d & c \end{pmatrix} \in LS(4)\right\}$
$(3,4)$ $(3,8)$ $(4,8)$	$\left\{\begin{pmatrix} a & b & c & d \\ d & c & b & a \\ b & a & d & c \\ c & d & a & b \end{pmatrix} \in LS(4)\right\}$	$(3,5)$ $(3,7)$ $(5,7)$	$\left\{\begin{pmatrix} a & b & c & d \\ d & c & b & a \\ c & d & a & b \\ b & a & d & c \end{pmatrix} \in LS(4)\right\}$

Where $a, b, c, d \in N$. Therefore, as all the previous intersection contains 4! Latin squares and $\Delta(\Theta_i) = 4\cdot 4!$ for all $i \in \{0, 1, ..., 9\}$, it can be seen that $\left|\bigcup_{i=1}^{9} LS(\Theta_i)\right| = 6\cdot 4! + 9\cdot 2\cdot 4! = 24\cdot 4! = 576 = |LS(4)|$. $\triangleleft$

2.3 Cycles of length $\frac{n}{3}$

Let us suppose now that α and β are both cycles of length $\frac{n}{3}$:

Proposition 2.6. *Let $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$, where $n > 3$ is a multiple of 3, be such that α and β are both the composition of three cycles of length $\frac{n}{3}$. So:*

$$\Delta(\Theta) = n! \cdot \left(\frac{n}{3}!\right)^6 \cdot \sum_{k=0}^{n/3} \left(\begin{array}{c} n/3 \\ k \end{array} \right)^3 .$$

Proof.

Let us suppose that:

$$\alpha = (a_0 a_1 ... a_{\frac{n}{3}-1})(a_{\frac{n}{3}} a_{\frac{n}{3}+1} ... a_{\frac{2n}{3}-1})(a_{\frac{2n}{3}} a_{\frac{2n}{3}+1} ... a_{n-1}),$$

$$\beta = (b_0 b_1 ... b_{\frac{n}{3}-1})(b_{\frac{n}{3}} b_{\frac{n}{3}+1} ... b_{\frac{2n}{3}-1})(b_{\frac{2n}{3}} b_{\frac{2n}{3}+1} ... b_{n-1}).$$

To obtain a Latin square $L = (l_{ij})$ such that $\Theta \in \mathcal{U}(L)$, it is useful to consider the sets $S^{i,j} = \{l_{a_{i\cdot\frac{n}{3}} b_{j\cdot\frac{n}{3}}}, l_{a_{i\cdot\frac{n}{3}} b_{j\cdot\frac{n}{3}+1}}, ..., l_{a_{i\cdot\frac{n}{3}} b_{(j+1)\cdot\frac{n}{3}-1}}\}$ and $S_i = \bigcup_j S^{i,j}$, where $i, j \in \{0, 1, 2\}$. Let us observe that, analogously to the previous results, if, fixed $i \in \{0, 1, 2\}$, we know the $\frac{n}{3}$ elements of S_i, we can define a Latin subrectangle R_i of L of $\frac{n}{3}$ rows and n columns. Indeed, each R_i is the conveniently ordered (that is, unless principal isotopism) following

$\frac{n}{3} \times n$ array:

$$\begin{pmatrix} l_{a_{i\cdot\frac{n}{3}}b_0} & l_{a_{i\cdot\frac{n}{3}}b_1} & \cdots & l_{a_{i\cdot\frac{n}{3}}b_{n-1}} \\ l_{a_{i\cdot\frac{n}{3}+1}b_0} & l_{a_{i\cdot\frac{n}{3}+1}b_1} & \cdots & l_{a_{i\cdot\frac{n}{3}+1}b_{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ l_{a_{(i+1)\cdot\frac{n}{3}-1}b_0} & l_{a_{(i+1)\cdot\frac{n}{3}-1}b_1} & \cdots & l_{a_{(i+1)\cdot\frac{n}{3}-1}b_{n-1}} \end{pmatrix}$$

Therefore, if we exactly know the elements of S_0, S_1 and S_2, we will obtain L. Indeed, the product of the different ways in which we can fix these three sets is the number of different Latin squares which have Θ as a principal autotopism.

