# A Note on the Quasigroup Lai-Massey Structures

George Teşeleanu[1,2]

[1] Advanced Technologies Institute
10 Dinu Vintilă, Bucharest, Romania
`tgeorge@dcti.ro`
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy
21 Calea Grivitei, Bucharest, Romania

**Abstract.** In our paper, we explore the consequences of replacing the commutative group operation used in Lai-Massey structures with a quasigroup operation. We introduce four quasigroup versions of the Lai-Massey structure, and prove that for quasigroups isotopic with a group $\mathbb{G}$, the complexity of launching a differential attack against these variants of the Lai-Massey structure is equivalent to attacking an alternative structure based on $\mathbb{G}$. Then we provide the conditions needed for correct decryption, and further refine the resulting structure. The emerging structure is both intriguing and novel, and we hope that it will form the basis for future secure block ciphers based on non-commutative groups. In the case of commutative groups, we show that the resulting structure reduces to the classical Lai-Massey structure.

## 1 Introduction

When developing a block cipher, a key challenge is to design a set of permutations that is both easily implementable and exhibits behavior akin to random permutations. In tackling this challenge, the literature presents three primary approaches [40]. The first approach involves substitution-permutation networks (SPNs), which create a large block random looking permutation by employing a series of substitution layers[3] and permutation layers iterated over multiple rounds. On the other hand, Feistel and Lai-Massey structures adopt a different strategy. Instead of relying on invertible building blocks, these structures construct permutations using non-invertible components.

Differential cryptanalysis, introduced by Biham and Shamir [3], stands out as one of the most efficient tools for attacking block ciphers [21]. This method exploits how changes in certain plaintext bits propagate to the corresponding ciphertext, aiming to uncover vulnerabilities in the encryption process. In an ideal scenario with truly random permutations, the probability of predicting these changes is precisely $1/2^n$, where $n$ denotes the number of input bits. For instance, if $n$ is set to 128 bits, this probability would be negligible, rendering

---

[3] composed of several substitution boxes (s-boxes) with a small block length

predictions practically infeasible. However, the challenge lies in the need for practical block ciphers where permutations can be easily described, a criterion not satisfied by ideal permutations.

To overcome this hurdle, designers often resort to theoretical estimates based on assumptions that might not always align with real-world conditions. Consequently, practical block ciphers deviate from the ideal, rendering them susceptible to differential cryptanalysis. Hence, guarding against this type of attack becomes a fundamental design criterion for ensuring the security of symmetric primitives [28].

Latin squares, defined as $\ell \times \ell$ matrices containing only $\ell$ symbols, possess the distinctive property that each symbol appears exactly once in every row and column [11]. When a set is equipped with a multiplication table that forms a Latin square, it establishes a quasigroup, a structure akin to a group but without the requirements of associativity and the presence of an identity element.

Despite quasigroups not being a prevalent choice in constructing cryptographic primitives, the literature showcases various designs based on these structures [1, 2, 8, 9, 12, 16, 17, 22, 23]. These cryptosystems highlight the versatility of quasigroups as group-like structures, offering an alternative perspective for certain cryptographic applications.

A recent approach, as highlighted in [4–6, 10], employs commutative regular subgroups within the symmetric group to design SPN structures that exhibit resilience against classical differential cryptanalysis. However, these structures have a vulnerability to a differential attack utilizing a different group operation. Specifically, the security level of such structures against differential attacks is operation-dependent, indicating a variation in susceptibility based on the chosen operation. This approach is similar to the methodology employed in our paper, where we also explore different operations for constructing differential attacks against the proposed Lai-Massey structures. It is worth noting that the focus of [4–6, 10] is to illustrate how a designer can embed a trapdoor into a symmetric structure, defined by knowledge of the weakening group operation. In contrast, our investigation aims to explore the potential strengthening of an Lai-Massey structure against differential cryptanalysis by changing the group operation to a quasigroup one.

In [36–38], the author proposes a direct extension of the three fundamental symmetric structures[4] by using quasigroup operations instead of traditional group operations between keys and (intermediary) plaintexts. The study focuses on quasigroup operations isotopic with a group operation, a popular method for constructing quasigroups. We further discuss only the results concerning Lai-Massey structures, since this is the focus of our paper. In [38], the author begins by establishing the necessary conditions for correct decryption when employing a quasigroup operation. Unfortunately, the previous conditions limit the generalization of the Lai-Massey structure solely to non-commutative groups. Then two structure categories are presented, one symmetric and one asymmetric. Sub-

---

[4] SPNs, Feistel, and Lai-Massey

sequently, the author employs several arguments to prove the equivalence of the two categories in terms of differential cryptanalysis.

In this paper, we study the quasigroup Lai-Massey structure from a different perspective. We commence by generalizing the structures outlined in [38], subsequently delving into the security analysis of the derived structures, and ultimately focusing on the necessary conditions needed for correct decryption. We managed to prove that the symmetric and asymmetric structures are differentially equivalent, and thus we only need to focus only on one of them. In the non-commutative group case, we obtain a novel symmetric structure that generalizes the symmetric structure from [38]. To the best of the authors' knowledge, this particular design has not been previously documented in the existing literature. Consequently, we believe that this structure warrants attention for future research, offering valuable insights from both theoretical and design perspectives.

In the case of commutative groups, the structure coincides with the classical Lai-Massey symmetric structure. Therefore, in this case we obtain a negative result. Nevertheless, we believe its significance is twofold.

1. In the majority of scientific reports and papers, authors often depict their results as if they were achieved seamlessly, without acknowledging the intricacies and challenges encountered during the process. This tendency contributes to a skewed perception of scientific research [19,27,34,42] and fosters the misconception that failure, serendipity, and unexpected outcomes are not integral aspects of scientific endeavors [19,32]. Consequently, our report aims to provide readers with insight into the authentic processes involved in the design phase of a cryptographic primitive.
2. Negative results and misguided directions are frequently underreported in the scientific literature [19, 39], leading to the risk of repeated errors. By sharing our findings, we aspire to prevent others from traversing similar unproductive paths, thereby contributing to a collective learning process. This approach aligns with the recommendation in [35], where the author advises documenting mistakes to avoid their recurrence in the future.

*Structure of the paper.* We introduce notations and definitions in Section 2. A generic Lai-Massey structure in introduced in Section 3 and its security is analyzed. We conclude in Section 4.

## 2    Preliminaries

*Notations.* Throughout the paper $|\mathbb{G}|$ will denote the cardinality of set $\mathbb{G}$ and $\oplus$ the bitwise xor operation. Also, by $x\|y$ we understand the concatenation of the strings $x$ and $y$ and by $\mathbb{G}^2$ the set $\{x\|y \mid x, y \in \mathbb{G}\}$. When defining a permutation $\pi$ we further use the shorthand $\pi = \{a_0, a_1, \ldots, a_\ell\}$ which translates into $\pi(i) = a_i$ for all $i$ values. We also define the identity permutation $Id = \{0, \ldots, \ell\}$. Let $\bullet$ and $\lhd$ be binary operators. We define the binary operators $\Delta_\bullet(X, Y) = X \bullet Y$ and $\Delta_{\bullet,\lhd}(X_0\|X_1, Y_0\|Y_1) = (X_0 \bullet Y_0, X_1 \lhd Y_1)$. Let $X \in \mathbb{G}^2$. By $X_l$ and $X_r$ we understand the left and, respectively, right half of $X$.

## 2.1 Quasigroups

In this section we introduce a few basic notions about quasigroups. We base our exposition on [33].

**Definition 1.** *A quasigroup $(\mathbb{G}, \otimes)$ is a set $\mathbb{G}$ equipped with a binary operation of multiplication $\otimes : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$, in which specification of any two of the values $x, y, z$ in the equation $x \otimes y = z$ determines the third uniquely.*

**Definition 2.** *For a quasigroup $(\mathbb{G}, \otimes)$ we define the left division $x \oslash z = y$ as the unique solution $y$ to $x \otimes y = z$. Similarly, we define the right division $z \oslash y = x$ as the unique solution $x$ to $x \otimes y = z$.*

**Lemma 1.** *The following identities hold*

$$y \oslash (y \otimes x) = x, \qquad\qquad (x \otimes y) \oslash y = x,$$
$$y \otimes (y \oslash x) = x, \qquad\qquad (x \oslash y) \otimes y = x.$$

**Lemma 2.** *If $(\mathbb{G}, \otimes)$ is a group then $x \oslash z = x^{-1} \otimes z$ and $z \oslash y = z \otimes y^{-1}$.*

One common approach for constructing quasigroups [16, 17, 22, 41] involves the following procedure. A group $(\mathbb{G}, \star)$, such as $(\mathbb{Z}_{2^n}, \oplus)$ or $(\mathbb{Z}_{2^n}, +)$, and three random permutations $\pi, \rho, \omega : \mathbb{G} \to \mathbb{G}$ are chosen. Subsequently, we define the quasigroup operation as $x \otimes y = \omega^{-1}(\pi(x) \star \rho(y))$. To understand why this leads to a quasigroup, observe that the mappings of $x$, $y$, and $z$ to $\pi(x)$, $\rho(y)$, and $\omega(z)$ are unique. Consequently, any equation of the form $\pi(x) \star \rho(y) = \omega(z)$ is uniquely resolved in the base group $\mathbb{G}$ when provided with any of $\pi(x)$, $\rho(y)$, or $\omega(z)$.

