*mathematics*

MDPI

*Article*

# A Discussion of a Cryptographical Scheme Based in $\mathfrak{F}$-Critical Sets of a Latin Square †

**Laura M. Johnson [1,*] and Stephanie Perkins [2]**

[1] School of Mathematics and Statistics, University of St. Andrews, St Andrews KY16 9SS, UK
[2] School of Computing and Mathematics, University of South Wales, Pontypridd CF37 1DL, UK; stephanie.perkins@southwales.ac.uk
* Correspondence: lj68@st-andrews.ac.uk

† The work detailed in this short communication was undertaken as part of an MMath research module at the University of South Wales.

**Abstract:** This communication provides a discussion of a scheme originally proposed by Falcón in a paper entitled "Latin squares associated to principal autotopisms of long cycles. Applications in cryptography". Falcón outlines the protocol for a cryptographical scheme that uses the $\mathfrak{F}$-critical sets associated with a particular Latin square to generate access levels for participants of the scheme. Accompanying the scheme is an example, which applies the protocol to a particular Latin square of order six. Exploration of the example itself, revealed some interesting observations about both the structure of the Latin square itself and the autotopisms associated with the Latin square. These observations give rise to necessary conditions for the generation of the $\mathfrak{F}$-critical sets associated with certain autotopisms of the given Latin square. The communication culminates with a table which outlines the various access levels for the given Latin square in accordance with the scheme detailed by Falcón.

**Keywords:** $\mathfrak{F}$-critical sets; Latin square; Latin subsquare; intercalate; secret sharing scheme



**Citation:** Johnson, L.M.; Perkins, S. A Discussion of a Cryptographical Scheme Based in $\mathfrak{F}$-Critical Sets of a Latin Square †. *Mathematics* **2021**, *9*, 285. https://doi.org/10.3390/math9030285

Academic Editor: Carsten Schneider
Received: 30 November 2020
Accepted: 27 January 2021
Published: 31 January 2021



## 1. Introduction and Preliminaries

A *Latin square* of order $n$ is an $n \times n$ array comprising of $n$ distinct elements, such that each element occurs exactly once in each row and column [1,2]. A *partial Latin square* is an $n \times n$ array with all entries of the array belonging to the set $\{0, 1, \ldots, n-1\}$. There can be blank entries within a *partial Latin square*, but each element of the set $\{0, 1, \ldots, n-1\}$ must only occur once in each row and column [3]. Partial Latin squares can be considered substructures of *Latin squares*, as such; a partial Latin square can be *completed* to form a Latin square by replacing the blank entries of the partial Latin square with elements of the set $\{0, 1, \ldots, n-1\}$ in such a way that each element in the set only occurs once in each row and column [3]. A *partial Latin square* is said to be *uniquely completable* if it only has one possible *completion* [3]. We consider two mechanisms by which a partial Latin square $P$ can be (uniquely) completed to a Latin square $L$. A triple $(i, j; k) \in P$ denotes an entry within a partial Latin square such that $i$ is the row component, $j$ is the column component and $k$ denotes the symbol in the cell $(i, j)$. A triple $(i, j; k)$ in a partial Latin square $P$ is *forced* if the cell $(i, j)$ is the only empty cell in either the $i$th row or $j$th column and the symbol $k$ is the only symbol not appearing in the respective row or column. Similarly a triple is forced if the symbol $k$ appears in every row and column of $L$ except the $i$th row and $j$th column [4].

The second mechanism considered is applying autotopisms to the set of triples of a partial Latin square $P$ to generate a Latin square $L$, on occasion this may additionally require the application of forced moves. Before defining an autotopism, it is important to define the notion of a quasigroup; a set $S$ is a *quasigroup* if there exists a binary operator $*$ such that $\forall a, b \in S$ $a * x = b$ and $y * a = b$ have exactly one solution. The multiplication table of a quasigroup forms a Latin square [1,2]. An autotopism is formally defined [1,2,5];

**Definition 1.** *Let $(B, \cdot)$ and $(C, *)$ be two quasigroups. An isotopism is an ordered triple of row, column and symbol permutations, $\theta = (\alpha, \beta, \gamma)$ that maps $(B, \cdot)$ onto $(C, *)$, providing that $\forall i, j \in B$, $i, j$ denote a pair of row and column coordinates $(\alpha(i)) * (\beta(j)) = \gamma(i \cdot j)$. An autotopism is an isotopism that maps a quasigroup onto itself.*

Let Atop($L$) denote the set of all autotopisms associated with a Latin square $L$. Atop($L$) constitutes a group under the composition of permutations; this is know as the autotopism group of $L$ [4]. As stated in [4], each autotopism $\theta = (\alpha, \beta, \gamma) \in$ Atop($L$) generates a subgroup of Atop($L$), denoted $\langle\theta\rangle$. This may be extended to the set generated by $\theta_1, .., \theta_q \in$ Atop($L$), which will also form a subgroup of Atop($L$), denoted $\langle\theta_1, \ldots, \theta_p\rangle$.

As in [4], let Ent($P$) denote the set of non-empty cells of a partial Latin square $P$. Further, Reference [4] defines the $\theta$-orbit of a triple $(i, j; k) \in$ Ent(L), for some autotopism $\theta = (\alpha, \beta, \gamma) \in$ Atop($L$), as the set

$$\mathrm{Orb}_\theta((i, j; k)) = \{(\alpha^m(i), \beta^m(j); \gamma^m(k) : m \geq 0\} \subseteq \mathrm{Ent(L)}$$

This idea can be extended to $\mathfrak{F}$-orbits [4]. For a collection of autotopisms $\mathfrak{F} \subseteq$ Atop($L$), the $\mathfrak{F}$-orbit of a triple $(i, j; k) \in$ Ent(L) is the set

$$\mathrm{Orb}_\mathfrak{F}((i, j; k)) = \bigcup_{\theta \in \mathfrak{F}} \{(\alpha^m(i), \beta^m(j); \gamma^m(k) : m \geq 0\} \subseteq \mathrm{Ent(L)}.$$

We are interested in using $\mathfrak{F}$-orbits to determine $\mathfrak{F}$-critical sets. A critical set is formally defined [5]:

**Definition 2.** *A critical set C in a Latin square, L, is a set*

$$C = \{(i, j; k) : i,j,k \in \{0, 1, ..., n - 1\}\}$$

*where:*

1. *L is the only Latin square of order n which has the symbol k in the cell $(i, j)$ for each $(i, j; k) \in C$.*
2. *No proper subset of C has property 1.*

Furthermore, we define a partial Latin square $P$ to be $\mathfrak{F}$-completable to a Latin square $L$, with $\mathfrak{F} \subseteq$ Atop(P), if there exists a partial Latin square $Q$ that is completable to $L$ such that;

$$\mathrm{Ent}(Q) = \bigcup_{t \in Ent(P)} Orb_\mathfrak{F}(t).$$

We can say that $P$ is uniquely $\mathfrak{F}$-completable if $L$ is unique, and moreover, $P$ is an $\mathfrak{F}$-critical set of the Latin square $L$ if no proper subset of Ent($P$) is $\mathfrak{F}$-completable to $L$ [4].

The paper by Falcón [6], on which this communication is based, looks at building a secret sharing scheme using $\mathfrak{F}$-critical sets.

A *secret sharing scheme* is a cryptographical scheme in which $k$ participants are each given a part of a secret key $K$, called a share [7]. In secret sharing schemes, certain shares may be combined to generate the original secret key $K$. These are referred to as authorised groups. All unauthorised groups will be unable to recover the secret key $K$ [6]. The *access structure* $\Gamma$ defines the set of authorised groups of shares [6]. Throughout this communication, the term *access level* will be used to refer to each minimal authorised group.