We can start with S_0, which can be fixed of $n!$ different ways. Now, to obtain S_1, we fix in a first step the elements of $S^{1,0}$. This set will contain k elements of $S^{0,1}$ and $\frac{n}{3}-k$ elements of $S^{0,2}$, where k can vary between 0 and $\frac{n}{3}$. That is, we can fix $S^{1,0}$ of $\frac{n}{3}! \cdot \sum_{k=0}^{n/3} \binom{n/3}{k}^2$ ways. Besides, for each of the previous ways, the k elements of $S^{0,2}$ which have not been chosen for $S^{1,0}$ must be in $S^{1,1}$ and the $\frac{n}{3}-k$ elements of $S^{0,1}$ which have not been chosen for $S^{1,0}$ must be in $S^{1,2}$. To complete these sets we must choose k elements of $S^{0,0}$ which will correspond to $S^{1,1}$, corresponding the rest of the elements of $S^{0,0}$ to $S^{1,2}$. So, S_1 can be chosen of $\left(\frac{n}{3}!\right)^3 \cdot \sum_{k=0}^{n/3} \binom{n/3}{k}^3$ different ways.

Finally, to obtain S_2, let us observe that according to the previous process, we know which elements correspond to each $S^{2,j}$ and we only must assign each of them to the corresponding $l_{a_{k\cdot\frac{2n}{3}}b_l}$. So, we can fix S_2 of $\left(\frac{n}{3}!\right)^3$ different ways. Therefore, we finally obtain that:

$$\Delta(\Theta) = n! \cdot \left(\frac{n}{3}!\right)^3 \cdot \sum_{k=0}^{n/3} \binom{n/3}{k}^3 \cdot \left(\frac{n}{3}!\right)^3 = n! \cdot \left(\frac{n}{3}!\right)^6 \cdot \sum_{k=0}^{n/3} \binom{n/3}{k}^3.$$

□

Let us see an example:

Example 2.7. Let us consider $n = 6$ and $N = \{0,1,2,3,4,5\}$. There are $15^2 = 225$ principal isotopisms $(\alpha, \beta, \epsilon) \in \mathcal{I}_6$, with α and β being a composition of three cycles of length 2. We will work, for example, with the following principal isotopisms:

$$\Theta_1 = \{((01)(23)(45), (02)(35)(14), \epsilon)\},$$

$$\Theta_2 = \{((02)(14)(35), (01)(23)(45), \epsilon)\}.$$

So:

$$LS(\Theta_1) = \left\{ \begin{pmatrix} a & b & c & d & e & f \\ c & e & a & f & b & d \\ g & h & i & j & k & l \\ i & k & g & l & h & j \\ m & o & p & q & r & s \\ p & r & m & s & o & q \end{pmatrix} \in LS(6) \right\}_{a,b,\ldots,r,s\in N},$$

$$LS(\Theta_2)=\left\{\begin{pmatrix} a & b & c & d & e & f\\ g & h & i & j & k & l\\ b & a & d & c & f & e\\ m & o & p & q & r & s\\ h & g & j & i & l & k\\ o & m & q & p & s & r\end{pmatrix}\in LS(6)\right\}_{a,b,\dots,r,s\in N}$$

From Proposition 2.6, $\Delta(\Theta_1)=\Delta(\Theta_2)=6!\cdot(2!)^6\cdot\sum_{k=0}^{2}\binom{2}{k}^3=460800$. Besides:

$$LS(\Theta_1)\cap LS(\Theta_2)=\left\{\begin{pmatrix} a & b & c & d & e & f\\ c & e & a & f & b & d\\ b & a & d & c & f & e\\ d & f & b & e & a & c\\ e & c & f & a & d & b\\ f & d & e & b & c & a\end{pmatrix}\in LS(6)\right\}_{a,b,\dots,k,l\in N},$$

being $|LS(\Theta_1)\cap LS(\Theta_2)|=6!=720$. $\triangleleft$

2.4 Cycles of length $\frac{n}{4}$

Let us now suppose that α and β are both the composition of four cycles of length $\frac{n}{4}$:

$$\alpha=(a_0a_1\dots a_{\frac{n}{4}-1})(a_{\frac{n}{4}}a_{\frac{n}{4}+1}\dots a_{\frac{2n}{4}-1})(a_{\frac{2n}{4}}a_{\frac{2n}{4}+1}\dots a_{\frac{3n}{4}-1})(a_{\frac{3n}{4}}a_{\frac{3n}{4}+1}\dots a_{n-1}),$$

$$\beta=(b_0b_1\dots b_{\frac{n}{4}-1})(b_{\frac{n}{4}}b_{\frac{n}{4}+1}\dots b_{\frac{2n}{4}-1})(b_{\frac{2n}{4}}b_{\frac{2n}{4}+1}\dots b_{\frac{3n}{4}-1})(b_{\frac{3n}{4}}b_{\frac{3n}{4}+1}\dots b_{n-1}).$$