**Definition 3.** *Let $(\mathbb{G}, \otimes)$, $(\mathbb{H}, \star)$ be two quasigroups. An ordered triple of bijections $\pi$, $\rho$, $\omega$ of a set $\mathbb{G}$ onto the set $\mathbb{H}$ is called an isotopy of $(\mathbb{G}, \otimes)$ to $(\mathbb{H}, \star)$ if for any $x, y \in \mathbb{G}$ $\pi(x) \star \rho(y) = \omega(x \otimes y)$. If such an isotopism exists, then $(\mathbb{G}, \otimes)$, $(\mathbb{H}, \star)$ are called isotopic.*

*Example 1.* Let $(\mathbb{G}, \star) = (\mathbb{Z}_4, \oplus)$, $\omega^{-1} = \{2, 1, 0, 3\}$, $\pi = \{2, 1, 3, 0\}$ and $\rho = \{2, 0, 3, 1\}$. The corresponding quasigroup operations for $(\mathbb{Z}_4, \otimes)$ can be found in Table 1. [36]

| $\otimes$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 2 | 0 | 1 | 3 |
| 1 | 3 | 1 | 0 | 2 |
| 2 | 1 | 3 | 2 | 0 |
| 3 | 0 | 2 | 3 | 1 |

| $\oslash$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 2 | 0 | 3 |
| 1 | 2 | 1 | 3 | 0 |
| 2 | 3 | 0 | 2 | 1 |
| 3 | 0 | 3 | 1 | 2 |

| $\oslash$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 3 | 0 | 1 | 2 |
| 1 | 2 | 1 | 0 | 3 |
| 2 | 0 | 3 | 2 | 1 |
| 3 | 1 | 2 | 3 | 0 |

Table 1: Quasigroup operations.

*Example 2.* Let $(\mathbb{G}, \star) = (\mathbb{Z}_n, -)$. Then $\mathbb{G}$ is isotopic with $(\mathbb{Z}_n, +)$, where $\omega, \pi = Id$ and $\rho(i) = n - i \bmod n$. [41]

To gain a deeper understanding of the concept of isotopy, it is helpful to note that its three permutations correspond to the permutation of rows, columns, and symbols within a Latin square. These permutations naturally lead to the creation of another Latin square. Notably, being isotopic establishes an equivalence relation among quasigroups but not among groups, as isotopisms do not generally preserve associativity. It is important to recall that every group is an associative quasigroup.

Note that counting the number of distinct Latin squares is challenging. More precisely, the exact number, together with that of their isotopism classes, is known only for Latin squares of order smaller or equal to 11 [20, 25, 26].

### 2.2 Group Differential Cryptanalysis

Differential cryptanalysis was introduced by Biham and Shamir in [3] for analysing the Data Encryption Standard, and as such, it was formulated exclusively for the group $(\mathbb{Z}_{2^n}, \oplus)$. Subsequently, the concept was generalized to commutative groups [24], non-commutative groups [36] and quasigroups [36–38]. Let $(\mathbb{G}, \star)$ be a group. We further present the notions of left and right differential probabilities for a permutation. Remark that these notions can also be defined for functions.

**Definition 4.** *Let* $\Delta_\star(X, X') = X \star X'$, *where* $X, X' \in (\mathbb{G}, \star)$. *We define the group differential probabilities*

$$LDP_\star(\sigma, \alpha, \beta) = \frac{1}{|\mathbb{G}|} \sum_{\substack{X, X' \in \mathbb{G} \\ \Delta_\star(X^{-1}, X') = \alpha}} [\Delta_\star(\sigma(X)^{-1}, \sigma(X')) = \beta]$$

$$RDP_\star(\sigma, \alpha, \beta) = \frac{1}{|\mathbb{G}|} \sum_{\substack{X, X' \in \mathbb{G} \\ \Delta_\star(X, X'^{-1}) = \alpha}} [\Delta_\star(\sigma(X), \sigma(X')^{-1}) = \beta].$$

*where* $\sigma : \mathbb{G} \to \mathbb{G}$ *is a permutation and* $\alpha, \beta \in \mathbb{G}$. *When* $(G, \star)$ *is commutative, we simply refer to* $LDP$ *and* $RDP$ *as* $DP$.

*Remark 1.* Let $\sigma$ be randomly chosen. When $(\mathbb{G}, \star) = (\mathbb{Z}_{2^n}, \star)$, the distribution of $DP$ values is studied in [30, 31] and when $(\mathbb{G}, \star)$ is a generic abelian group in [18]. When $\sigma$ is static[5], the distribution of $DP$s for $(\mathbb{Z}_{2^n}, \oplus)$ is studied for example in [7, 13, 29].

## 3 Lai-Massey Structure

### 3.1 Description

We further present two non-commutative versions of the Lai-Massey structure: a symmetric construction Figure 1a and an asymmetric one Figure 1b. Note that, as mentioned in Section 1, we currently do not focus on their invertibility.

---

[5] *i.e* fixed and public for all symmetric structure's implementations

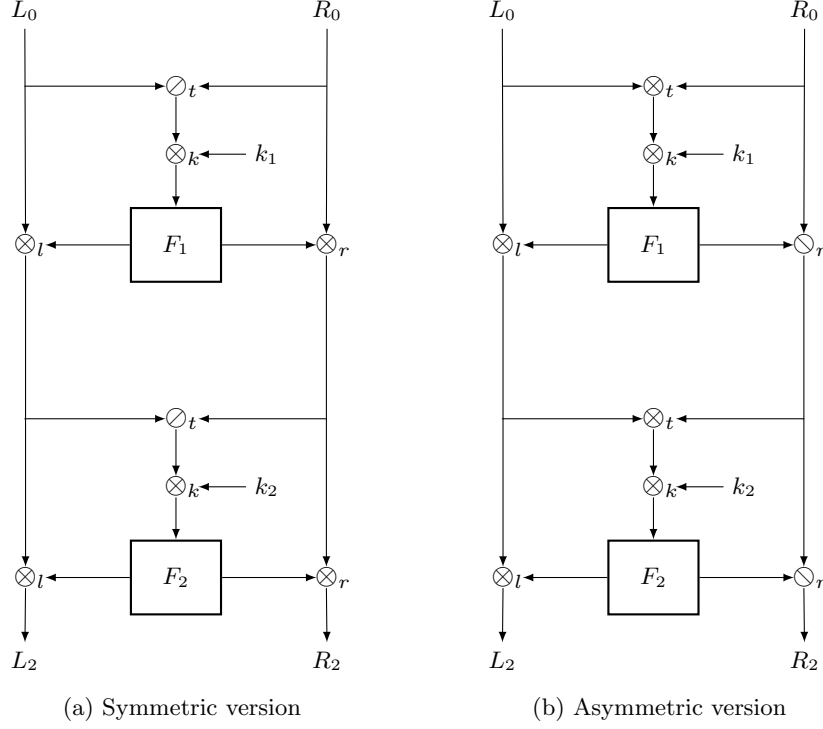(a) Symmetric version        (b) Asymmetric version

Fig. 1: Quasigroup Lai-Massey structures

In both constructions the first step is to parse the plaintext into two halves $L_0$ and $R_0$. Note that for all versions, we make use of four quasigroup operation defined on $\mathbb{G}$ indexed by $t$ - top, $l$ - left, $r$ - right and $k$ - key, which are not necessary distinct. In the symmetric case, for $r$ rounds we compute

$$L_i = L_{i-1} \otimes_l F_i(k_i, L_{i-1} \oslash_t R_{i-1}) \text{ and } R_i = R_{i-1} \otimes_r F_i(k_i, L_{i-1} \oslash_t R_{i-1}),$$

where $F_i(k_i, x)$ is defined as $F_i(k_i \otimes_k x)$ or $F_i(x \otimes_k k_i)$. We further call these versions the left symmetric Lai-Massey structures. We can also define the right symmetric Lai-Massey structures as follows

$$L_i = F_i(k_i, L_{i-1} \oslash_t R_{i-1}) \otimes_l L_{i-1} \text{ and } R_i = F_i(k_i, L_{i-1} \oslash_t R_{i-1}) \otimes_r R_{i-1}.$$

In the asymmetric case we define the outer versions as

$$L_i = L_{i-1} \otimes_l F_i(k_i, L_{i-1} \otimes_t R_{i-1}) \text{ and } R_i = F_i(k_i, L_{i-1} \otimes_t R_{i-1}) \oslash_r R_{i-1}$$

and the inner versions as

$$L_i = F_i(k_i, L_{i-1} \otimes_t R_{i-1}) \otimes_l L_{i-1} \text{ and } R_i = R_{i-1} \oslash_r F_i(k_i, L_{i-1} \otimes_t R_{i-1}).$$

*Remark 2.* When $\otimes = \star$, and we define $\otimes_t = \oslash$, $\otimes_k = \otimes_r = \otimes$, and $\otimes_l = \rho(x \otimes y)$, the result is the symmetric non-commutative group Lai-Massey structure as detailed in [37]. For the asymmetric version, as outlined in [37], we need to set $\otimes_r = \oslash$, $\otimes_k = \otimes_t = \otimes$ in our asymmetric structure.

### 3.2 Symmetric Structure Analysis

In this subsection, we extend the differential probabilities introduced in [37] for non-commutative group symmetric Lai-Massey structures to our quasigroup version.