A previous secret sharing scheme based on critical sets in Latin squares was proposed by Cooper et al [8]. In this secret sharing scheme, a particular Latin square $K$ of order $n$ is chosen as the secret key. The $k$ shares distributed to participants in this scheme are triples of Ent($K$). The access structure for this scheme is the set $\Gamma = \{S \mid \mathrm{Ent(C)} \subseteq \mathrm{Ent(S)} \subseteq \mathrm{Ent(K)}$, where C is a critical set of K$\}$.

The scheme proposed by Falcón, seeks to extend the scheme proposed by Cooper et al. to $\mathfrak{F}$-critical sets of Latin squares. The secret key for the scheme proposed in [6] is also a Latin square $K$. However, in this scheme there are two types of shares that may be distributed to the $k$ participants of the scheme; a group of the shares will be

autotopisms $\theta \in \mathfrak{F}$, such that $\mathfrak{F} \subseteq \text{Atop}(K)$ and the remaining shares will be triples $T_i \in \text{Ent}(K)$. Formally, the access structure for the scheme is then the set $\Gamma = \{S \mid \text{Ent(C)} \subseteq \text{Ent(S)} \subseteq \text{Ent(K)}, \text{ where C is an } \mathfrak{F}\text{-critical set of K}\}$.

Below, an overview of the scheme proposed in [6] is given:

**Overview of the secret sharing scheme:**

- A Latin Square $K$ of order $n$ is selected as the key for the scheme. The order $n$ of the Latin Square $K$ is made public, whilst $K$ is kept private.
- A set of $T$ triples, where $\text{Ent}(T) \subset \text{Ent}(K)$ is selected, along with a collection of $\mathfrak{F}$ autotopisms associated with $K$.
- The triples of $\text{Ent}(T)$ and autotopisms in $\mathfrak{F}$ associated with $K$ are distributed to the $k$ participants in the secret sharing scheme in such a way that when a group of $t$ participants come together, the union of whose shares form an $\mathfrak{F}$-critical set of $K$. They are thus able to combine their shares in order to find the key $K$.

In [6], Falcón provides an example to accompany the scheme, which demonstrates how the secret sharing scheme may be applied to a particular Latin square of order 6. The example is detailed below.

**Example 1.** *The Latin square K is chosen as the key for the secret sharing scheme, where;*

$$K = \begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 1 & 2 & 0 & 4 & 5 & 3 \\ \hline 2 & 0 & 1 & 5 & 3 & 4 \\ \hline 3 & 4 & 5 & 0 & 1 & 2 \\ \hline 4 & 5 & 3 & 1 & 2 & 0 \\ \hline 5 & 3 & 4 & 2 & 0 & 1 \\ \hline \end{array}$$

The $k$ participants in the scheme will be assigned autotopisms belonging to $\mathfrak{F}$ and triples belonging to a partial Latin square $T$, where $\text{Ent}(T) \subset \text{Ent}(K)$. In this example, the set $\mathfrak{F}$ consists of the four autotopisms $\mathfrak{F}$=$\{\theta_1,\theta_2,\theta_3,\theta_4\}$ associated with the Latin square $K$. These are defined;

$$\begin{aligned} \theta_1 &= ((012)(345),(0)(1)(2)(3)(4)(5),(021)(354)) \\ \theta_2 &= ((0)(1)(2)(3)(4)(5),(012)(345),(021)(354)) \\ \theta_3 &= ((03)(14)(25),(03)(14)(25),(0)(1)(2)(3)(4)(5)) \\ \theta_4 &= ((0)(1)(2)(3)(4)(5),(03)(14)(25),(03)(14)(25)) \end{aligned}$$

There are 11 triples in the partial Latin square $T$. Each triple in the set $T$=$\{T_1,...,T_{11}\}$ is defined;

$$\begin{aligned} T_1 = (0,4;4), T_2 = (1,1;2), T_3 = (1,5;3), T_4 = (2,2;1), T_5 = (2,4;3), T_6 = (3,1;4), T_7 = (3,2;5), T_8 = (3,3;0), \\ T_9 = (4,0;4), T_{10} = (5,3;2), T_{11} = (5,5;1) \end{aligned}$$

The autotopisms and $T$ triples are assigned to participants within the scheme in accordance with Table 1, where Table 1 provides examples of access levels for the autotopisms and $T$ triples given in Example 1. Note that $m$ in Table 1 denotes the number of shares within each access level. There has also been a change in notation from the original example in [6]; the notation $\langle \ldots \rangle$ has been used in Table 1 in place of the notation $\{\ldots\}$. This is to highlight more clearly that the autotopisms in each access level will generate a subgroup of $\text{Atop}(K)$.

**Table 1.** Access level definitions in [6].

| $m$ | Permutations | Triples of $P$ | $m$ | Permutations | Triples of $P$ |
|---|---|---|---|---|---|
| 11 | - | $T$ | 6 | $\{\theta_1,\theta_2\}$ | $\{T_1,T_2,T_6,T_8\}$ |
| 11 | $\langle\theta_4\rangle$ | $T\backslash\{T_9\}$ | 6 | $\langle\theta_1,\theta_4\rangle$ | $\{T_2,T_3,T_7,T_9\}$ |
| 10 | $\langle\theta_3\rangle$ | $T\backslash\{T_1,T_{11}\}$ | 6 | $\langle\theta_2,\theta_3\rangle$ | $\{T_3,T_6,T_8,T_{10}\}$ |
| 10 | $\langle\theta_3,\theta_4\rangle$ | $T\backslash\{T_1,T_9,T_{11}\}$ | 6 | $\langle\theta_1,\theta_3,\theta_4\rangle$ | $\{T_2,T_4,T_8\}$ |
| 9 | $\langle\theta_1\rangle$ | $T\backslash\{T_5,T_7,T_{10}\}$ | 5 | $\langle\theta_1,\theta_2,\theta_3\rangle$ | $\{T_1,T_2\}$ |
| 9 | $\langle\theta_2\rangle$ | $T\backslash\{T_1,T_7,T_{10}\}$ | 5 | $\langle\theta_2,\theta_3,\theta_4\rangle$ | $\{T_1,T_2\}$ |
| 7 | $\langle\theta_1,\theta_3\rangle$ | $\{T_2,T_3,T_4,T_6,T_9\}$ | 5 | $\langle\theta_1,\theta_2,\theta_4\rangle$ | $\{T_2,T_4\}$ |
| 7 | $\langle\theta_2,\theta_4\rangle$ | $\{T_1,T_2,T_4,T_6,T_9\}$ | 5 | $\langle\theta_1,\theta_2,\theta_3,\theta_4\rangle$ | $\{T_1\}$ |

To give an example of how these access levels work; take the set of shares $\theta_3$ and $T\backslash\{T_1,T_{11}\}$. Table 1, shown above, states that the union of $\mathfrak{F}$-orbits for each triple in the set $T\backslash\{T_1,T_{11}\}$, should form an $\mathfrak{F}$-critical set, when $\mathfrak{F}$ is the subgroup of autotopisms generated by $\langle\theta_3\rangle$. The autotopisms within this subgroup are;

$$Id = ((0)(1)(2)(3)(4)(5),(0)(1)(2)(3)(4)(5),(0)(1)(2)(3)(4)(5))$$
$$\theta_3 = ((03)(14)(25),(03)(14)(25),(0)(1)(2)(3)(4)(5))$$