To obtain $\Delta(\Theta)$, we will now indicate a possible algorithm to follow. So, to get a Latin square $L\in LS(n)$ which has Θ as a principal autotopism, we can define, fixed $i,j\in\{0,1,2,3\}$ and analogously to the proof of Proposition 2.6, the sets $S^{i,j}=\{l_{a_{i\cdot\frac{n}{4}}b_{j\cdot\frac{n}{4}}}, l_{a_{i\cdot\frac{n}{4}}b_{j\cdot\frac{n}{4}+1}},\dots,l_{a_{i\cdot\frac{n}{4}}b_{(j+1)\cdot\frac{n}{4}-1}}\}$ and $S_i=\bigcup_j S^{i,j}$. Fixed the elements l_{st} corresponding to each S_i, we can obtain a subrectangle R_i of L, in a similar way as we have just done it in the mentioned proof. Therefore, to get L, we must fix all the sets S_i and to do it, we can follow the next algorithm: first, we fix S_0, which can be obtained of $n!$ different ways. Then, we are going to fix the sets S_i with i from 1 to 3, in this order. To obtain each S_i we must fix the sets $S^{i,j}$, with j from 0 to 3, also in this order.

Let us observe that, once we have fixed the elements of $S^{0,j}$ for all $j\in\{0,1,2,3\}$, whenever we want to fix the elements of a set $S^{i,j}$, with $i\neq 0$, we must choose x_t elements of $S^{0,t}$ with $t\in\{0,1,2,3\}\setminus\{j\}$, in such a way that $\sum_t x_t=\frac{n}{4}$. Besides, all these elements must be adequately chosen to obtain finally a Latin square. So, to simplify the notation, we are going to define for each $i\in\{1,2,3\}$ and $j\in\{0,1,2,3\}$:

$$s^{i,j}=\left(s_0^{i,j},s_1^{i,j},s_2^{i,j},s_3^{i,j}\right)\in\left\{0,1,\dots,\frac{n}{4}\right\}^4,$$

such that:

i) $s_j^{i,j} = 0$, for all $i \in \{1,2,3\}$ and $j \in \{0,1,2,3\}$,

ii) $\sum_{t=0}^{3} s_t^{i,j} = \frac{n}{4}$, for all $i \in \{1,2,3\}$ and $j \in \{0,1,2,3\}$,

iii) $\sum_{j=0}^{3} s_t^{i,j} = \frac{n}{4}$, for all $i \in \{1,2,3\}$ and $t \in \{0,1,2,3\}$,

iv) $\sum_{i=1}^{3} s_t^{i,j} = \frac{n}{4}$, for all $j \in \{0,1,2,3\}$ and $t \in \{0,1,2,3\} \setminus \{j\}$.

Then, fixed a subset $A \subseteq S_0$, we will say that we choose $s^{i,j} = (s_0^{i,j}, s_1^{i,j}, s_2^{i,j},\ s_3^{i,j})$ elements of $S_0 \setminus A$ to fix the elements which belong to $S^{i,j}$, if we choose $s_0^{i,j}$ ones of $S^{0,0} \setminus A$, $s_1^{i,j}$ ones of $S^{0,1} \setminus A$, $s_2^{i,j}$ ones of $S^{0,2} \setminus A$ and $s_3^{i,j}$ ones of $S^{0,3} \setminus A$. Let us observe that the previous conditions (i) to (iv) are therefore necessary to get a Latin square starting from all the so fixed $S^{i,j}$.

Therefore, the canonical construction path method in this case follows the next algorithm:

Algorithm 2.8.

i) S_0 can be fixed of $n!$ different ways.

ii) To determine $S^{1,0}$ we must choose $(0, s_1^{1,0}, s_2^{1,0}, \frac{n}{4} - s_1^{1,0} - s_2^{1,0})$ elements of S_0, where $s_1^{1,0} + s_2^{1,0} \leq \frac{n}{4}$.

Fixed $s_1^{1,0}$ and $s_2^{1,0}$:

iii) To determine $S^{1,1}$ we must choose $(s_0^{1,1}, 0, s_2^{1,1}, \frac{n}{4} - s_0^{1,1} - s_2^{1,1})$ elements of $S_0 \setminus S^{1,0}$, where $s_2^{1,1} \leq \frac{n}{4} - s_2^{1,0}$ and $\frac{n}{4} - s_1^{1,0} - s_2^{1,0} \leq s_0^{1,1} + s_2^{1,1} \leq \frac{n}{4}$.

iv) To determine $S^{2,0}$ we must choose $(0, s_1^{2,0}, s_2^{2,0}, \frac{n}{4} - s_1^{2,0} - s_2^{2,0})$ elements of $S_0 \setminus S^{1,0}$, where $s_1^{2,0} \leq \frac{n}{4} - s_1^{1,0}$, $s_2^{2,0} \leq \frac{n}{4} - s_2^{1,0}$ and $\frac{n}{4} - s_1^{1,0} - s_2^{1,0} \leq s_1^{2,0} + s_2^{2,0} \leq \frac{n}{4}$.