**Definition 5.** *Let $K$ be a key, $X^i, Y^i \in \mathbb{G}^2$ for $i \in \{0,1\}$ and $j \in \{l, r\}$. We define the symmetric Lai-Massey quasigroup differential probabilities*

1. *Let $Z^i = X_l^i \oslash_t X_r^i$ and $Y_j^i = X_j^i \otimes_j F(K \otimes_k Z^i)$. Then*

$$LLM_{\oslash, \otimes_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash_l, \oslash_r}(X^0, X^1) = \alpha \\ \Delta_{\otimes_k}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash_l, \oslash_r}(Y^0, Y^1) = \beta];$$

2. *Let $Z^i = X_l^i \oslash_t X_r^i$ and $Y_j^i = X_j^i \otimes_j F(Z^i \otimes_k K)$. Then*

$$LLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash_l, \oslash_r}(X^0, X^1) = \alpha \\ \Delta_{\oslash_k}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash_l, \oslash_r}(Y^0, Y^1) = \beta];$$

3. *Let $Z^i = X_r^i \oslash_t X_l^i$ and $Y_j^i = F(K \otimes_k Z^i) \otimes_j X_j^i$. Then*

$$RLM_{\oslash, \otimes_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash_l, \oslash_r}(X^0, X^1) = \alpha \\ \Delta_{\otimes_k}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash_l, \oslash_r}(Y^0, Y^1) = \beta];$$

4. *Let $Z^i = X_r^i \oslash_t X_l^i$ and $Y_j^i = F(Z^i \otimes_k K) \otimes_j X_j^i$. Then*

$$RLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash_l, \oslash_r}(X^0, X^1) = \alpha \\ \Delta_{\oslash_k}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash_l, \oslash_r}(Y^0, Y^1) = \beta];$$

*where $F : \mathbb{G} \to \mathbb{G}$ is a function, $\alpha, \beta \in \mathbb{G}^2$ and $\gamma \in \mathbb{G}$.*

*Remark 3.* Let $F_l, F_r : \mathbb{G} \to \mathbb{G}$ be two functions. When $Y_j^i = X_j^i \otimes_j F_j(K \otimes_k Z^i)$ we denote the differential probability with $LLM_{\oslash, \otimes_k}(F_l, F_r, \alpha, \beta, \gamma, K)$. We also, use the same convention for the rest of the Lai-Massey differential probabilities.

Let $x \otimes_i y = \omega_i^{-1}(\pi_i(x) \star \rho_i(y))$, where $i \in \{k, l, r, t\}$. We further study the impact of the $\omega_i$s, $\pi_i$s and $\rho_i$s on the symmetric Lai-Massey structures.

**Lemma 3.** *Let $i \in \{l, r\}$, $\pi_i' = \pi_i \circ \omega_i^{-1}$, $\rho_i' = \rho_i \circ \omega_i^{-1}$, $F_i = \omega_i \circ F \circ \pi_t^{-1}$. Also, let $\rho_t' = \rho_t \circ \omega_r^{-1}$, $\omega_t' = \omega_t \circ \omega_l^{-1}$, $\pi_k' = \pi_k \circ \pi_t^{-1}$, $\rho_k' = \rho_k \circ \pi_t^{-1}$ and $\omega_k' = \omega_k \circ \pi_t^{-1}$. We define $x *_i y = \pi_i'(x) \star \rho_i'(y)$, $x *_t y = \omega_t'^{-1}(x \star \rho_t'(y))$, $x *_k y = \omega_k'^{-1}(\pi_k'(x) \star \rho_k'(y))$ and $\backslash_j$, $/_j$ the associated left and right divisions, where $j \in \{l, r, t, k\}$. Then the following identities hold*

$$LLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = LLM_{\backslash, \backslash_k}(F_l, F_r, A, B, \pi_t(\gamma), \pi_t(K)),$$
$$LLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = LLM_{\backslash, /_k}(F_l, F_r, A, B, \pi_t(\gamma), \pi_t(K)),$$

*where $A = \omega_l(\alpha_l) \| \omega_r(\alpha_r)$ and $B = \omega_l(\beta_l) \| \omega_r(\beta_r)$.*

*Proof.* Let $i \in \{0, 1\}$ and $j \in \{l, r\}$. First we rewrite $LLM_{\oslash, \oslash_k}$ as

$$LLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\otimes_l, \otimes_r}(X^0, \alpha) = X^1 \\ \Delta_{\otimes_k}(Z^0, \gamma) = Z^1}} [\Delta_{\otimes_l, \otimes_r}(Y^0, \beta) = Y^1].$$

Let $\omega_j(X_j^i) = S_j^i$. Then

$$
\begin{aligned}
X_j^0 \otimes_j \alpha_j = X_j^1 &\iff \pi_j(X_j^0) \star \rho_j(\alpha_j) = \omega_j(X_j^1) \\
&\iff \pi_j'(\omega_j(X_j^0)) \star \rho_j'(\omega_j(\alpha_j)) = \omega_j(X_j^1) \\
&\iff \pi_j'(S_j^0) \star \rho_j'(A_j) = S_j^1 \\
&\iff S_j^0 *_j A_j = S_j^1
\end{aligned}
\tag{1}
$$

and

$$
\begin{aligned}
Z^j = X_l^j \oslash_t X_r^j &\iff Z^j \otimes_t X_r^j = X_l^j \\
&\iff \pi_t(Z^j) \star \rho_t(X_r^j) = \omega_t(X_l^j) \\
&\iff \pi_t(Z^j) = \omega_t(X_l^j) \star \rho_t(X_r^j)^{-1} \\
&\iff \pi_t(Z^j) = \omega_t'(\omega_l(X_l^j)) \star \rho_t'(\omega_r(X_r^j))^{-1} \\
&\iff Z^j = \pi_t^{-1}(\omega_t'(S_l^j) \star \rho_t'(S_r^j)^{-1}) \\
&\iff Z^j = \pi_t^{-1}(S_l^j /_t S_r^j).
\end{aligned}
\tag{2}
$$

Let $T^j = S_l^j /_t S_r^j$, $\pi_t(\gamma) = \Gamma$ and $\pi_t(K) = K'$. Then using Equation (2) we obtain

$$
\begin{aligned}
Z^0 \otimes_k Z^1 = \gamma &\iff \pi_k(\pi_t^{-1}(T^0)) \star \rho_k(\gamma) = \omega_k(\pi_t^{-1}(T^1)) \\
&\iff \pi_k'(T^0) \star \rho_k'(\pi_t(\gamma)) = \omega_k'(T^1) \\
&\iff T^0 *_k \Gamma = T^1 \\
&\iff T^0 \backslash_k T^1 = \Gamma
\end{aligned}
\tag{3}
$$

and

$$F(K \otimes_k Z^j) = F(\omega_k^{-1}(\pi_k(K) \star \rho_k(Z^j)))$$
$$= F(\pi_t^{-1}(\omega_k'^{-1}(\pi_k'(\pi_t(K)) \star \rho_k'(\pi_t(Z^j)))))$$
$$= F(\pi_t^{-1}(K' *_k T^j)). \tag{4}$$

Let $W_j^i = S_j^i *_j F_j(K' *_k T^i)$. From Equation (4) we derive

$$Y_j^i = X_j^i \otimes_j F(K \otimes_k Z^i) \iff \omega_j(Y_j^i) = \pi_j(X_j^i) \star \rho_j(F(K \otimes_k Z^i))$$
$$\iff \omega_j(Y_j^i) = \pi_j'(\omega_j(X_j^i)) \star \rho_j'(\omega_j(F(\pi_t^{-1}(K' *_k T^i))))$$
$$\iff \omega_j(Y_j^i) = \pi_j'(S_j^i) \star \rho_j'(F_j(K' *_k T^i))$$
$$\iff \omega_j(Y_j^i) = S_j^i *_j F_j(K' *_k T^i)$$
$$\iff \omega_j(Y_j^i) = W_j^i,$$

which leads to

$$Y_j^0 \otimes_j \beta_j = Y_j^1 \iff \pi_j(Y_j^0) \star \rho_j(\beta_j) = \omega_j(Y_j^1)$$
$$\iff \pi_j'(W_j^0) \star \rho_j'(\omega_j(\beta_j)) = W_j^1$$
$$\iff W_j^0 *_j B_j = W_j^1. \tag{5}$$

Using Equations (1), (3) and (5) we obtain

$$LLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0, S^1 \in \mathbb{G}^2 \\ \Delta_{*_l, *_r}(S^0, A) = S^1 \\ \Delta_{*_k}(T^0, \Gamma) = T^1}} [\Delta_{*_l, *_r}(W^0, B) = W^1]$$
$$= LLM_{\backslash, \backslash_k}(F_l, F_r, A, B, \Gamma, K').$$

The remaining equality is proven using similar techniques. $\qquad \square$

The proof of Lemma 4 follows a similar rationale to the proof of Lemma 3, and thus, it is omitted.