This subgroup of Atop($K$) will generate the following $\mathfrak{F}$-orbits for the shares $T\backslash\{T_1,T_{11}\}$;

$$\begin{gathered}
Orb_{\mathfrak{F}}(T_2) = Orb_{\mathfrak{F}}((1,1;2)) = \{(1,1;2),(4,4;2)\}\\
Orb_{\mathfrak{F}}(T_3) = Orb_{\mathfrak{F}}((1,5;3)) = \{(1,5;3),(4,2;3)\}\\
Orb_{\mathfrak{F}}(T_4) = Orb_{\mathfrak{F}}((2,2;1)) = \{(2,2;1),(5,5;1)\}\\
Orb_{\mathfrak{F}}(T_5) = Orb_{\mathfrak{F}}((2,4;3)) = \{(2,4;3),(5,1;3)\}\\
Orb_{\mathfrak{F}}(T_6) = Orb_{\mathfrak{F}}((3,1;4)) = \{(3,1;4),(0,4;4)\}\\
Orb_{\mathfrak{F}}(T_7) = Orb_{\mathfrak{F}}((3,2;5)) = \{(3,2;5),(0,5;5)\}\\
Orb_{\mathfrak{F}}(T_8) = Orb_{\mathfrak{F}}((3,3;0)) = \{(3,3;0),(0,0;0)\}\\
Orb_{\mathfrak{F}}(T_9) = Orb_{\mathfrak{F}}((4,0;4)) = \{(4,0;4),(1,3;4)\}\\
Orb_{\mathfrak{F}}(T_{10}) = Orb_{\mathfrak{F}}((5,3;2)) = \{(5,3;2),(2,0;2)\}
\end{gathered}$$

$$\mathrm{Ent}(Q_1) = \bigcup_{T_i\in T\backslash\{T_1,T_{11}\}} Orb_{\mathfrak{F}}(T_i).$$

Let $q_1$=Ent($Q_1$) be a partial Latin square, where;

$$q_1 = \begin{array}{|c|c|c|c|c|c|}
\hline
0 & & & & 4 & 5\\ \hline
 & 2 & & 4 & & 3\\ \hline
2 & & 1 & & 3 & \\ \hline
 & 4 & 5 & 0 & & \\ \hline
4 & & 3 & & 2 & \\ \hline
 & 3 & & 2 & & 1\\ \hline
\end{array}$$

Observe that the partial Latin square $q_1$ is uniquely completable, hence applying the subgroup of Atop($K$) generated by $\langle\theta_3\rangle$ to the set of triples $T\backslash\{T_1,T_{11}\}$ will give a uniquely $\mathfrak{F}$-completable set. Notice that the removal of any $\mathfrak{F}$-orbit of Ent($Q_1$) will generate a partial Latin square $q_1$=Ent($Q_1$) that is not uniquely completable to $K$. This demonstrates that $\mathfrak{F}$-orbits of $T\backslash\{T_1,T_{11}\}$ under the autotopism $\theta_3$ form an $\mathfrak{F}$-critical set. As the set is a minimal collection of shares that combine to generate the secret key $K$, it is an access level for the scheme.

## 2. Interesting Observations about Uniquely Completable Partial Latin Squares and the Applications of These Observations to the Example

The Applications of These Observations to the Example in [6], In this section, we will consider further substructures of Latin squares and demonstrate how the existence of these substructures within a Latin square $L$ informs how the $\mathfrak{F}$-critical sets of $L$ may be constructed.

**Definition 3.** *[9] A Latin subsquare of a Latin square is an $m \times m$ submatrix of (not necessarily adjacent) entries that is itself a Latin square. Note that a Latin subsquare has order at least 2.*

**Definition 4.** *[9] An intercalate of order 2 is a Latin subsquare of order 2.*

**Example 2.** *Observe that the four quadrants of the Latin square K given in the example in [6] form four Latin subsquares of order 3, which will form a set $S = \{S_{(0,0)}, S_{(0,3)}, S_{(3,0)}, S_{(3,3)}\}$, where $S_{(i,j)} = \{(i,j;k), (i,j+1;k+1), (i,j+2;k+2), (i+1,j;k+1), (i+1,j+1;k+2), (i+1,j+2;k), (i+2,j;k+2), (i+2,j+1;k), (i+2,j+2;k+1)\}$ for $i,j,k \in \{0,3\}$. There are also nine intercalates of the form $I_{(i,j)} = \{(i,j;k), (i+3,j;k+3), (i,j+3;k+3), (i+3,j+3;k)\}$ for $i,j,k \leq 2$ within K. The set of intercalates will be denoted $I = \{I_{(0,0)}, I_{(0,1)}, I_{(0,2)}, I_{(1,0)}, I_{(1,1)}, I_{(1,2)}, I_{(2,0)}, I_{2,1)}, I_{(2,2)}\}$.*

**Lemma 1.** *All Latin squares of order $n \geq 2$ contain critical sets.*

**Proof.** Let $L$ be a Latin square of order $n \geq 2$. Removing the triple $(i,j;k)$ from $L$ will generate a partial Latin square $P$ in which the cell $(i,j)$ is empty, but all other cells within $P$ are non-empty. Hence, $P$ is a uniquely completable to the Latin square $L$ and $P \subset L$.

The empty partial Latin square $P'$ of order $n \geq 2$ is not uniquely completable to any Latin square of order $n$.

Therefore, every Latin square $L$ of order $n$ contains a non-empty partial Latin square $P$ that is uniquely completable to $L$ and a partial Latin square that is not uniquely completable to $L$. Therefore, there exists a minimal partial Latin square $P^*$ that is uniquely completable to $L$, such that every subset of $P^*$ is not uniquely completable to $L$. Hence, every Latin square of order $n \geq 2$ contains a critical set. □

**Corollary 1.** *For each Latin subsquare $Q$ of order $m \geq 2$ there exists a partial Latin square $A$ such that $A$ is not uniquely completable to $Q$.*

**Proof.** A Latin subsquare $Q$ is a Latin square of order $m$ within a Latin square of order $n$. By Lemma 1, as $Q$ has order $m \geq 2$, it has a critical set and hence there will be some partial Latin square $A$ such that $A$ is not uniquely completable to $Q$. □

**Lemma 2.** *Let $Q$ be a Latin subsquare of order $m \geq 2$ contained within a Latin square $L$ and let $A$ be a partial Latin square that is not uniquely completable to the Latin subsquare $Q$. If a partial Latin square $P$ contains $A$ and no other elements of Ent($Q$), then $P$ will not be uniquely completable to $L$.*

**Proof.** By Corollary 1, every Latin subsquare $Q$ of order $m$, where $|m| \geq 2$, contains a partial Latin square $A$, where $A$ is not uniquely completable to $Q$. Note, when Q is an intercalate, $A$ is the empty partial Latin square. Let $P$ denote a partial Latin square, such that $P \subset L$. If a partial Latin square $P$ contains $A$ and no other triples in Ent($Q$), then the partial Latin square $P$ will not force the entries of the Latin subsquare $Q$. As $Q \subset L$ and the triples of $Q$ are not forced from the triples of $P$, then $P$ is not uniquely completable to $L$. □

Although Lemma 2 does not imply that a partial Latin square $P$ will always be uniquely completable to a Latin square $L$ if it contains a critical set of each Latin subsquare

$Q \in L$, it does imply that if this condition is not met, then $P$ will not be uniquely completable to $L$.

To relate this to $\mathfrak{F}$-critical sets in the example in [6]; if the $\mathfrak{F}$-orbits for some partial Latin square $P$ do not intersect with the critical sets of each Latin subsquare within $S_{(i,j)}$, $I_{(i,j)} \in K$, then the partial Latin square $P$ will not be an $\mathfrak{F}$-critical set of $K$. Example 3 details the more specific implications of Lemma 2 to the example in [6].