Fixed $s_0^{1,1}$ and $s_2^{1,1}$:

v) The rest of the $s_1^{1,0} + s_2^{1,0} + s_0^{1,1} + s_2^{1,1} - \frac{n}{4}$ elements of $S^{0,3}$ which we have not yet used to fix $S^{1,0}$ and $S^{1,1}$ must be in $S^{1,2}$. Besides, we must choose $s_0^{1,2}$ elements of $S^{0,0} \setminus S^{1,1}$ and $\frac{n}{2} - s_1^{1,0} - s_2^{1,0} - s_0^{1,1} - s_2^{1,1} - s_0^{1,2}$ elements of $S^{0,1} \setminus S^{1,0}$, where $\frac{n}{4} - s_2^{1,0} - s_0^{1,1} - s_2^{1,1} \leq s_0^{1,2} \leq \frac{n}{4} - s_0^{1,1}$ and $s_1^{1,0} + s_2^{1,0} + s_0^{1,1} + s_2^{1,1} - \frac{n}{4} + s_0^{1,2} \leq \frac{n}{4}$.

Fixed $s_1^{2,0}$ and $s_2^{2,0}$:

vi) To determine $S^{2,1}$ we must choose $(s_0^{2,1}, 0, s_2^{2,1}, \frac{n}{4} - s_0^{2,1} - s_2^{2,1})$ elements of $S_0 \setminus \{S^{1,1} \cup S^{2,0}\}$, where $s_0^{2,1} \leq \frac{n}{4} - s_0^{1,1}$, $s_2^{2,1} \leq \frac{n}{4} - s_2^{1,1} - s_2^{2,0}$ and $\frac{n}{2} - s_1^{2,0} - s_2^{2,0} - s_0^{1,1} - s_2^{1,1} \leq s_0^{2,1} + s_2^{2,1} \leq \frac{n}{4}$. Besides:

a) As to fix $S^{2,1}$ and $S^{1,2}$, we would have used $s_0^{2,1} + s_0^{1,2}$ elements of $S^{0,0}$, to exist $S^{2,2}$ we must also impose that $s_0^{2,1} + s_0^{1,2} \leq \frac{n}{4}$.

b) As to fix $S^{2,0}$ and $S^{1,2}$, we would have used $s_1^{2,0} + \frac{n}{2} - s_1^{1,0} - s_2^{1,0} - s_0^{1,1} - s_2^{1,1} - s_0^{1,2}$ elements of $S^{0,1}$, to exist $S^{2,2}$ we must also impose that $s_1^{2,0} + \frac{n}{2} - s_1^{1,0} - s_2^{1,0} - s_0^{1,1} - s_2^{1,1} - s_0^{1,2} \leq \frac{n}{4}$.

c) As to fix $S^{2,0}$, $S^{2,1}$ and $S^{1,2}$, we would have used $\frac{n}{4} - (s_1^{2,0} + s_2^{2,0} + s_0^{2,1} + s_2^{2,1} - s_1^{1,0} - s_2^{1,0} - s_0^{1,1} - s_2^{1,1})$ elements of $S^{0,3}$, to exist $S^{2,2}$ we must impose that $0 \leq s_1^{2,0} + s_2^{2,0} + s_0^{2,1} + s_2^{2,1} - s_1^{1,0} - s_2^{1,0} - s_0^{1,1} - s_2^{1,1} \leq \frac{n}{4}$.

Finally, fixed $s_0^{2,1}$ and $s_2^{2,1}$:

vii) The rest of the $s_1^{2,0} + s_2^{2,0} + s_0^{2,1} + s_2^{2,1} - s_1^{1,0} - s_2^{1,0} - s_0^{1,1} - s_2^{1,1}$ elements of $S^{0,3}$ which we have not yet used to fix $S^{2,0}$, $S^{2,1}$ and $S^{1,2}$ must be in $S^{2,2}$. Besides, we must choose $s_0^{2,2}$ elements of $S^{0,0} \backslash \{S^{1,2} \cup S^{2,1}\}$ and $\frac{n}{4} - s_1^{2,0} - s_2^{2,0} - s_0^{2,1} - s_2^{2,1} + s_1^{1,0} + s_2^{1,0} + s_0^{1,1} + s_2^{1,1} - s_0^{2,2}$ elements of $S^{0,1} \backslash \{S^{2,0} \cup S^{1,2}\}$, where $\frac{n}{2} - s_2^{2,0} - s_0^{2,1} - s_2^{2,1} - s_0^{1,2} \leq s_0^{2,2} \leq \frac{n}{4} - s_0^{1,2} - s_0^{2,1}$ and $s_1^{2,0} + s_2^{2,0} + s_0^{2,1} + s_2^{2,1} - s_1^{1,0} - s_2^{1,0} - s_0^{1,1} - s_2^{1,1} + s_0^{2,2} \leq \frac{n}{4}$.