**Lemma 4.** *Let* $i \in \{l, r\}$, $\pi_i' = \pi_i \circ \omega_i^{-1}$, $\rho_i' = \rho_i \circ \omega_i^{-1}$, $F_i = \omega_i \circ F \circ \pi_t^{-1}$. *Also, let* $\pi_t' = \pi_t \circ \omega_r^{-1}$, $\omega_t' = \omega_t \circ \omega_l^{-1}$, $\pi_k' = \pi_k \circ \rho_t^{-1}$, $\rho_k' = \rho_k \circ \rho_t^{-1}$ *and* $\omega_k' = \omega_k \circ \rho_t^{-1}$. *We define* $x *_i y = \pi_i'(x) \star \rho_i'(y)$, $x *_t y = \omega_t'^{-1}(\pi_t'(x) \star y)$, $x *_k y = \omega_k'^{-1}(\pi_k'(x) \star \rho_k'(y))$ *and* $\backslash_j, /_j$ *the associated left and right divisions, where* $j \in \{l, r, t, k\}$. *Then the following identities hold*

$$RLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = RLM_{/, \backslash_k}(F_l, F_r, A, B, \rho_t(\gamma), \rho_t(K)),$$
$$RLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = RLM_{/, /_k}(F_l, F_r, A, B, \rho_t(\gamma), \rho_t(K)),$$

*where* $A = \omega_l(\alpha_l) \| \omega_r(\alpha_r)$ *and* $B = \omega_l(\beta_l) \| \omega_r(\beta_r)$.

Lemmas 3 and 4 tell us that it is irrelevant from a differential point of view[6] if we define the quasigroup operation with $\omega_i \neq Id$ or $\omega_i = Id$, where $i \in \{l, r\}$. The same is true for $\pi_t$ (left case) or $\rho_t$ (right case). Thus, we further restrict our study[7] to the quasigroup operations $x \otimes_i y = \pi_i(x) \star \rho_i(y)$ and $x \otimes_{tl} y = \omega_t^{-1}(x \star \rho_t(y))$ (left case) or $x \otimes_{tr} y = \omega_t^{-1}(\pi_t(x) \star y)$ (right side). Now, considering the non-linear layer $F$, we observe, according to Lemmas 3 and 4, that it would be simpler to study $F_l$ and $F_r$ instead of $F$.

**Lemma 5.** *Let $\pi_l' = \pi_l \circ \omega_t^{-1}$, $\pi_r' = \pi_r \circ \rho_t^{-1}$, $F_i' = \rho_i \circ F_i$, where $i \in \{l, r\}$. We define $x *_l y = \omega_t(\pi_l'(x) \star y)$, $x *_r y = \rho_t(\pi_r'(x) \star y)$ and $\backslash_i, /_i$ the associated left and right divisions, where $i \in \{l, r\}$. Then the following identities hold*

$$LLM_{\oslash, \otimes_k}(F_l, F_r, \alpha, \beta, \gamma, K) = LLM_{\backslash, \otimes_k}(F_l', F_r', A, B, \gamma, K),$$
$$LLM_{\oslash, \oslash_k}(F_l, F_r, \alpha, \beta, \gamma, K) = LLM_{\backslash, \oslash_k}((F_l', F_r', A, B, \gamma, K),$$

*where $A = \rho_l(\alpha_l) \| \rho_r(\alpha_r)$ and $B = \rho_l(\beta_l) \| \rho_r(\beta_r)$.*

*Proof.* As before, let $i \in \{0, 1\}$ and $j \in \{l, r\}$. Also, let $\omega_t(X_l^i) = S_l^i$ and $\rho_t(X_r^i) = S_r^i$. Then

$$
\begin{aligned}
X_l^0 \otimes_l \alpha_l = X_l^1 &\iff \pi_l(X_l^0) \star \rho_l(\alpha_l) = X_l^1 \\
&\iff \omega_t(\pi_l'(\omega_t(X_l^0)) \star A_l) = \omega_t(X_l^1) \\
&\iff \omega_t(\pi_l'(S_l^0) \star A_l) = S_l^1 \\
&\iff S_l^0 *_l A_l = S_l^1.
\end{aligned}
\tag{6}
$$

$$
\begin{aligned}
X_r^0 \otimes_r \alpha_r = X_r^1 &\iff \rho_t(\pi_r'(S_r^0) \star A_r) = S_r^1 \\
&\iff S_r^0 *_r A_r = S_r^1.
\end{aligned}
\tag{7}
$$

and

$$
\begin{aligned}
Z^j = X_l^j \oslash_{tl} X_r^j &\iff Z^j = \omega_t(X_l^j) \star \rho_t(X_r^j)^{-1} \\
&\iff Z^j = S_l^j \star (S_r^j)^{-1}.
\end{aligned}
\tag{8}
$$

Let $W_l^i = S_l^i *_l F_l'(K \otimes_k Z^i)$ and $W_r^i = S_r^i *_r F_r'(K \otimes_k Z^i)$. Then we derive

$$
\begin{aligned}
Y_l^i &= X_l^i \otimes_l F_l(K \otimes_k Z^i) = \pi_l(X_l^i) \star \rho_l(F_l(K \otimes_k Z^i)) \\
&= \pi_l'(\omega_t(X_l^i)) \star F_l'(K \otimes_k Z^i) = \omega_t^{-1}(S_l^i *_l F_l'(K \otimes_k Z^i))
\end{aligned}
$$

$$
Y_r^i = \pi_r'(S_r^i) \star F_r'(K \otimes_k Z^i) = \rho_t^{-1}(S_r^i *_r F_r'(K \otimes_k Z^i))
$$

---

[6] *e.g.* we obtain the same differential probabilities $LLM$ and $RLM$
[7] without loss of generality

which leads to

$$Y_l^0 \otimes_l \beta_l = Y_l^1 \iff \pi_l(Y_l^0) \star \rho_l(\beta_l) = Y_l^1$$
$$\iff \pi_l'(W_l^0) \star B_l = \omega_t^{-1}(W_l^1)$$
$$\iff W_l^0 *_l B_l = W_l^1 \tag{9}$$

$$Y_r^0 \otimes_r \beta_r = Y_r^1 \iff \pi_r'(W_r^0) \star B_r = \omega_t^{-1}(W_r^1)$$
$$\iff W_r^0 *_r B_r = W_r^1. \tag{10}$$

Using Equations (6) to (10) we obtain

$$LLM_{\oslash,\oslash_k}(F_l, F_r, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0, S^1 \in \mathbb{G}^2 \\ \Delta_{*_l, *_r}(S^0, A) = S^1 \\ \Delta_{\oslash_k}(Z^0, \gamma) = Z^1}} [\Delta_{*_l, *_r}(W^0, B) = W^1]$$
$$= LLM_{\backslash,\oslash_k}(F_l', F_r', A, B, \gamma, K).$$

The second equality is proven using similar techniques. □

The proof of Lemma 6 follows a similar rationale to the proof of Lemma 5, and thus, it is omitted.

**Lemma 6.** Let $\rho_l' = \rho_l \circ \pi_t^{-1}$, $\rho_r' = \rho_r \circ \omega_t^{-1}$, $F_i' = \pi_i \circ F_i$, where $i \in \{l, r\}$. We define $x *_l y = \pi_t(x \star \rho_l'(y))$, $x *_r y = \omega_t(x \star \rho_r'(y))$ and $\backslash_i, /_i$ the associated left and right divisions, where $i \in \{l, r\}$. Then the following identities hold

$$RLM_{\oslash,\oslash_k}(F_l, F_r, \alpha, \beta, \gamma, K) = RLM_{/,\oslash_k}(F_l', F_r', A, B, \gamma, K),$$
$$RLM_{\oslash,\oslash_k}(F_l, F_r, \alpha, \beta, \gamma, K) = RLM_{/,\oslash_k}((F_l', F_r', A, B, \gamma, K),$$

where $A = \pi_l(\alpha_l) \| \pi_r(\alpha_r)$ and $B = \pi_l(\beta_l) \| \pi_r(\beta_r)$.

Lemmas 5 and 6 indicate that the choice of $\rho_i$ (in the left case) and $\pi_i$ (in the right case) is irrelevant from a differential perspective. As illustrated in Equation (8), we can restrict our study to $\otimes_t = \star$. Therefore, we further consider $\rho_i = Id$ (in the left case) and $\pi_i = Id$ (in the right case) and that $\otimes = \otimes_t = \star$. Moreover, these lemmas indicate that we can consider $F_l'$ and $F_r'$ instead of $F_l$ and $F_r$. A closer examination of the non-linear layers reveals that they can be expressed as $F_i'' = F_i' \circ \omega_k^{-1}$. Consequently, it is more convenient to investigate $F_i''$ rather than $F_i'$.

Since $K$ and, for example, $\pi_k$ are generated as a pair, it suffices from a differential point of view to simply consider $K' = \pi_k(K)$ as being the key that we want to recover. This is possible, since our final scope is to recover the plaintexts and not the initial key used by the symmetric structure. As a consequence, it suffices to restrict our study to $x \otimes_{kl} y = \pi_k(x) \star y$ (left version) and $x \otimes_{kr} y = x \star \rho_k(y)$ (right version).
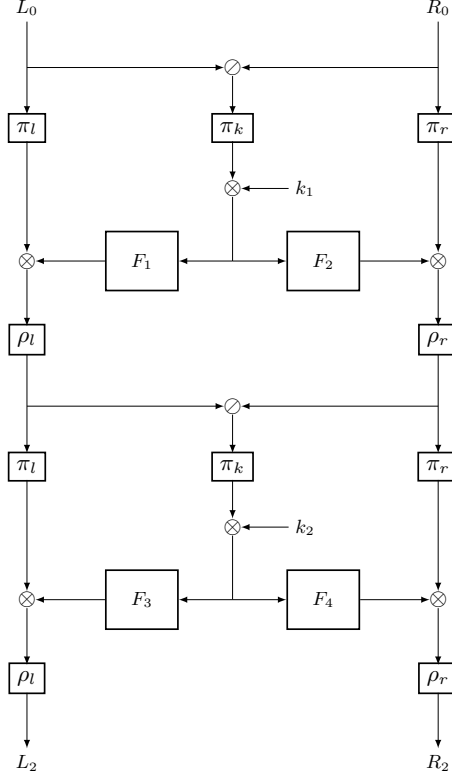
Fig. 2: Symmetric non-commutative group Lai-Massey structure (version 1)

Taking into account the previous arguments, we obtain the Lai-Massey structure depicted in Figure 2.