**Example 3.** *In [4], it was demonstrated that the critical sets of Latin squares of order 3 either consist of two triples $(i_1, j_1; k_1)$ and $(i_2, j_2; k_2)$, where $i_1 \neq i_2$, $j_1 \neq j_2$ and $k_1 \neq k_2$, or a critical set of a Latin square of order 3 consists of a set of three triples such that each pair of triples in this set share exactly one common ith, jth or kth component. The key observation here is that critical sets of Latin squares of order 3 must contain entries in at least two distinct rows, two distinct columns and the critical sets contain two sets of distinct symbols. By Lemma 2, a partial Latin square P is not uniquely completable to the Latin square K if it does not contain a critical set of each Latin subsquare in K. This implies that if a partial Latin square P does not contain an entry in at least two distinct rows and columns of each order 3 Latin subsquare $S_{i,j} \in K$, or if each of the Latin subsquare $S_{i,j}$ in P does not contain at least two distinct symbols, then P will not be uniquely completable to K.*

*Furthermore, the Latin square K contains nine intercalates, each denoted by $I_{(i,j)}$ for $i, j \leq 2$. Since order 2 Latin squares have a critical set of size 1, if a partial Latin square does not contain at least one entry in each intercalate $I_{(i,j)} \in K$, then P will not be uniquely completable to K.*

## 3. Interesting Observations about the Autotopisms $\theta_1$,$\theta_2$,$\theta_3$ and $\theta_4$ in the Example

Interesting Observations about the Autotopisms $\theta_1$,$\theta_2$,$\theta_3$ and $\theta_4$ in the Example in [6]. Each individual autotopism $\theta \subseteq \text{Atop}(L)$ for some Latin square $L$ will act differently on the triples of $L$. The actions of individual autotopisms on a Latin square $L$ is important in determining the structure of $\mathfrak{F}$-critical sets of $L$. It is therefore worth examining the actions of the individual autotopisms $\theta_1$,$\theta_2$,$\theta_3$,$\theta_4 \subseteq \text{Atop}(K)$, where $K$ is the Latin square in example [6], to determine the structure of each $\mathfrak{F}$-critical set associated with each subgroup of autotopisms in the group Atop($K$).

**Example 4.** *The autotopisms $\theta_1$ and $\theta_2$ permute the elements of some Latin subsquare of order 3 $S_i \in S$ to two other triples within the same Latin subsquare $S_{(i,j)}$. Both $\theta_1$ and $\theta_2$ map each triple $T$ in some intercalate $I_{(i,j)}$ to some intercalate $I_{(i',j')}$, where $I_{(i,j)} \neq I_{(i',j')}$.*

*The autotopisms $\theta_3$ and $\theta_4$ permute the sets {0,3}, {1,4} and {2,5}. They map triples of an intercalate $I_{(i,j)}$ to another triple within the same intercalate, and map triples in a particular Latin subsquare $S_{(i,j)}$ of order three to some Latin subsquare $S_{(i',j')}$ of order three, where $i \neq i'$ and $j \neq j'$.*

## 4. Discussion of Example

Ref [6]. Not all autotopisms listed in example [6] are members of the autotopism group Atop($K$). Further to this, there are some minor errors in the access levels listed in Table 1 in Section 1. Lemma 2 and the observations about the autotopisms discussed in Section 3, make it possible to modify to the example. Each amendment will be discussed in detail within this section.

### *4.1. Discussion Regarding the Autotopisms $\theta_1$ and $\theta_2$*

Discussion Regarding the Autotopisms $\theta_1$ and $\theta_2$ in [6]. The first two modifications are changes to some of the autotopisms associated with the Latin square $K$ in [6]. Two of the autotopisms, $\theta_1$ and $\theta_2$, are not associated with the Latin square $K$. By definition, applying an autotopism to a Latin square that it is associated with should generate another element of that Latin square. However, applying the autotopisms $\theta_1$ and $\theta_2$ to any of the 11 chosen shares from the set $\{T_1,...,T_{11}\}$ does not generate another element of $K$. To demonstrate this, $\theta_1$ and $\theta_2$ are applied to the share $T_1$;

$$T_1 = (0,4;4) \implies \theta_1(T_1) = (1,4;3), \theta_2(T_1) = (0,5;3)$$

Observe, applying $\theta_1$ and $\theta_2$ to $T_1$ does not generate elements of the original Latin square, $L$. Hence, these autotopisms are not associated with Atop($K$). It is believed that the intended autotopisms for $\theta_1$ and $\theta_2$ should be;

$$\theta_1 = ((012)(345), (0)(1)(2)(3)(4)(5), (012)(345))$$
$$\theta_2 = ((0)(1)(2)(3)(4)(5), (012)(345), (012)(345))$$

From this point in the communication, when $\theta_1$ and $\theta_2$ are referred to, they refer to the autotopisms $\theta_1$ and $\theta_2$ given above and not the autotopisms given in [6].

All subsequent suggested amendments focus on the access levels.

*4.2. Discussion Regarding the Access Level for the Autotopisms in the Subgroup $\langle\theta_4\rangle$*

Discussion Regarding the Access Level for the Autotopisms in the Subgroup $\langle\theta_4\rangle$ in [6]. The access level generated by the autotopism subgroup $\langle\theta_4\rangle$ was mis-recorded in [6]. According to the example in [6], combining the subgroup of Atop($K$), $\langle\theta_4\rangle$, with all triples in the set $T\backslash\{T_9\}$ should generate a uniquely completable partial Latin square. However, combining $\langle\theta_4\rangle$ with the stated triples generates the following $\mathfrak{F}$-orbits;

$$Orb_{\mathfrak{F}}(T_1) = Orb_{\mathfrak{F}}((0,4;4)) = \{(0,4;4),(0,1;1)\}$$
$$Orb_{\mathfrak{F}}(T_2) = Orb_{\mathfrak{F}}((1,1;2)) = \{(1,1;2),(1,4;5)\}$$
$$Orb_{\mathfrak{F}}(T_3) = Orb_{\mathfrak{F}}((1,5;3)) = \{(1,5;3),(1,2;0)\}$$
$$Orb_{\mathfrak{F}}(T_4) = Orb_{\mathfrak{F}}((2,2;1)) = \{(2,2;1),(2,5;4)\}$$
$$Orb_{\mathfrak{F}}(T_5) = Orb_{\mathfrak{F}}((0,4;4)) = \{(2,4;3),(2,1;0)\}$$
$$Orb_{\mathfrak{F}}(T_6) = Orb_{\mathfrak{F}}((3,1;4)) = \{(3,1;4),(3,4;1)\}$$
$$Orb_{\mathfrak{F}}(T_7) = Orb_{\mathfrak{F}}((3,1;4)) = \{(3,2;5),(3,5;2)\}$$
$$Orb_{\mathfrak{F}}(T_8) = Orb_{\mathfrak{F}}((3,3;0)) = \{(3,3;0),(3,0;3)\}$$
$$Orb_{\mathfrak{F}}(T_{10}) = Orb_{\mathfrak{F}}((5,3;2)) = \{(5,3;2),(5,0;5)\}$$
$$Orb_{\mathfrak{F}}(T_{11}) = Orb_{\mathfrak{F}}((5,5;1)) = \{(5,5;1),(5,2;4)\}$$

The union of these $\mathfrak{F}$-orbits gives the partial Latin square $P_1$, where;

$$P_1 = \begin{array}{|c|c|c|c|c|c|}\hline * & 1 & * & * & 4 & * \\ \hline * & 2 & 0 & * & 5 & 3 \\ \hline * & 0 & 1 & * & 3 & 4 \\ \hline 3 & 4 & 5 & 0 & 1 & 2 \\ \hline * & * & * & * & * & * \\ \hline 5 & * & 4 & 2 & * & 1 \\ \hline \end{array}$$

This partial Latin square $P_1$ is not uniquely completable as it only uniquely completes to the partial Latin square $P_2$, where;

$$P_2 = \begin{array}{|c|c|c|c|c|c|}\hline 0 & 1 & 2 & 3 & 4 & 5 \\ \hline * & 2 & 0 & * & 5 & 3 \\ \hline 2 & 0 & 1 & 5 & 3 & 4 \\ \hline 3 & 4 & 5 & 0 & 1 & 2 \\ \hline * & 5 & 3 & * & 2 & 0 \\ \hline 5 & 3 & 4 & 2 & 0 & 1 \\ \hline \end{array}$$

Since there are no entries in the intercalate $I_{(1,0)}$, by Lemma 2, $P_2$ is not uniquely completable to $L$. In order for the partial Latin square $P_1$ to be uniquely completable to $L$, the share $T_9$ needs to be included within this access level so that there is an entry in the intercalate $I_{(1,0)}$.