After this process, the elements of the sets $S^{1,3}, S^{2,3}, S^{3,0}, S^{3,1}, S^{3,2}$ and $S^{3,3}$ are all determined. So, we can obtain a Latin square L which has Θ as a principal autotopism. To get it, we must only fix in each $S^{i,j}$ the elements which correspond with each $l_{a_{i\cdot\frac{n}{4}} b_{j\cdot\frac{n}{4}+t}}$ with $t \in \{0,1,...,n-1\}$. It can be done, once we know which elements are in $S^{i,j}$, of $\frac{n}{4}!$ different ways.

So, if we denote by $\Omega(\Theta)$ the number of different ways in which we can choose the elements that are included in all the subsets $S^{i,j}$ with $i \in \{1,2,3\}$ and $j \in \{0,1,2,3\}$, by following the previous algorithm, we obtain finally the following:

Proposition 2.9. *Let* $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$, *where* $n > 4$ *is a multiple of* 4, *be such that* α *and* β *are both the composition of four cycles of length* $\frac{n}{4}$. *So:*

$$\Delta(\Theta) = n! \cdot \left(\frac{n}{4}!\right)^{12} \cdot \Omega(\Theta)$$

□

In the next table, we can see some values of $\Omega(\Theta)$, obtained by computing the previous algorithm with Maple®:

n	8	12	16	20	24	28
$\Omega(\Theta)$	535	60582	10144679	1829667628	362014297870	75689842399097

Let us see an example:

Example 2.10. Let us consider $n = 8$ and $N = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and let us take the following principal isotopisms:

$$\Theta_1 = \{((01)(23)(45)(67), (01)(24)(35)(67), \epsilon)\},$$
$$\Theta_2 = \{((02)(13)(46)(57), (02)(14)(36)(57), \epsilon)\},$$
$$\Theta_3 = \{((04)(15)(26)(37), (03)(15)(26)(47), \epsilon)\}.$$

So:

$$LS(\Theta_1) = \left\{ \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & a & e & f & c & d & h & g \\ i & j & k & l & m & o & p & q \\ j & i & m & o & k & l & q & p \\ r & s & t & u & v & w & x & y \\ s & r & v & w & t & u & y & x \\ z & A & B & C & D & E & F & G \\ A & z & D & E & B & C & G & F \end{pmatrix} \in LS(8) \right\}_{a,b,\ldots,y,z,A,B,\ldots,F,G \in N},$$

$$LS(\Theta_2) = \left\{ \begin{pmatrix} a & b & c & d & e & f & g & h \\ i & j & k & l & m & o & p & q \\ c & e & a & g & b & h & d & f \\ k & m & i & p & j & q & l & o \\ r & s & t & u & v & w & x & y \\ z & A & B & C & D & E & F & G \\ t & v & r & x & s & y & u & w \\ B & D & z & F & A & G & C & E \end{pmatrix} \in LS(8) \right\}_{a,b,\ldots,y,z,A,B,\ldots,F,G \in N},$$

$$LS(\Theta_3) = \left\{ \begin{pmatrix} a & b & c & d & e & f & g & h \\ i & j & k & l & m & o & p & q \\ r & s & t & u & v & w & x & y \\ z & A & B & C & D & E & F & G \\ d & f & g & a & h & b & c & e \\ l & o & p & i & q & j & k & m \\ u & w & x & r & y & s & t & v \\ C & E & F & z & G & A & B & D \end{pmatrix} \in LS(8) \right\}_{a,b,\ldots,y,z,A,B,\ldots,F,G \in N}.$$

From Proposition 2.9, $\Delta(\Theta_1) = \Delta(\Theta_2) = \Delta(\Theta_3) = 8! \cdot (4!)^{12} \cdot 535 = 88355635200$. Besides:

$$LS(\Theta_1) \cap LS(\Theta_2) \cap LS(\Theta_3) = \left\{ \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & a & e & f & c & d & h & g \\ c & e & a & g & b & h & d & f \\ e & c & b & h & a & g & f & d \\ d & f & g & a & h & b & c & e \\ f & d & h & b & g & a & e & c \\ g & h & d & c & f & e & a & b \\ h & g & f & e & d & c & b & a \end{pmatrix} \in LS(8) \right\}_{a,b,c,d,e,f,g,h \in N},$$

being $|LS(\Theta_1) \cap LS(\Theta_2) \cap LS(\Theta_3)| = 8! = 40320$. $\triangleleft$