A different point of view of studying the version 1 structure is to redefine the differential probabilities as follows

1. Let $Z^i = X_l^i \oslash X_r^i$ and $Y_j^i = \rho_j(\pi_j(X_j^i) \otimes F_j(K \otimes \pi_k(Z^i)))$. Then

$$LLM_{\otimes,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\otimes,\oslash}(X^0, X^1) = \alpha \\ \Delta_{\oslash}(Z^0, Z^1) = \gamma}} [\Delta_{\otimes,\oslash}(Y^0, Y^1) = \beta];$$

2. Let $Z^i = X_l^i \oslash X_r^i$ and $Y_j^i = \rho_j(\pi_j(X_j^i) \otimes F_j(\pi_k(Z^i) \otimes K))$. Then

$$LLM_{\otimes,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\otimes,\oslash}(X^0, X^1) = \alpha \\ \Delta_{\oslash}(Z^0, Z^1) = \gamma}} [\Delta_{\otimes,\oslash}(Y^0, Y^1) = \beta];$$

3. Let $Z^i = X_r^i \oslash X_l^i$ and $Y_j^i = \rho_j(F_j(K \otimes \pi_k(Z^i)) \otimes \pi_j(X_j^i))$. Then

$$RLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0, X^1) = \alpha \\ \Delta_{\oslash}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash,\oslash}(Y^0, Y^1) = \beta];$$

4. Let $Z^i = X_r^i \oslash X_l^i$ and $Y_j^i = \rho_j(F_j(\pi_k(Z^i) \otimes K) \otimes \pi_j(X_j^i))$. Then

$$RLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0, X^1) = \alpha \\ \Delta_{\oslash}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash,\oslash}(Y^0, Y^1) = \beta].$$

We further provide the reader with some condition that guarantee key independence for the differential probabilities associated with the Lai-Massey round functions.

**Lemma 7.** *If $\pi_k$, $\pi_l$ and $\rho_l$ are morphisms then $LLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K)$ and $RLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K)$ are key independent.*

*Proof.* We begin by rewriting $X_l^i = \pi_k^{-1}(K^{-1}) \otimes S_l^i$ and $X_r^i = S_r^i$. Then

$$\alpha_l = (X_l^0)^{-1} \otimes X_l^1 = (S_l^0)^{-1} \otimes \pi_k^{-1}(K \otimes K^{-1}) \otimes S_l^1 = (S_l^0)^{-1} \otimes S_l^1 \qquad (11)$$

and

$$Z^i = X_l^i \otimes (X_r^i)^{-1} = \pi_k^{-1}(K^{-1}) \otimes S_l^i \otimes (S_r^i)^{-1}. \qquad (12)$$

Let $T^i = S_l^i \oslash S_r^i$ and $F_j' = \pi_l^{-1} \circ F_j \circ \pi_k$. Using Equations (11) and (12) we obtain

$$\begin{aligned}
\gamma = (Z^0)^{-1} \otimes Z^1 &= (\pi_k^{-1}(K^{-1}) \otimes S_l^0 \otimes (S_r^0)^{-1})^{-1} \otimes (\pi_k^{-1}(K^{-1}) \otimes S_l^1 \otimes (S_r^1)^{-1}) \\
&= S_r^0 \otimes (S_l^0)^{-1} \otimes \pi_k^{-1}(K \otimes K^{-1}) \otimes S_l^1 \otimes (S_r^1)^{-1} \\
&= S_r^0 \otimes (S_l^0)^{-1} \otimes S_l^1 \otimes (S_r^1)^{-1} \\
&= (T^0)^{-1} \otimes T^1 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (13)
\end{aligned}$$

and

$$\begin{aligned}
F_j(K \otimes \pi_k(Z^i)) &= F_j(K \otimes K^{-1} \otimes \pi_k(S_l^i \otimes (S_r^i)^{-1})) \\
&= \pi_l(F_j'(S_l^i \otimes (S_r^i)^{-1})) = \pi_l(F_j'(T^i)). \qquad (14)
\end{aligned}$$

Let $\pi_r' = \pi_l^{-1} \circ \pi_r$, $\rho_l' = \rho_l \circ \pi_l$ and $\rho_r' = \rho_r \circ \pi_l$. From Equation (14) we derive

$$\begin{aligned}
Y_r^i &= \rho_r(\pi_r(X_r^i) \otimes F_r(K \otimes \pi_k(Z^i))) \\
&= \rho_r(\pi_r(X_r^i) \otimes \pi_l(F_r'(T^i))) \\
&= \rho_r(\pi_l(\pi_r'(X_r^i) \otimes F_r'(T^i))) \\
&= \rho_r'(\pi_r'(S_r^i) \otimes F_r'(T^i))
\end{aligned}$$

and

$$Y_l^i = \rho_l(\pi_l(X_l^i) \otimes F_l(K \otimes \pi_k(Z^i)))$$
$$= \rho_l(\pi_l(X_l^i) \otimes \pi_l(F_l'(T^i)))$$
$$= \rho_l(\pi_l(X_l^i \otimes F_l'(T^i)))$$
$$= \rho_l'(X_l^i \otimes F_l'(T^i))$$
$$= \rho_l'(\pi_k^{-1}(K))^{-1} \otimes \rho_l'(S_l^i \otimes F_l'(T^i)).$$

Hence, we have

$$Y_l^0 \oslash Y_l^1 = (\rho_l'(S_l^0 \otimes F_l'(T^0)))^{-1} \otimes \rho_l'(S_l^1 \otimes F_l'(T^1)) \tag{15}$$
$$Y_r^0 \oslash Y_r^1 = (\rho_r'(\pi_r'(S_r^0) \otimes F_r'(T^0)))^{-1} \otimes (\rho_r'(\pi_r'(S_r^1) \otimes F_r'(T^1))). \tag{16}$$

Note that Equation (15) is equivalent with

$$\rho_l'^{-1}(\beta_l) = (S_l^0 \otimes F_l'(T^0))^{-1} \otimes S_l^1 \otimes F_l'(T^1).$$

Using Equations (11), (13), (15) and (16) we obtain the desired equality. The remaining relations are proven similarly. $\square$

Upon closer examination of Lemma 7's proof, it becomes evident that we can derive the equivalent structure depicted in Figure 3. Its corresponding differential probabilities are

$$LLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0,X^1)=\alpha \\ \Delta_{\oslash}(Z^0,Z^1)=\gamma}} [\Delta_{\oslash,\oslash}(Y^0, Y^1) = \beta],$$

where $Y_l^i = X_l^i \otimes F_l(Z^i)$ and $Y_r^i = \rho_r(\pi_r(X_r^i) \otimes F_r(Z^i))$, and

$$RLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0,X^1)=\alpha \\ \Delta_{\oslash}(Z^0,Z^1)=\gamma}} [\Delta_{\oslash,\oslash}(Y^0, Y^1) = \beta],$$

where $Y_l^i = F_l(Z^i) \otimes X_l^i$ and $Y_r^i = \rho_r(F_r(Z^i) \otimes \pi_r(X_r^i))$. When $LLM$ and $RLM$ are independent of the key the security analysis simplifies and we can offers higher security guarantees[8]. Hence, we restrict our study to $\rho_l = \pi_l = \pi_k = Id$ for $LLM_{\oslash,\oslash}$ and $RLM_{\oslash,\oslash}$.

We further state without proof the conditions required for key independence for the remaining differential probabilities.

**Lemma 8.** *If $\pi_k$, $\pi_r$ and $\rho_r$ are morphisms then $LLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K)$ and $RLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K)$ are key independent.*

---

[8] In practice we can not check the differential probabilities for all the keys.

Fig. 3: Symmetric non-commutative group Lai-Massey structure (version 2)

Similarly to the previous case, we can derive an equivalent structure using Lemma 8's proof. We provide only its corresponding differential probabilities

$$LLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0, X^1) = \alpha \\ \Delta_{\oslash}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash,\oslash}(Y^0, Y^1) = \beta],$$

where $Y_l^i = \rho_l(\pi_l(X_l^i) \otimes F_l(Z^i))$ and $Y_r^i = X_r^i \otimes F_r(Z^i)$, and

$$RLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0, X^1) = \alpha \\ \Delta_{\oslash}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash,\oslash}(Y^0, Y^1) = \beta],$$

where $Y_l^i = \rho_l(F_l(Z^i) \otimes \pi_l(X_l^i))$ and $Y_r^i = F_r(Z^i) \otimes X_r^i$.

The following corollaries indicate that it is sufficient to focus solely on a version 2 structure from a differential perspective if $\rho_r$ is a morphism.

