1 Outline of the Document

We will take bottom-up approach to construct the d-dimensional Latin square with desired property. We will first define what is a 2-dimensional Latin square, and pose some restrictions on it to make it 'cryptographically secure'. We then extend the notion to higher dimensions and prove that our construction satisfies the properties we want.

2 The 2-dimensional Case

Definition 1 *Let $\mathcal{K} = \{1, 2, \ldots, k\}$. A $k \times k$ square L with entries taking value from $\mathcal{K}$ is called a k by k Latin square if:*

1. *$L(i, j) \neq L(i, k)$ for all $j \neq k$,*
2. *$L(i, j) \neq L(k, j)$ for all $i \neq k$.*

Definition 2 *Let σ_1, σ_2 be permutation on $\mathcal{K}$ with order k. We say that k by k Latin square L is (σ_1, σ_2)-permutable if for all $i, j \in \mathcal{K}$, $L(i, j) = L(\sigma_1(i), \sigma_2(j))$*

Example 1 *Consider a 4 by 4 Latin square L (with indexing) as below:*

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Let $\sigma_1 = (1\ 3\ 4\ 2)$ and $\sigma_2 = (1\ 2\ 4\ 3)$. Then L is (σ_1, σ_2)-permutable. To see this visually, $L(\sigma_1(i), \sigma_2(j))$ is:

	3	1	4	2
2	1	2	3	4
4	2	4	1	3
1	3	1	4	2
3	4	3	2	1

In fact, as soon as we know L is (σ_1, σ_2)-permutable for some σ_1, σ_2 of order k, we know that L is (σ_1^l, σ_2^l)-permutable for all $l \in \{1, \ldots, k-1\}$. We formalise the statement in the following lemma.

Lemma 1 *Let L be a k by k (σ_1, σ_2)-permutable Latin square, with $ord(\sigma_1) = ord(\sigma_2) = k$. Then L is (σ_1^l, σ_2^l)-permutable for all $l \in \{1, \ldots, k-1\}$.*

Proof: We prove the statement by induction on i. The proposition is trivially true for $l = 1$, so the base case is verified. Now we assume that the proposition is true for some arbitrary l, and try to show that it is true for $l + 1$.

By definition, L is (σ_1^l, σ_2^l)-permutable means $L(i, j) = L(\sigma_1^l(i), \sigma_2^l(j))$ for all $i, j \in \mathcal{K}$. The same result holds if we apply σ_1 and σ_2 to indices on both sides, i.e. $L(\sigma_1(i), \sigma_2(j)) = L(\sigma_1^{l+1}(i), \sigma_2^{l+1}(j))$ for all $i, j \in \mathcal{K}$. But

by assumption, we know that $L(i,j) = L(\sigma_1(i), \sigma_2(j))$ for all $i, j \in \mathcal{K}$, so $L(i,j) = L(\sigma_1^{l+1}(i), \sigma_2^{l+1}(j))$ for all $i, j \in \mathcal{K}$. $\square$

The property in lemma 1 ensures indistinguishability of row and column indices because there are k different configurations that gives the same Latin square. In particular, each row index can be assigned to any other row index and we still obtain the same Latin square, so no one can guess the correct row index with probability higher than $1/k$ if he is given the Latin square without the indices.

3 Generalization to Higher Dimensions