2.5 Cycles of length $\frac{n}{k}$

Let us finally study the general case. So, fixed $n \in \mathbb{N}$ and $N = \{0, 1, ..., n-1\}$, let us suppose that α and β are both the composition of k cycles of length $\frac{n}{k}$:

$$\alpha = (a_0 a_1 ... a_{\frac{n}{k}-1})(a_{\frac{n}{k}} a_{\frac{n}{k}+1} ... a_{\frac{2n}{k}-1}) ... (a_{\frac{(k-1)n}{k}} a_{\frac{(k-1)n}{k}+1} ... a_{n-1}),$$

$$\beta = (b_0 b_1 ... b_{\frac{n}{k}-1})(b_{\frac{n}{k}} b_{\frac{n}{k}+1} ... b_{\frac{2n}{k}-1}) ... (b_{\frac{(k-1)n}{k}} b_{\frac{(k-1)n}{k}+1} ... b_{n-1}).$$

To obtain $\Delta(\Theta)$, we can follow a similar algorithm to the previously indicated. So, to get a Latin square $L \in LS(n)$ which has Θ as a principal autotopism, we can define:

$$S^{i,j} = \{l_{a_{i \cdot \frac{n}{k}} b_{j \cdot \frac{n}{k}}}, l_{a_{i \cdot \frac{n}{k}} b_{j \cdot \frac{n}{k}+1}}, ..., l_{a_{i \cdot \frac{n}{k}} b_{(j+1) \cdot \frac{n}{k}-1}}\}; \qquad S_i = \bigcup_{j=0}^{k-1} S^{i,j}, \text{ for all } i, j \in \{0, 1, ..., k-1\}.$$

Then, it is easy to prove the following:

Theorem 2.11. *Fixed $k \in \mathbb{N}$, let $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$, where $n > k$ is a multiple of k, be such that α and β are both the composition of k cycles of length $\frac{n}{k}$. Then:*

$$\Delta(\Theta) = n! \cdot \left(\frac{n}{k}!\right)^{k(k-1)} \cdot \Omega(\Theta),$$

where $\Omega(\Theta)$ is 1, if $k = 1$, and the number of different ways in which we can choose the elements that are included in the corresponding subsets $S^{i,j}$, if $k > 1$. □

In the next table we can see the values of $\Omega(\Theta)$ and $\Delta(\Theta)$, if $2 \leq n \leq 9$:

n	k	$\Omega(\Theta)$	$\Delta(\Theta)$	$N(n,n)$
2	1	1	2	2
3	1	6	12	12
4	1	1	24	576
	2	1	96	
5	1	1	120	161280
6	1	1	720	812851200
	2	1	25920	
	3	10	460800	
7	1	1	5040	61479419904000
8	1	1	40320	108776032459082956800
	2	1	23224320	
	4	535	88355635200	
9	1	1	362880	5524751496156892842531225600
	3	56	948109639680	

2.6 Concluding remarks

Although we have studied in this section the case in which Θ is a principal autotopism, an analogous study can be done with the other two possibilities given in Proposition 2.1, that is, $\Theta = (\epsilon, \beta, \gamma)$ or $\Theta = (\alpha, \epsilon, \gamma)$, although in the first one, the canonical construction path must be done with columns blocks in place of row blocks. So, this algorithm and as a consequence, Theorem 2.11, proves indeed that the necessary condition of Proposition 2.1 is also sufficient.

3 Application in Cryptography: $\mathfrak{F}$-critical sets

A *secret sharing scheme* [3], [19] is a method of sharing a secret key K, by giving n pieces of information called *shares* to n participants, in such a way that K can be reconstructed from certain authorized groups of shares and it cannot be done from unauthorized groups of them. The *access structure* Γ is the set of all the previous authorized groups. A *key management scheme* consists of a number of secret sharing schemes, all of them with a common participant, which can have more than one share. In a *multilevel scheme* the participants are ranked in m ranks, in such a way that l_i of them are in the rank r_i for $i \in \{1, ..., m\}$, where $\sum_{i=1}^{m} l_i = n$ and the secret key can be recovered from the shares of the l_i participants of rank r_i.

There are different mathematical models of secret sharing schemes: geometric configurations, polynomial interpolation, block designs, matroids, vector spaces, graphs, etc. One of this model uses critical sets in Latin squares: We fix a Latin square $L = (l_{ij}) \in LS(n)$ which will be the secret key, although its order n is made public. Each share is then a triple $(i, j, l_{ij}) \in L$ and the set of all the used triples is denoted by S. So, if some participants get a critical set of L by sharing its corresponding triples, they will obtain as consequence the secret key L. The access structure is then $\Gamma = \{P \in PLS(n) : P \subseteq \bigcup_S (i, j, l_{ij}) \subseteq L$ and $\exists C \in CS(L)$ such that $C \subseteq P\}$. In this model all the participants have shares of the same "weight". By the other way, a multilevel scheme can also be analogously given, by placing all the participants in different levels, in such a way that it exists only a critical set in each level. If one participant is in more than one level, then we have an example of a key management scheme.