**Corollary 1.** *Let* $\bar{\alpha} = \alpha_r \| \alpha_l$ *and* $\bar{\beta} = \beta_r \| \beta_l$. *Then*

$$LLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma) = LLM_{\oslash,\oslash}(F_r, F_l, \bar{\alpha}, \bar{\beta}, \gamma^{-1})$$
$$RLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma) = RLM_{\oslash,\oslash}(F_l, F_r, \bar{\alpha}, \bar{\beta}, \gamma^{-1}).$$

*Proof.* We first observe that

$$\gamma = Z^0 \oslash Z^1 = Z_0^{-1} \otimes Z_1 = (Z_1^{-1} \otimes Z_0)^{-1} = (Z_1 \oslash Z_0)^{-1}.$$

So, $\Delta_{\oslash}(Z^1, Z^0) = \gamma^{-1}$. Also,

$$\Delta_{\oslash,\oslash}(X_r^0 \| X_l^0, X_r^1 \| X_l^1) = \bar{\alpha} \text{ and } \Delta_{\oslash,\oslash}(Y_r^0 \| Y_l^0, Y_r^1 \| Y_l^1) = \bar{\beta}.$$

Thus, we obtain the desired result. □

**Corollary 2.** *We define* $G_l(x) = F_l(x)^{-1}$, $G_r(x) = F_r(x)^{-1}$ *and* $\varepsilon_r(x) = \pi_r(x^{-1})^{-1}$. *If* $\rho_r$ *is a morphisms then*

$$LLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma) = RLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma).$$

*Proof.* Let $j \in \{l, r\}$ and $S_j^i = (X_j^i)^{-1}$. We observe that

$$\alpha_j = X_j^0 \oslash X_j^1 = (X_j^0)^{-1} \otimes X_j^1 = S_j^0 \otimes (S_j^1)^{-1} = S_j^0 \oslash S_j^1$$
$$Z^i = X_l^i \oslash X_r^i = X_l^i \otimes (X_r^i)^{-1} = (S_l^i)^{-1} \otimes S_r^i = S_l^i \oslash S_r^i$$

and

$$\begin{aligned}
Y_l^0 \oslash Y_l^1 &= F_l(Z^0)^{-1} \otimes (X_l^0)^{-1} \otimes X_l^1 \otimes F_l(Z^1) \\
&= G_l(Z^0) \otimes S_j^0 \otimes (S_j^1)^{-1} \otimes G_l(Z^1)^{-1} \\
&= \Delta_{\oslash}(G_l(Z^0) \otimes S_l^0, G_l(Z^1) \otimes S_l^1)
\end{aligned}$$

$$\begin{aligned}
Y_r^0 \oslash Y_r^1 &= \rho_r(\pi_r(X_r^0) \otimes F_r(Z^0))^{-1} \otimes \rho_r(\pi_r(X_r^1) \otimes F_r(Z^1)) \\
&= \rho_r(F_r(Z^0)^{-1} \otimes \pi_r(X_r^0)^{-1} \otimes \pi_r(X_r^1) \otimes F_r(Z^1) \\
&= \rho_r(G_r(Z^0) \otimes \varepsilon_r(S_r^0)^{-1} \otimes \varepsilon_r(S_r^1)^{-1} \otimes G_r(Z^1)^{-1} \\
&= \rho_r(G_r(Z^0) \otimes \varepsilon_r(S_r^0)^{-1}) \otimes \rho_r(G_r(Z^1) \otimes \varepsilon_r(S_r^1))^{-1} \\
&= \Delta_{\oslash}(\rho_r(G_r(Z^0) \otimes \varepsilon_r(S_r^0)^{-1}), \rho_r(G_r(Z^1) \otimes \varepsilon_r(S_r^1))).
\end{aligned}$$

Thus, we obtain the desired equality. □

We further delve into the conditions required for correct decryption. We can observe that this requirement translates into

$$X_l \oslash X_r = (X_l \otimes F_l(Z)) \oslash (\pi_r(X_r) \otimes F_r(Z)), \tag{17}$$

where $Z = X_l \oslash X_r$. We remark that Equation (17) is equivalent to

$$\begin{aligned}
X_l \otimes X_r^{-1} &= (X_l \otimes F_l(Z)) \otimes (\pi_r(X_r) \otimes F_r(Z))^{-1} \\
&= X_l \otimes F_l(Z) \otimes F_r(Z)^{-1} \otimes \pi_r(X_r)^{-1},
\end{aligned}$$

which leads to

$$\pi_r(X_r) \otimes X_r^{-1} = F_l(Z) \otimes F_r(Z)^{-1}. \tag{18}$$

**Lemma 9.** *Let $\eta \in \mathbb{G}$. We can decrypt if and only if $\pi_r(x) = \eta \otimes x$ and $F_l(x) = \eta \otimes F_r(x)$.*

*Proof.* First note that Equation (18) holds for any $X_r$ and $X_l$. Therefore, we can fix an arbitrary $X_r$ and denote by $\eta = \pi_r(X_r) \otimes X_r^{-1}$. Thus, we obtain that $F_l(Z) = \eta \otimes F_r(Z)$ for any $X_l$. This leads to $F_l(x) = \eta \otimes F_r(x)$ for any $x$, since $Z$ is simply a translation of any $X_l$ with a fixed point. Consequently, from Equation (18) we obtain that $\pi_r(x) = \eta \otimes x$ for any $x$. We leave the converse as an exercise. □

Taking into account the previous arguments, we obtain the Lai-Massey structure depicted in Figure 4.
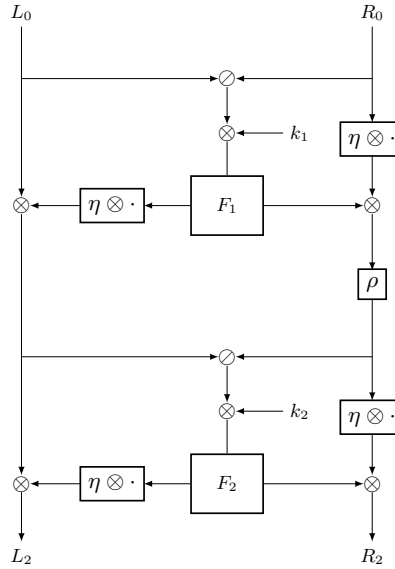


Fig. 4: Symmetric non-commutative group Lai-Massey structure (version 3)

The following corollary tells us that in the case of commutative groups, the only meaningful[9] structure is the one with $\pi_r = Id$ and $F_l = F_r$.[10]

**Corollary 3.** *If $(\mathbb{G}, \otimes)$ is Abelian and $\rho_r$ is a morphisms then*

$$LLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma) = LLM_{\oslash,\oslash}(F_r, F_r, \alpha, \beta, \gamma).$$

*Proof.* Let $j \in \{l, r\}$ and $S_j^i = X_j^i \otimes \eta$. We observe that

$$\alpha_j = X_j^0 \oslash X_j^1 = (X_j^0)^{-1} \otimes X_j^1 = (X_j^0)^{-1} \otimes \eta^{-1} \otimes \eta \otimes X_j^1 = S_j^0 \oslash S_j^1$$

$$Z^i = X_l^i \oslash X_r^i = X_l^i \otimes (X_r^i)^{-1} = X_l^i \otimes \eta \otimes \eta^{-1} \otimes (X_r^i)^{-1} = S_l^i \oslash S_r^i.$$

---

[9] from a differential perspective

[10] Equivalently, the one with $\eta = \mathbb{1}_{\mathbb{G}}$, where $\mathbb{1}_{\mathbb{G}}$ is the identity element of $\mathbb{G}$.

and

$$Y_l^0 \oslash Y_l^1 = F_l(Z^0)^{-1} \otimes (X_l^0)^{-1} \otimes X_l^1 \otimes F_l(Z^1)$$
$$= F_r(Z^0)^{-1} \otimes \eta^{-1} \otimes (X_l^0)^{-1} \otimes X_l^1 \otimes \eta \otimes F_r(Z^1)$$
$$= F_r(Z^0)^{-1} \otimes (S_l^0)^{-1} \otimes S_l^1 \otimes F_r(Z^1)$$
$$= \Delta_\oslash(S_l^0 \otimes F_r(Z^0), S_l^1 \otimes F_r(Z^1))$$

$$Y_r^0 \oslash Y_r^1 = \rho_r(\pi_r(X_r^0) \otimes F_r(Z^0))^{-1} \otimes \rho_r(\pi_r(X_r^1) \otimes F_r(Z^1))$$
$$= \rho_r(\eta \otimes X_r^0 \otimes F_r(Z^0))^{-1} \otimes \rho_r(\eta \otimes X_r^1 \otimes F_r(Z^1))$$
$$= \rho_r(S_r^0 \otimes F_r(Z^0))^{-1} \otimes \rho_r(S_r^1 \otimes F_r(Z^1))$$
$$= \Delta_\oslash(\rho_r(S_r^0 \otimes F_r(Z^0)), \rho_r(S_r^1 \otimes F_r(Z^1))).$$

Thus, we obtain the desired equality. $\qquad\square$

When $\rho = Id$, the version 3 structure can be easily distinguished from a random permutation by simply checking if, for example, $L_2 \oslash R_2 = L_0 \oslash R_0$. We further introduce a definition from [38], which will prove useful for removing this vulnerability.