It is also worth noting that $\mathfrak{F}$-critical sets are supposed to be minimal. As $T_1$ and $T_6$ are both members of the intercalate $I_{(0,1)}$ and similarly $T_4$ and $T_{11}$ both belong to the intercalate $I_{(2,2)}$, this set is not minimal. By removing one element of each set $\{T_1, T_6\}$ and $\{T_4, T_{11}\}$, the access level becomes an $\mathfrak{F}$-critical set comprising of nine triples from the set $T$ and the

autotopism $\theta_4$; giving ten individual shares in total. An example of a viable $\mathfrak{F}$-critical set is to take the $\mathfrak{F}$-orbits of the triples $\{T_1, T_2, T_3, T_4, T_5, T_7, T_8, T_9, T_{10}\}$, where $\mathfrak{F}$ is the subgroup of Atop($K$) generated by the autotopism $\theta_4$.

### *4.3. Discussion Regarding the Access Level for the Autotopisms in the Subgroup* $\langle\theta_3, \theta_4\rangle$

Discussion Regarding the Access Level for the Autotopisms in the Subgroup $\langle\theta_3, \theta_4\rangle$ in [6]. Access levels can also be generated by $\mathfrak{F}$-orbits, where $\mathfrak{F}$ is a subgroup of the Atop($K$) generated by more than one autotopism. The first access level to be generated by a set of multiple autotopisms, is the access level generated by the $\mathfrak{F}$-orbits of the subgroup of autotopisms $\langle\theta_3, \theta_4\rangle$. This subgroup consists of the following non-trivial autotopisms;

$$\begin{aligned}
\theta_3 &= ((03)(14)(25), (03)(14)(25), (0)(1)(2)(3)(4)(5))\\
\theta_4 &= ((0)(1)(2)(3)(4)(5), (03)(14)(25), (03)(14)(25))\\
\theta_3\theta_4 &= ((03)(14)(25), (0)(1)(2)(3)(4)(5), (03)(14)(25))
\end{aligned}$$

The example in [6] (see Table 1 in Section 1) suggests that applying this subgroup of Atop($K$) to the set of triples $\{T_2,T_3,T_4,T_5,T_6,T_7,T_8,T_{10}\}$ will generate an $\mathfrak{F}$-critical set. However, when $\mathfrak{F}$ is the subgroup of Atop($K$) generated by $\langle\theta_3, \theta_4\rangle$, the $\mathfrak{F}$-orbits of the set of triples $\{T_2,T_3,T_4,T_5,T_6,T_7,T_8,T_{10}\}$ forms a partial Latin square that is not uniquely completable, as the $\mathfrak{F}$-orbits do not contain an entry in the intercalate $I_{(1,0)}$. As above, if the triple $T_9$ is included within the set of triples for this access level, then the resultant partial Latin square is uniquely completable to the Latin square $K$. However, adding $T_9$ to this set means that this access level consists of nine triples from the set $T$ and both autotopisms $\theta_3$ and $\theta_4$. This gives a total of eleven shares. As previously shown, the $\mathfrak{F}$-orbits of the triples $\{T_2,T_3,T_4,T_5,T_6,T_7,T_8,T_9,T_{10}\}$ under the subgroup of Atop($K$), $\langle\theta_4\rangle$, form an $\mathfrak{F}$-critical set of size 10. Hence, the autotopisms $\langle\theta_3, \theta_4\rangle$ will generate a uniquely $\mathfrak{F}$-completable set that is not minimal, and therefore not an $\mathfrak{F}$-critical set. Therefore, the autotopisms $\theta_3$ and $\theta_4$ cannot be used in combination to generate an access level for this scheme.

### *4.4. Discussion Regarding the Access Level for for the Autotopisms in the Subgroup* $\langle\theta_2, \theta_3, \theta_4\rangle$

Discussion Regarding the Access Level for for the Autotopisms in the Subgroup $\langle\theta_2, \theta_3, \theta_4\rangle$ in [6]. This access level uses the subgroup of Atop($K$) generated by $\langle\theta_2, \theta_3, \theta_4\rangle$. As $\theta_2$ is an autotopism based upon length 3 cycles and $\theta_3$ and $\theta_4$ are based upon length 2 cycles, this subgroup of Atop($K$) consists of eleven non-trivial autotopisms, these autotopisms are;

$$\begin{aligned}
\theta_2 &= ((0)(1)(2)(3)(4)(5), (012)(345), (012)(345))\\
\theta_2\theta_2 &= ((0)(1)(2)(3)(4)(5), (021)(354), (021)(354))\\
\theta_3 &= ((03)(14)(25), (03)(14)(25), (0)(1)(2)(3)(4)(5))\\
\theta_4 &= ((0)(1)(2)(3)(4)(5), (03)(14)(25), (03)(14)(25))\\
\theta_2\theta_3 &= ((03)(14)(25), (042315), (012)(345))\\
\theta_2\theta_2\theta_3 &= ((03)(14)(25), (051324), (021)(354))\\
\theta_2\theta_4 &= ((0)(1)(2)(3)(4)(5), (042315), (042315))\\
\theta_2\theta_2\theta_4 &= ((0)(1)(2)(3)(4)(5), (051324), (051324))\\
\theta_3\theta_4 &= ((03)(14)(25), (0)(1)(2)(3)(4)(5), (03)(14)(25))\\
\theta_2\theta_3\theta_4 &= ((03)(14)(25), (012)(345), (042315))\\
\theta_2\theta_2\theta_3\theta_4 &= ((03)(14)(25), (021)(354), (051324))
\end{aligned}$$

The example in [6] suggests that, when $\mathfrak{F}$ is generated by $\langle\theta_2, \theta_3, \theta_4\rangle$, the union of the $\mathfrak{F}$-orbits $\mathrm{Orb}_{\mathfrak{F}}(T_1)$ and $\mathrm{Orb}_{\mathfrak{F}}(T_2)$ should be uniquely $\mathfrak{F}$-completable to $K$. However, combining these $\mathfrak{F}$-orbits generates the partial Latin square $P_3$, where;

$$P_3 = \begin{array}{|c|c|c|c|c|c|}\hline 0&1&2&3&4&5\\\hline 1&2&0&4&5&3\\\hline *&*&*&*&*&*\\\hline 3&4&5&0&1&2\\\hline 4&5&3&1&2&0\\\hline *&*&*&*&*&*\\\hline\end{array}$$

As the intercalates $I_{(2,0)}$, $I_{(2,1)}$ and $I_{(2,2)}$ are missing from $P_3$, it is not uniquely completable under the autotopism $\theta_2$. A triple present in any one of these intercalates will generate an $\mathfrak{F}$-orbit that spans all three intercalates under the subgroup of Atop($K$) generated by $\langle\theta_2,\theta_3,\theta_4\rangle$. Hence, to make this an access level, one triple from the set $\{T_4, T_5, T_{10}, T_{11}\}$ should be included in the set of triples.