There are models in which shares are not of the same weight, that is, models in which some shares can offer more information than other ones. It is useful for example in *hierarchical models* in which there exists some need to provide different levels of confidentiality for data. So, in the previous example, we can obtain a hierarchical model if we give to each participant a different number of triples as share. An other possibility would be to consider different types of shares. In this sense, we can study the use of autotopisms of a Latin square as shares of a secret sharing scheme. To do it, let us observe that, as we have seen in previous sections, each autotopism can be associated to a different number of Latin squares. So, the information about L which gives each autotopism is not the same. To give a possible measure of this difference, we give the following:

Definition 3.1. Let $\Theta \in \mathcal{I}_n$. We define the *weight of* Θ *in* $LS(n)$ as:

$$\omega(\Theta) = \begin{cases} 0 \text{ , if } \Delta(\Theta) = 0, \\ \frac{1}{\Delta(\Theta)} \text{ , if } \Delta(\Theta) \neq 0. \end{cases} .$$

By the other way, a set of autotopisms can never define an unique Latin square, because autotopisms are associated to symmetries of Latin squares and so, given a Latin square L associated to a set $\mathfrak{F}$ of autotopisms, every Latin square L' isotopic to L by an isotopism of type (Id, Id, γ) is also associated to $\mathfrak{F}$. So, if we want to define a secret sharing scheme by using autotopisms as shares, we must also use one or more triples of the corresponding

Latin square to finally get the secret key. Indeed, fixed a subgroup $\mathfrak{F}$ of $\mathcal{U}(L)$ it will be necessary to use the triples of a $\mathfrak{F}$-critical set of L. In this sense, it is interesting to extend in a similar way the previous concept of weight to these triples. To do it, as, fixed a triple $T=(i,j,k)\in N^3$, there are $\frac{N(n,n)}{n}$ Latin squares of order n which contain T, it is enough to define the *weight of* T *in* $LS(n)$ as $\omega(T)=\frac{n}{N(n,n)}$.

It can be interesting to extend these concepts to sets of isotopisms and partial Latin squares (as sets of triples), because, in this way, it could be studied the possible relations of interest to cooperate among participants in such a model. Leaving it for a future study, we have therefore interested in the following protocol:

- We fix a Latin square L of order n. The number n is made public, but L is kept secret as the key.
- A set S which is the union of a number of triples and autotopisms of L is defined.
- Each element of S is privately distributed to an unique participant.
- When a group of participants whose shares constitute a subset $\mathfrak{F}$ of $\mathcal{U}(L)$ and a $\mathfrak{F}$-critical set come together, they can reconstruct L and hence, the secret key.

To finish this paper, let us see an example of this protocol:

Example 3.2. Let us consider $L=\begin{pmatrix}0&1&2&3&4&5\\1&2&0&4&5&3\\2&0&1&5&3&4\\3&4&5&0&1&2\\4&5&3&1&2&0\\5&3&4&2&0&1\end{pmatrix}\in LS(6)$, and the shares:

$$\Theta_1=((012)(345),Id,(021)(354)),\qquad \Theta_2=(Id,(012)(345),(021)(354)),$$

$$\Theta_3=((03)(14)(25),(03)(14)(25),Id),\qquad \Theta_4=(Id,(03)(14)(25),(03)(14)(25)),$$

$$T_1=(0,4,4),\quad T_2=(1,1,2),\quad T_3=(1,5,3),\quad T_4=(2,2,1),$$

$$T_5=(2,4,3),\quad T_6=(3,1,4),\quad T_7=(3,2,5),\quad T_8=(3,3,0),$$

$$T_9=(4,0,4),\quad T_{10}=(5,3,2),\quad T_{11}=(5,5,1).$$

So, we have that:

$$\omega(\Theta_1)=\omega(\Theta_2)=\frac{1}{25920},\qquad \omega(\Theta_3)=\omega(\Theta_4)=\frac{1}{460800},$$

$$\omega(T_i)=\frac{6}{812851200}=\frac{1}{135475200},\ \text{for all } i\in\{1,2,...,11\}.$$