**Definition 6.** *A permutation $\varphi$ is a right orthomorphism if $\varphi'(x) = \varphi(x) \oslash x$ is a permutation. If $\varphi'(x) = x \oslash \varphi(x)$ is a permutation, then $\varphi$ is called a left orthomorphism.*

**Lemma 10.** *Let $Z = K \otimes (X_l \oslash X_r)$ and $t = F_r(K, Z)$. The following property holds*

$$Y_l \oslash Y_r = (X_l \otimes \eta) \oslash (\eta \otimes X_r) \otimes (\eta \otimes X_r \otimes t) \oslash \rho_r(\eta \otimes X_r \otimes t).$$

*Proof.* We observe that

$$Y_l \oslash Y_r = X_l \otimes F_l(Z) \otimes \rho_r(\pi_r(X_r) \otimes F_r(Z))^{-1}$$
$$= X_l \otimes \eta \otimes t \otimes \rho_r(\eta \otimes X_r \otimes t)^{-1}.$$

If we denote by $A = \eta \otimes X_r \otimes t$, we obtain that

$$Y_l \oslash Y_r = X_l \otimes \eta \otimes t \otimes \rho_r(A)^{-1}$$
$$= X_l \otimes \eta \otimes (\eta \otimes X_r)^{-1} \otimes \eta \otimes X_r \otimes t \otimes \rho_r(A)^{-1}$$
$$= (X_l \otimes \eta) \oslash (\eta \otimes X_r) \otimes A \oslash \rho_r(A),$$

and thus, we obtain the desired property. $\qquad\square$

**Corollary 4.** *If $\rho_r$ is a right orthomorphism, then $Y_l \oslash Y_r$ is a random element.*

*Proof.* Let $\rho_r'(x) = \rho_r(x) \oslash x$. According to Lemma 10, we have that

$$Y_l \oslash Y_r = (X_l \otimes \eta) \oslash (\eta \otimes X_r) \otimes \rho_r'(A)^{-1}.$$

Since $F(K, \cdot)$ is random function, then $A$ is randomly distributed. Since $\rho_r$ is a right orthomorphism, then $\rho_r'(A)$ is also random. Therefore, we obtain that $Y_l \oslash Y_r$ is uniformly distributed. $\qquad\square$

To summarise all the lemmas and observations we provide the reader with Proposition 1.

**Proposition 1.** *A symmetric quasigroup Lai-Massey structure derived from a symmetric non-commutative group Lai-Massey structure using an isotopy has the same differential security as version 3 (see Figure 4) if $\rho$ is a morphism and we require correct decryption. If the group is commutative we obtain that symmetric group Lai-Massey structure and version 3 are equivalent.*

### 3.3   Asymmetric Structure Analysis

In this section we extend the notion of differential cryptanalysis to asymmetric Lai-Massey structures. Then, as in the symmetric case, we show that the structure can be defined using only group operations. Finally, we show that the resulting structure is equivalent to the version 1 symmetric structure.

**Definition 7.** *Let $K$ be a key and $X^i, Y^i \in \mathbb{G}^2$ for $i \in \{0, 1\}$. We define the asymmetric Lai-Massey quasigroup differential probabilities*

1. *Let $Z^i = X_l^i \otimes_t X_r^i$, $Y_l^i = X_l^i \otimes_l F(K \otimes Z^i))$ and $Y_r^i = F(K \otimes Z^i) \oslash_r X_r^i$. Then*

$$OLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash_l, \oslash_r}(X^0, X^1) = \alpha \\ \Delta_{\oslash_k}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash_l, \oslash_r}(Y^0, Y^1) = \beta];$$

2. *Let $Z^i = X_l^i \otimes_t X_r^i$, $Y_l^i = X_l^i \otimes_l F(Z^i \otimes K)$ and $Y_r^i = F(Z^i \otimes K) \oslash_r X_r^i$. Then*

$$OLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash_l, \oslash_r}(X^0, X^1) = \alpha \\ \Delta_{\oslash_k}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash_l, \oslash_r}(Y^0, Y^1) = \beta];$$

3. *Let $Z^i = X_r^i \otimes_t X_l^i$, $Y_l^i = F(K \otimes Z^i) \otimes_l X_l^i$ and $Y_r^i = X_r^i \oslash_r F(K \otimes Z^i)$. Then*

$$ILM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash_l, \oslash_r}(X^0, X^1) = \alpha \\ \Delta_{\oslash_k}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash_l, \oslash_r}(Y^0, Y^1) = \beta];$$

4. *Let $Z^i = X_r^i \otimes_t X_l^i$, $Y_l^i = F(Z^i \otimes K) \otimes_l X_l^i$ and $Y_r^i = X_r^i \oslash_r F(Z^i \otimes K)$. Then*

$$ILM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0, X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash_l, \oslash_r}(X^0, X^1) = \alpha \\ \Delta_{\oslash_k}(Z^0, Z^1) = \gamma}} [\Delta_{\oslash_l, \oslash_r}(Y^0, Y^1) = \beta];$$

*where $F \colon \mathbb{G} \to \mathbb{G}$ is a function, $\alpha, \beta \in \mathbb{G}^2$ and $\gamma \in \mathbb{G}$.*

The next lemmas enable us to restrict our study to the case where $\omega_l = \omega_r = \omega_t = Id$, due to the differential equivalency. Note that the Lemmas 11 and 12 are proven similarly to Lemma 3, and hence, we omit their proof.

**Lemma 11.** *Let $i \in \{l, r\}$, $\pi'_i = \pi_i \circ \omega_i^{-1}$, $\rho'_i = \rho_i \circ \omega_i^{-1}$, $F_i = \omega_i \circ F \circ \omega_t^{-1}$. Also, let $\rho'_t = \rho_t \circ \omega_r^{-1}$, $\pi'_t = \pi_t \circ \omega_l^{-1}$, $\pi'_k = \pi_k \circ \omega_t^{-1}$, $\rho'_k = \rho_k \circ \omega_t^{-1}$ and $\omega'_k = \omega_k \circ \omega_t^{-1}$. We define $x *_i y = \pi'_i(x) \star \rho'_i(y)$, $x *_t y = \pi'_t(x) \star \rho'_t(y)$, $x *_k y = \omega_k'^{-1}(\pi'_k(x) \star \rho'_k(y))$ and $\backslash_j$, $/_j$ the associated left and right divisions, where $j \in \{l, r, t, k\}$. Then the following identities hold*

$$OLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = OLM_{\backslash, \backslash_k}(F_l, F_r, A, B, \omega_t(\gamma), \omega_t(K)),$$
$$OLM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = OLM_{\backslash, /_k}(F_l, F_r, A, B, \omega_t(\gamma), \omega_t(K)),$$

*where $A = \omega_l(\alpha_l) \| \omega_l(\alpha_l)$ and $B = \omega_l(\beta_l) \| \omega_l(\beta_l)$.*

**Lemma 12.** *Let $i \in \{l, r\}$, $\pi'_i = \pi_i \circ \omega_i^{-1}$, $\rho'_i = \rho_i \circ \omega_i^{-1}$, $F_i = \omega_i \circ F \circ \omega_t^{-1}$. Also, let $\rho'_t = \rho_t \circ \omega_l^{-1}$, $\pi'_t = \pi_t \circ \omega_r^{-1}$, $\pi'_k = \pi_k \circ \omega_t^{-1}$, $\rho'_k = \rho_k \circ \omega_t^{-1}$ and $\omega'_k = \omega_k \circ \omega_t^{-1}$. We define $x *_i y = \pi'_i(x) \star \rho'_i(y)$, $x *_t y = \pi'_t(x) \star \rho'_t(y)$, $x *_k y = \omega_k'^{-1}(\pi'_k(x) \star \rho'_k(y))$ and $\backslash_j$, $/_j$ the associated left and right divisions, where $j \in \{l, r, t, k\}$. Then the following identities hold*

$$ILM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = ILM_{/, \backslash_k}(F_l, F_r, A, B, \omega_t(\gamma), \omega_t(K)),$$
$$ILM_{\oslash, \oslash_k}(F, \alpha, \beta, \gamma, K) = ILM_{/, /_k}(F_l, F_r, A, B, \omega_t(\gamma), \omega_t(K)),$$

*where $A = \omega_l(\alpha_l) \| \omega_l(\alpha_l)$ and $B = \omega_l(\beta_l) \| \omega_l(\beta_l)$.*

The following lemmas are the asymmetric equivalent of Lemmas 5 and 6, and thus, we state them without proof.

**Lemma 13.** *Let $\pi'_l = \pi_l \circ \pi_t^{-1}$, $\rho'_r = \rho_r \circ \rho_t^{-1}$, $F'_l = \rho_l \circ F_l$, $F'_r = \pi_r \circ F_r$. We define $x *_l y = \pi_t(\pi'_l(x) \star y)$, $x *_r y = \rho_t(x \star \rho'_r(y))$ and $\backslash_i$, $/_i$ the associated left and right divisions, where $i \in \{l, r\}$. Then the following identities hold*

$$OLM_{\oslash, \oslash_k}(F_l, F_r, \alpha, \beta, \gamma, K) = OLM_{\backslash, \oslash_k}(F'_l, F'_r, A, B, \gamma, K),$$
$$OLM_{\oslash, \oslash_k}(F_l, F_r, \alpha, \beta, \gamma, K) = OLM_{\backslash, \oslash_k}(F'_l, F'_r, A, B, \gamma, K),$$

*where $A = \rho_l(\alpha_l) \| \pi_r(\alpha_l)$ and $B = \rho_l(\beta_l) \| \pi_r(\beta_l)$.*

**Lemma 14.** *Let $\rho'_l = \rho_l \circ \rho_t^{-1}$, $\pi'_r = \pi_r \circ \pi_t^{-1}$, $F'_l = \pi_l \circ F_l$, $F'_r = \rho_r \circ F_r$. We define $x *_l y = \rho_t(x \star \rho'_l(y))$, $x *_r y = \pi_t(\pi'_r(x) \star y)$ and $\backslash_i$, $/_i$ the associated left and right divisions, where $i \in \{l, r\}$. Then the following identities hold*

$$ILM_{\oslash, \oslash_k}(F_l, F_r, \alpha, \beta, \gamma, K) = ILM_{/, \oslash_k}(F'_l, F'_r, A, B, \gamma, K),$$
$$ILM_{\oslash, \oslash_k}(F_l, F_r, \alpha, \beta, \gamma, K) = ILM_{/, \oslash_k}(F'_l, F'_r, A, B, \gamma, K),$$