There are multiple $\mathfrak{F}$-critical sets that may be formed using this subgroup of Atop($K$). As discussed in Section 3, each autotopism within the autotopism group Atop($K$) has a unique action. When multiple autotopisms are combined in an $\mathfrak{F}$-critical set, each autotopism generated by the union of any subgroup of autotopisms will also take on a unique action. Observe that in combination, the subgroup of Atop($K$) generated by autotopisms $\langle\theta_3, \theta_4\rangle$ takes a triple $T_i \in I_{(i,j)}$ and maps it to every other triple within the same intercalate. The autotopism subgroup generated by $\langle\theta_2\rangle$ maps each $T_{i'} = (i', j'; k') \in S_{(i,j)}$ to all other triples in the $i'$th row of the Latin subsquare $S_{(i,j)}$. This means that the combined action of the autotopism subgroup generated by $\langle\theta_2, \theta_3, \theta_4\rangle$ takes a triple $T_{i'} \in K$ and maps $T_{i'} = (i', j'; k')$ to all triples in $i'$th and $i' + 3$ mod 6 row of $K$. Hence, any $\mathfrak{F}$-critical set under the subgroup of autotopisms $\langle\theta_2, \theta_3, \theta_4\rangle$ must contain 3 triples, with one triple in either the 0th or 3rd row, one triple in either the 1st or 4th row and finally one triple in either the 2nd or 5th row. This ensures that the $\mathfrak{F}$-orbits contain a critical set of each intercalate $I_{(i,j)}$ and each Latin subsquare $S_{(i,j)}$.

Therefore, exactly one entry must be chosen from each of the following three sets; $\{T_1,T_6,T_7,T_8\}$, $\{T_2,T_3,T_9\}$ and $\{T_4,T_5,T_{10},T_{11}\}$, as each individual set contains all entries of the $i$th and $i + 3$th rows, where $i \leq 2$.

### *4.5. Discussion Regarding the Access Level for for the Autotopisms in the Subgroup $\langle\theta_1, \theta_2, \theta_4\rangle$*

Discussion Regarding the Access Level for for the Autotopisms in the Subgroup $\langle\theta_1, \theta_2, \theta_4\rangle$ in [6]. This access level uses the subgroup of Atop($K$) generated by $\langle\theta_1, \theta_2, \theta_4\rangle$. As $\theta_1$ and $\theta_2$ are both autotopisms based upon length 3 cycles, and $\theta_4$ is an autotopism based upon length 2 cycle; this subgroup of Atop($K$) will consist of 17 non-trivial autotopisms. Example 4 states that autotopism $\theta_1$ maps a triple $T_i \in S_{(i,j)}$, where $T_i = (i, j; k)$ to the other two triples in the $i$th row of the Latin subsquare $S_{(i,j)} \in S$, while the autotopism $\theta_2$ maps each triple $T_i \in S_{(i,j)}$ to the other two triples in the $j$th column of the Latin subsquare $S_{(i,j)} \in S$ and the autotopism $\theta_4$ maps a triple $T_i \in I_{(i,j)}$, where $I_{(i,j)} \in I$, to the triple $I_{(i,j+3)}$mod 6. This means that the subgroup of autotopisms generated by $\theta_1$, $\theta_2$ and $\theta_4$ will map a triple $T_i \in S_{(i,j)}$, for $S_{(i,j)} \in S$ to all other triples in the Latin subsquare $S_{(i,j)}$, as well as all triples in the Latin subsquare $S_{(i,j+3)}$ mod $6 \in S$

The access level in the example in [6] suggests that this subgroup of Atop($K$) should be combined with the triples $\{T_1,T_2\}$ and from here it should be possible to generate the Latin square $L$. However, when $\mathfrak{F}$ is generated by $\langle\theta_1, \theta_2, \theta_4\rangle$, $\mathrm{Orb}_{\mathfrak{F}}(T_1) \cup \mathrm{Orb}_{\mathfrak{F}}(T_2)$ is the partial Latin square $P_4$, where:

$$P_4 = \begin{array}{|c|c|c|c|c|c|}\hline 0&1&2&3&4&5\\\hline 1&2&0&4&5&3\\\hline 2&0&1&5&3&4\\\hline *&*&*&*&*&*\\\hline *&*&*&*&*&*\\\hline *&*&*&*&*&*\\\hline\end{array}$$

The entries of the Latin subsquares $S_{(3,0)}$ and $S_{(3,3)}$ are missing from the partial Latin square $P_4$, hence by Lemma 2, $P_4$ is not uniquely completable to $K$. To amend this access level, either $T_1$ or $T_2$ should be removed and replaced with a triple from the set $\{T_6, T_7, T_8, T_9, T_{10}, T_{11}\}$.

There are multiple pairs of $\mathfrak{F}$-orbits that constitute an $\mathfrak{F}$-critical set when $\mathfrak{F}$ is the subgroup of Atop($K$) generated by $\langle\theta_1, \theta_2, \theta_4\rangle$. As an $\mathfrak{F}$-orbit of a triple $T_i$ under these autotopisms will span two adjacent Latin subsquares $S_{(i,j)}$ and $S_{(i,j+3)}$mod 6, when $T_i \in S_{(i,j)}$ each $\mathfrak{F}$-orbit contains a critical set of each intercalate $I_{(i,j)} \in I$. Therefore, a second $\mathfrak{F}$-orbit is only required to ensure that the union of $\mathfrak{F}$-orbits contains a critical set of the Latin subsquares $S_{(i+3,j)}$mod 6 and $S_{(i+3,j+3)}$mod 6. Hence, any two triples $T_i, T_j \in T$, where $T_i \neq T_j$ will generate an $\mathfrak{F}$-critical set under the autotopisms $\theta_1$,$\theta_2$ and $\theta_4$ providing that if $T_i$ is a triple in some Latin subsquare $S_{(i,j)} \in S$, then the triple $T_j$ is either in the Latin subsquare $S_{(i+3,j)}$ or the Latin subsquare $S_{(i+3,j+3)}$. All triples in the set $\{T_1, T_2, T_3, T_4, T_5\}$ belong either to the Latin subsquare $S_{(0,0)}$ or the Latin subsquare $S_{(0,3)}$, while triples in the set $\{T_6, T_7, T_8, T_9, T_{10}, T_{11}\}$ belong either to the Latin subsquare $S_{(3,0)}$ or the Latin subsquare $S_{(3,3)}$. Therefore, if $T_i \in \{T_1, T_2, T_3, T_4, T_5\}$ and $T_j \in \{T_6, T_7, T_8, T_9, T_{10}, T_{11}\}$ then the union of the $\mathfrak{F}$-orbits $\mathrm{Orb}_{\mathfrak{F}}(T_i) \cup \mathrm{Orb}_{\mathfrak{F}}(T_j)$ will be an $\mathfrak{F}$-critical set, when $\mathfrak{F}$ is generated by $\langle\theta_1, \theta_2, \theta_4\rangle$.

### *4.6. Discussion Regarding the Access Level for the Autotopisms in the Subgroup $\langle\theta_1, \theta_3\rangle$*

Discussion Regarding the Access Level for the Autotopisms in the Subgroup $\langle\theta_1, \theta_3\rangle$ in [6]. Whereas other access levels given in the example in [6] contain too little information, the access level specified for the subgroup of Atop($K$) generated by $\langle\theta_1, \theta_3\rangle$ gives too much information.