We can therefore see that Θ_1 and Θ_2 are the shares which give more information about L. By the other way, there are a lot of possible combinations to reconstruct L, by taking together a subset A of $\mathfrak{F}=\{\Theta_1,\Theta_2,\Theta_3,\Theta_4\}$ and a subset B of $T=\{T_1,T_2,...,T_{11}\}$. So, for example, if m is the total number of shared shares, we have the following minimal subsets of the corresponding access structure Γ of this secret sharing scheme:

m	A	B	m	A	B
11	–	T	6	$\Theta_1 \cup \Theta_2$	$\{T_1, T_2, T_6, T_8\}$
11	Θ_4	$T \setminus \{T_9\}$	6	$\Theta_1 \cup \Theta_4$	$\{T_2, T_3, T_7, T_9\}$
10	Θ_3	$T \setminus \{T_1, T_{11}\}$	6	$\Theta_2 \cup \Theta_3$	$\{T_3, T_6, T_8, T_{10}\}$
10	$\Theta_3 \cup \Theta_4$	$T \setminus \{T_1, T_9, T_{11}\}$	6	$\Theta_1 \cup \Theta_3 \cup \Theta_4$	$\{T_2, T_4, T_8\}$
9	Θ_1	$T \setminus \{T_5, T_7, T_{10}\}$	5	$\Theta_1 \cup \Theta_2 \cup \Theta_3$	$\{T_1, T_2\}$
9	Θ_2	$T \setminus \{T_1, T_7, T_{10}\}$	5	$\Theta_2 \cup \Theta_3 \cup \Theta_4$	$\{T_1, T_2\}$
7	$\Theta_1 \cup \Theta_3$	$\{T_2, T_3, T_4, T_6, T_9\}$	5	$\Theta_1 \cup \Theta_2 \cup \Theta_4$	$\{T_2, T_4\}$
7	$\Theta_2 \cup \Theta_4$	$\{T_1, T_2, T_4, T_6, T_9\}$	5	$\mathfrak{F}$	$\{T_1\}$

$\lhd$

References

[1] Albert, A. A., Quasigroups I, Transactions of the American Mathematical Society 54 (1943) 507 - 519.

[2] S. E. Bammel and J. Rothstein, The number of 9x9 Latin squares, Discrete Math., 11 (1975) 93 - 95.

[3] G. R. Blakley, Safeguarding cryptographic keys. Proc. AFIPS 1979 Natl. Computer Conference, New York, 48, June 1979, pp. 313 - 317.

[4] R. H. Bruck, Some results in the theory of quasigroups, Transactions of the American Mathematical Society 55 (1944) 19-54.

[5] J. A. Cooper, D. Donovan, J. Seberry, Secret Sharing Schemes arising from Latin squares, Bull. Inst. Combin. Appl. 12 (1994) 33 - 43.

[6] D. Curran, G.H.J. van Rees, Critical sets in latin squares, Proceedings of the Eighth Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Congr. Numer. 22 (1979) 165 - 168.

[7] A. A. Drisko, On the Number of Even and Odd Latin Squares of Order $p+1$, Advances in Mathematics 128 (1997) 20-35.

[8] R. M. Falcón Ganfornina, Study of Critical Sets in Latin Squares by using the Autotopism Group, submitted (2005).

[9] I. A. Faradzev, Constructive enumeration of combinatorial objects, Problemes Combinatoires des Graphes Colloque International. CNRS 260. CNRS Paris (1978) 131 - 135.

[10] C. Kościelny, Generating quasigroups for cryptographic applications, International Journal of Applied Mathematics and Computer Science 12 (4) (2002) 559 - 569

[11] B.D. McKay, Nauty user's guide (version 1.5), Technical Report TR-CS-90-02, Department of Computer Science, Australian National University, 1990.

[12] B. D. McKay, Isomorph-free exhaustive generation, J. Algorithms 26 (1998) 306 - 324.

[13] B.D. McKay, A. Meynert, W. Myrvold, Small Latin Squares, Quasigroups and Loops, submitted (2004).

[14] B. D. McKay, I. M. Wanless, Latin squares of order eleven. Preprint 2004. http://cs.anu.edu.au/ bdm/papers/ls11.pdf

[15] J. Nelder, Critical sets in Latin squares, CSIRO Division of Math. and Stats, Newsletter 38:4 (1977).

[16] R. C. Read, Every one a winner, Annals Discrete Math. 2 (1978) 107 - 120.

[17] A. Sade, Autotopies des quasigroupes et des systémes associatifs, Arch. Math. 4 No. 1 (1968) 1 - 23.

[18] J. Seberry, Secret sharing and group identification, R & D Studies, Stage 3, Report from the Centre for Computing and Communication Research to Telecom Australia (1990).

[19] A. Shamir, How to share a secret. Comm. ACM 22, No. 11, Nov. 1979, pp. 612 - 613.

[20] M. B. Wells, The number of Latin squares of order 8, J. Combin. Theory 3 (1967) 98 - 99.

Department of Geometry and Topology. University of Seville.
Apdo. 1160. 41080 - Seville, Spain.