The subgroup $\langle\theta_1, \theta_3\rangle$ consists of 5 non-trivial autotopisms, these are autotopisms denoted by; $\theta_1$, $\theta_1\theta_1$, $\theta_3$, $\theta_1\theta_3$ and $\theta_1\theta_1\theta_3$. The example suggests that the $\mathfrak{F}$-orbits, where $\mathfrak{F}$ is generated $\langle\theta_1, \theta_3\rangle$, for the triples {$T_2$,$T_3$,$T_4$,$T_6$,$T_9$} should be an $\mathfrak{F}$-critical set. However, the union $\mathfrak{F}$-orbits of these triples is the partial Latin square $P_5$, where;

$$P_5 = \begin{array}{|c|c|c|c|c|c|}\hline * & 1 & 2 & 3 & 4 & 5 \\ \hline * & 2 & 0 & 4 & 5 & 3 \\ \hline * & 0 & 1 & 5 & 3 & 4 \\ \hline 3 & 4 & 5 & * & 1 & 2 \\ \hline 4 & 5 & 3 & * & 2 & 0 \\ \hline 5 & 3 & 4 & * & 0 & 1 \\ \hline \end{array}$$

Observe that $P_5$ is uniquely completable to $L$, however, access levels are supposed to provide the minimal amount of information required to generate the original key. Note that if either one of the shares $T_3$ or $T_6$ were to be removed from this access level, then one is still able to generate a uniquely $\mathfrak{F}$-completable partial Latin square, hence the specified set of triples is not an $\mathfrak{F}$-critical set when $\mathfrak{F}$ is generated by $\langle\theta_1, \theta_3\rangle$. To amend this, each access level should be defined in such a way that only one triple from the set $\{T_3, T_6\}$ is included.

### *4.7. Summary of Findings*

The above subsections discuss amendments to particular errors in the example in [6].

Following this, it is possible to generalise sets of triples of $T$ that can be combined with each possible subgroup of the autotopism group Atop($K$) generated by some collection of the autotopisms $\theta_1$, $\theta_2$, $\theta_3$ and $\theta_4$. Using the results discussed in Sections 2 and 3, it is possible to generalise combinations of triples that form $\mathfrak{F}$-critical sets under the subgroups of Atop($K$) defined by the autotopisms $\theta_1$, $\theta_2$, $\theta_3$ and $\theta_4$. Table A1 in Appendix A details the combinations of triples that will generate a $\mathfrak{F}$-critical set when combined with the autotopisms stated in the same row of the table. Reasoning behind the constructions of certain $\mathfrak{F}$-critical sets in Table A1 in Appendix A is outlined in Section 4. Table A2 in

Appendix A provides an example of an $\mathfrak{F}$-critical set for each subgroup of autotopisms generated by elements of the set $\{\theta_1, \theta_2, \theta_3, \theta_4\}$.

## 5. Conclusions

In this correspondence, minor errors in the original definitions of the $\mathfrak{F}$-critical sets detailed within the paper [6] are amended. The importance of Lemma 2 in determining both critical sets and $\mathfrak{F}$-critical sets within a Latin square is highlighted.

Lemma 2 states that if a partial Latin square $P$ does not contain a critical set for each Latin subsquare $Q \in L$, where $L$ is a Latin square, $P$ is not be uniquely completable to $L$. Further, let a partial Latin square $P \subset L$, where $L$ is a Latin square and let $\mathfrak{F}$ denote a subgroup of the autotopism group of $L$. If the $\mathfrak{F}$-orbits of a partial Latin square $P$, do not contain a critical set for each Latin subsquare $Q \in L$, then the combination of these triples and autotopisms do not form an $\mathfrak{F}$-critical set. Lemma 2 can therefore be used to eliminate several partial Latin squares that are not $\mathfrak{F}$-critical sets of a Latin square $L$.

By considering $\mathfrak{F}$-orbits that satisfy Lemma 2, $\mathfrak{F}$-critical sets of a Latin square $K$ can be generated, where:

$$K = \begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 1 & 2 & 0 & 4 & 5 & 3 \\ \hline 2 & 0 & 1 & 5 & 3 & 4 \\ \hline 3 & 4 & 5 & 0 & 1 & 2 \\ \hline 4 & 5 & 3 & 1 & 2 & 0 \\ \hline 5 & 3 & 4 & 2 & 0 & 1 \\ \hline \end{array}$$

The $\mathfrak{F}$-critical sets detailed within the correspondence use subgroups of the autotopism group of $K$ to generate all possible combinations of the autotopisms $\theta_1$, $\theta_2$, $\theta_3$ and $\theta_4$, where;

$$\begin{aligned} \theta_1 &= ((012)(345), (0)(1)(2)(3)(4)(5), (012)(345)) \\ \theta_2 &= ((0)(1)(2)(3)(4)(5), (012)(345), (012)(345)) \\ \theta_3 &= ((03)(14)(25), (03)(14)(25), (0)(1)(2)(3)(4)(5)) \\ \theta_4 &= ((0)(1)(2)(3)(4)(5), (03)(14)(25), (03)(14)(25)) \end{aligned}$$

The $\mathfrak{F}$-critical sets generated by the $\mathfrak{F}$-orbits of the triples (0,4;4),(1,1;2),(1,5;3),(2,2;1), (2,4;3),(3,1;4),(3,2;5), (3,3;0),(4,0;4),(5,3;2),(5,5;1) $\subseteq$ Ent($K$) are listed in Table A1 of Appendix A. For comparison, the suggested $\mathfrak{F}$-critical sets for the example in [6] are listed in Table 1 in Section 1.

If a partial Latin square $P$ satisfies Lemma 2, this does not guarantee that $P$ is uniquely completable to a Latin square $L$; however, Lemma 2 does provide a necessary condition, that if not met, means a partial Latin square $P$ is not uniquely completable. Lemma 2 can then be applied to all partial Latin squares $P$ of order $n$. In other words, by looking at all Latin subsquares of order $m$ within a Latin square $L$ of order $n$, where $m < n$, one can ascertain the critical sets of each Latin subsquare $Q$ within $L$. Each partial Latin square $P$ that is uniquely completable to $L$ then contains some combination of critical sets of Latin subsquares of $L$, hence by determining the Latin subsquares of $L$, the problem of generating the critical sets of $L$ is reduced in size. This approach may similarly be applied to $\theta$-critical sets or $\mathfrak{F}$-critical sets.

Further work is needed to determine necessary conditions for ensuring that a partial Latin square $P$ is a critical set of a Latin square $L$, but by the application of Lemma 2, it may be possible for larger Latin squares of order $n$ to be analysed.

**Author Contributions:** This short communication was written as part of an MMath research project at the University of South Wales undertaken by L.M.J. and supervised by S.P. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** We would like to thank Raul Falcón for his advice about the original example, as well as his help with proof reading.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A

Table A1 details the newly defined access levels, generated by results in this communication. Note that $m$ the number of individual shares in each access level.

Observe, that the access level defined by the autotopisms $\langle \theta_3, \theta_4 \rangle$ has been removed from Table A1, as it is shown that these autotopisms cannot form an $\mathfrak{F}$-critical set.

Table A2 gives specific examples of $\mathfrak{F}$-critical sets for the Latin square $K$ under the autotopisms $\{\theta_1, \theta_2, \theta_3, \theta_4\}$. Each $\mathfrak{F}$-critical set is constructed in accordance with the specifications of Table A1.

**Table A1.** Redefined access levels based upon results of this communication.

| $m$ | Permutations | Triples of $P$ |
|---|---|---|
| 11 | - | T |
| 10 | $\langle \theta_3 \rangle$ | $T$ exluding one entry from each of the sets $\{T_1,T_6\}$ and $\{T_4,T_{11}\}$ |
| 10 | $\langle \theta_4 \rangle$ | $T$ exluding one entry from each of the sets $\{T_1,T_6\}$ and $\{T_4,T_{11}\}$ |
| 9 | $\langle \theta_1 \rangle$ | $T$ excluding one entry from each of the sets $\{T_1,T_5\}$, $\{T_8,T_{10}\}$ and $\{T_6,T_7,T_9\}$ |
| 9 | $\langle \theta_2 \rangle$ | $T$ excluding one entry from each of the sets $\{T_6,T_7\}$, $\{T_{10},T_{11}\}$ and $\{T_1,T_3,T_5\}$ |
| 7 | $\langle \theta_2, \theta_4 \rangle$ | Exactly one entry from five out of the following six sets; $\{T_1\}$,$\{T_2,T_3\}$,$\{T_4,T_5\}$, $\{T_6,T_7,T_8\}$,$\{T_9\}$,$\{T_{10},T_{11}\}$ |
| 6 | $\langle \theta_1, \theta_3 \rangle$ | To ensure that two distinct columns of $S_{(0,3)}$ and $S_{(3,0)}$ contain two entries, one triple should be selected from two of the following three sets $\{T_1, T_5, T_6\}, \{T_3, T_7\}, \{T_9\}$, to ensure two distinct columns of $S_{(0,0)}$ and $S_{(3,3)}$ contain entries, two of the three sets; $\{T_2\}, \{T_4, T_{11}\}, \{T_8, T_{10}\}$ should be selected. To ensure each intercalate contains at least one entry, at least one element from the following sets should be chosen; $\{T_1, T_2, T_5, T_6\}, \{T_3, T_4, T_7, T_{11}\}, \{T_8, T_9, T_{10}\}$ |
| 6 | $\langle \theta_1, \theta_2 \rangle$ | Exactly one entry should be chosen from each of the sets $\{T_1,T_3,T_5\}$, $\{T_2,T_4\}$, $\{T_6,T_7,T_9\}$ and $\{T_8,T_{10},T_{11}\}$. |
| 6 | $\langle \theta_1, \theta_4 \rangle$ | To ensure that two distinct columns of $S_{(0,0)}$ and $S_{(0,3)}$ contain entries, one triple should be selected from both of the following sets $\{T_1, T_2, T_5\}, \{T_3, T_4\}$, to ensure two distinct columns of $S_{(0,0)}$ and $S_{(3,3)}$ contain entries, one entry from two of the sets; $\{T_6\}, \{T_7, T_{11}\}, \{T_8, T_9, T_{10}\}$ should be selected. To ensure each intercalate contains at least one entry, at least one element from the following sets should be chosen; $\{T_1, T_2, T_5, T_6\}, \{T_3, T_4, T_7, T_{11}\}, \{T_8, T_9, T_{10}\}$ |
| 6 | $\langle \theta_2, \theta_3 \rangle$ | To ensure that two distinct columns of $S_{(0,3)}$ and $S_{(3,0)}$ contain entries, one triple should be selected from two of the following three sets $\{T_1,T_6,T_7\}$ $\{T_3,T_9\}$, $\{T_5\}$, to ensure two distinct columns of $S_{(0,0)}$ and $S_{(3,3)}$ contain entries, two of the three sets; $\{T_2\}$ $\{T_4,T_{10},T_{11}\}$, $\{T_8\}$ should be selected. To ensure each intercalate contains at least one entry, at least one element from the following sets should be chosen; $\{T_1, T_6, T_7, T_8\}, \{T_2, T_3, T_9\}$,$\{T_4, T_5, T_{10}, T_{11}\}$ |
| 6 | $\langle \theta_1,\theta_3,\theta_4 \rangle$ | One entry from each of the sets $\{T_1,T_2,T_5,T_6\}$, $\{T_3,T_4,T_7,T_{11}\}$ and $\{T_8,T_9,T_{10}\}$ |
| 6 | $\langle \theta_2,\theta_3,\theta_4 \rangle$ | One entry from each of the sets $\{T_1,T_6,T_7,T_8\}$, $\{T_2,T_3,T_9\}$ and $\{T_4,T_5,T_{10},T_{11}\}$ |
| 5 | $\langle \theta_1, \theta_2, \theta_3 \rangle$ | One entry from each of the sets $\{T_1,T_3,T_5,T_6,T_7,T_9\}$ and $\{T_2,T_4,T_8,T_{10},T_{11}\}$ |
| 5 | $\langle \theta_1, \theta_2, \theta_4 \rangle$ | One entry from each of the sets $\{T_1,T_2,T_3,T_4,T_5\}$ and $\{T_6,T_7,T_8,T_9,T_{10},T_{11}\}$ |
| 5 | $\langle \theta_1, \theta_2, \theta_3, \theta_4 \rangle$ | One share of $T$ |

**Table A2.** Examples of access levels as outlined in Table A1.

| $m$ | Permutations | Triples of $P$ | $m$ | Permutations | Triples of $P$ |
|---|---|---|---|---|---|
| 11 | - | T | 6 | $\langle\theta_1,\theta_4\rangle$ | $\{T_1,T_4,T_6,T_{10}\}$ |
| 10 | $\langle\theta_3\rangle$ | $T\backslash\{T_1,T_4\}$ | 6 | $\langle\theta_2,\theta_3\rangle$ | $\{T_1,T_2,T_9,T_{10}\}$ |
| 10 | $\langle\theta_4\rangle$ | $T\backslash\{T_6,T_{11}\}$ | 6 | $\langle\theta_1,\theta_3,\theta_4\rangle$ | $\{T_1,T_3,T_{10}\}$ |
| 9 | $\langle\theta_1\rangle$ | $T\backslash\{T_5,T_7,T_{10}\}$ | 6 | $\langle\theta_2,\theta_3,\theta_4\rangle$ | $\{T_1,T_2,T_4\}$ |
| 9 | $\langle\theta_2\rangle$ | $T\backslash\{T_5,T_6,T_{11}\}$ | 5 | $\langle\theta_1,\theta_2,\theta_3\rangle$ | $\{T_1,T_2\}$ |
| 7 | $\langle\theta_2,\theta_4\rangle$ | $\{T_1,T_2,T_4,T_6,T_9\}$ | 5 | $\langle\theta_1,\theta_2,\theta_4\rangle$ | $\{T_1,T_6\}$ |
| 6 | $\langle\theta_1,\theta_3\rangle$ | $\{T_1,T_3,T_4,T_8\}$ | 5 | $\langle\theta_1,\theta_2,\theta_3,\theta_4\rangle$ | $\{T_7\}$ |
| 6 | $\langle\theta_1,\theta_2\rangle$ | $\{T_1,T_2,T_6,T_8\}$ | | | |

## References


1. Laywine, C.F.; Mullen, G.L. *Discrete Mathematics Using Latin Squares*; Wiley-Interscience: New York, NY, USA, 1998.
2. Dénes, J.; Keedwell, A.D. *Latin Squares and Their Applications*; English Universities Press Limited Ltd.: London, UK, 1974.
3. Burton, B.A. Completion of Partial Latin Squares. Ph.D. Thesis, University of Queensland, Brisbane, Australia, 1996.
4. Falcón, R.M.; Johnson, L.; Perkins, S. A census of critical sets based on non-trivial autotopisms of Latin squares of order up to five. *AIMS Math.* **2020**, *6*, 261–295. [CrossRef]
5. Olsson, C. Discreet Discrete Mathematics: Secret Communication Using Latin Squares and Quasigroups. Independent Bachelor Thesis, Umeå University, Umeå, Sweden, 2017.
6. Falcón, R. Latin squares associated to principal autotopisms of long cycles. Applications in cryptography. In *Proceedings of Transgressive Computing 2006: A Conference in Honor of Jean Della Dora*; Universidad de Granada: Granada, Spain, 2006; pp. 213–230.
7. Piper, F.; Murphy, S. *Cryptography A Very Short Introduction*; Oxford University Press Inc.: New York, NY, USA, 2002.
8. Cooper, J.; Donovan, D.; Seberry, J. Secret Sharing Schemes Arising From Latin Squares. *Bull. ICA* **1994**, *12*, 33–43.
9. Wanless, I.M. Latin squares with one subsquare. *J. Comb. Des.* **2001**, *9*, 128–146. [CrossRef]