*where $A = \pi_l(\alpha_l) \| \rho_r(\alpha_l)$ and $B = \pi_l(\beta_l) \| \rho_r(\beta_l)$.*

Let $\otimes = \star$. Before presenting the resulting asymmetric structure, we would like to point out that

$$Y_r^i = F(t) \oslash_r X_r^i \Leftrightarrow F(t) \otimes_r Y_r^i = X_r^i \Leftrightarrow \rho_t(F(t) \star \rho_r'(Y_r^i)) = X_r^i$$
$$\Leftrightarrow Y_r^i = \rho_r'^{-1}(F(t)^{-1} \star \rho_t^{-1}(X_r^i))$$
$$\Leftrightarrow Y_r^i = \rho_r'^{-1}(F(t) \oslash \rho_t^{-1}(X_r^i))$$

$$Y_r^i = X_r^i \oslash_r F(t) \Leftrightarrow Y_r^i \otimes_r F(t) = X_r^i \Leftrightarrow \pi_t(\pi_r'(Y_r^i) \star F(t)) = X_r^i$$
$$\Leftrightarrow Y_r^i = \pi_r'^{-1}(\pi_t^{-1}(X_r^i) \star F(t)^{-1})$$
$$\Leftrightarrow Y_r^i = \pi_r'^{-1}(\pi_t^{-1}(X_r^i) \oslash F(t)),$$

where for the last equalities we used Lemma 2.

Considering the aforementioned remark and employing arguments akin to the symmetric counterpart, we obtain a Lai-Massey structure similar[11] to the one depicted in Figure 2. The associated differential properties are

1. Let $Z^i = X_l^i \otimes X_r^i$, $Y_l^i = \rho_l(\pi_l(X_l^i) \otimes F(K \otimes \pi_k(Z^i)))$ and $Y_r^i = \rho_r(F(K \otimes \pi_k(Z^i)) \oslash \pi_r(X_r^i))$. Then

$$OLM_{\oslash,\oslash}(F,\alpha,\beta,\gamma,K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0,X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0,X^1)=\alpha \\ \Delta_{\oslash}(Z^0,Z^1)=\gamma}} [\Delta_{\oslash,\oslash}(Y^0,Y^1) = \beta];$$

2. Let $Z^i = X_l^i \otimes X_r^i$, $Y_l^i = \rho_l(\pi_l(X_l^i) \otimes F(\pi_k(Z^i) \otimes K))$ and $Y_r^i = \rho_r(F(\pi_k(Z^i) \otimes K) \oslash \pi_r(X_r^i))$. Then

$$OLM_{\oslash,\oslash}(F,\alpha,\beta,\gamma,K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0,X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0,X^1)=\alpha \\ \Delta_{\oslash}(Z^0,Z^1)=\gamma}} [\Delta_{\oslash,\oslash}(Y^0,Y^1) = \beta];$$

3. Let $Z^i = X_r^i \otimes X_l^i$, $Y_l^i = \rho_l(F(K \otimes \pi_k(Z^i)) \otimes \pi_l(X_l^i))$ and $Y_r^i = \rho_r(\pi_r(X_r^i) \oslash F(K \otimes \pi_k(Z^i)))$. Then

$$ILM_{\oslash,\oslash}(F,\alpha,\beta,\gamma,K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0,X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0,X^1)=\alpha \\ \Delta_{\oslash}(Z^0,Z^1)=\gamma}} [\Delta_{\oslash,\oslash}(Y^0,Y^1) = \beta];$$

4. Let $Z^i = X_r^i \otimes X_l^i$, $Y_l^i = \rho_l(F(\pi_k(Z^i) \otimes K) \otimes \pi_l(X_l^i))$ and $Y_r^i = \rho_r(\pi_r(X_r^i) \oslash F(\pi_k(Z^i) \otimes K))$. Then

$$ILM_{\oslash,\oslash}(F,\alpha,\beta,\gamma,K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X^0,X^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(X^0,X^1)=\alpha \\ \Delta_{\oslash}(Z^0,Z^1)=\gamma}} [\Delta_{\oslash,\oslash}(Y^0,Y^1) = \beta].$$

---

[11] the top and right operations are changed to $\otimes$ and $\oslash$ (OLM) or $\oslash$ (ILM)

The following lemma shows that the asymmetric and the symmetric structures are differentially equivalent. Therefore, we can directly apply the results from Section 3.2.

**Lemma 15.** *Let $\pi'_r(x) = \pi_r(x^{-1})^{-1}$, $\rho'_r(x) = \rho_r(x^{-1})$. Then the following identities hold*

$$OLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K) = LLM_{\oslash,\oslash}(F_l, F_r, A, B, \gamma, K),$$
$$OLM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K) = LLM_{\oslash,\oslash}(F_l, F_r, A, B, \gamma, K),$$
$$ILM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K) = RLM_{\oslash,\oslash}(F_l, F_r, A, B, \gamma, K),$$
$$ILM_{\oslash,\oslash}(F_l, F_r, \alpha, \beta, \gamma, K) = RLM_{\oslash,\oslash}(F_l, F_r, A, B, \gamma, K).$$

*Proof.* Let $S_l^i = X_l^i$ and $S_r^i = (X_r^i)^{-1}$. We observe that

$$\alpha_r = X_r^0 \oslash X_r^1 = X_r^0 \otimes (X_r^1)^{-1} = (S_r^0)^{-1} \otimes S_r^1 = S_r^0 \oslash S_r^1$$
$$Z^i = X_l^i \otimes X_r^i = S_l^i \otimes (S_r^i)^{-1} = S_l^i \oslash S_r^i$$

and

$$Y_r^i = \rho_r(F(K \otimes \pi_k(Z^i)) \oslash \pi_r(X_r^i))$$
$$= \rho_r(F(K \otimes \pi_k(Z^i))^{-1} \otimes \pi_r(X_r^i))$$
$$= \rho_r(F(K \otimes \pi_k(Z^i))^{-1} \otimes \pi'_r(S_r^i)^{-1})$$
$$= \rho_r((\pi'_r(S_r^i) \otimes F(K \otimes \pi_k(Z^i)))^{-1})$$
$$= \rho'_r(\pi'_r(S_r^i) \otimes F(K \otimes \pi_k(Z^i))).$$

The remaining equalities are proven similarly. $\qquad\square$

To summarise all the lemmas and observations we provide the reader with Proposition 2.

**Proposition 2.** *An asymmetric quasigroup Lai-Massey structure has the same differential security a symmetric quasigroup Lai-Massey structure.*

## 4  Conclusions

In this paper we studied the effect of quasigroups isotopic to groups in the design of cryptographic symmetric structures. More precisely, for quasigroup extensions of the Lai-Massey structure, we investigated the security implications and unveiled interesting equivalencies with other symmetric structures based on the underlying group. Furthermore, we highlighted the necessary conditions for having correct decryption and we established that mounting a differential attack against the symmetric version is equivalent to attacking an alternative asymmetric structure.

*Future work.* It would be intriguing to investigate the effect of using quasigroups that do not exhibit isotopy to groups. Additionally, exploring the influence of other symmetries, such as parastrophisms [14] or paratopisms [15], could provide valuable insights. Another interesting area of research is to compare the performance and security of the proposed non-commutative structure with other block cipher architectures, such as SPNs or Feistel networks.

# References

1. Bakeva, V., Popovska-Mitrovikj, A., Mechkaroska, D., Dimitrova, V., Jakimovski, B., Ilievski, V.: Gaussian Channel Transmission of Images and Audio Files Using Cryptcoding. IET Communications **13**(11), 1625–1632 (2019)
2. Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J.: A Message Authentication Code Based on Latin Squares. In: ACISP 1997. Lecture Notes in Computer Science, vol. 1270, pp. 194–203. Springer (1997)
3. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: CRYPTO 1990. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1991)
4. Brunetta, C., Calderini, M., Sala, M.: On Hidden Sums Compatible with a Given Block Cipher Diffusion Layer. Discret. Math. **342**(2), 373–386 (2019)
5. Calderini, M., Civino, R., Sala, M.: On Properties of Translation Groups in the Affine General Linear Group with Applications to Cryptography. Journal of Algebra (2021)
6. Calderini, M., Sala, M.: On Differential Uniformity of Maps that May Hide an Algebraic Trapdoor. In: CAI 2015. Lecture Notes in Computer Science, vol. 9270, pp. 70–78. Springer (2015)
7. Canteaut, A., Charpin, P., Dobbertin, H.: Weight Divisibility of Cyclic Codes, Highly Nonlinear Functions on $F_{2^m}$, and Crosscorrelation of Maximum-Length Sequences. SIAM J. Discrete Math. **13**(1), 105–138 (2000)
8. Chauhan, D., Gupta, I., Verma, R.: Construction of Cryptographically Strong S-boxes from Ternary Quasigroups of Order 4. Cryptologia **569**, 658–680 (2021)
9. Chauhan, D., Gupta, I., Verma, R.: Quasigroups and Their Applications in Cryptography. Cryptologia **45**(3), 227–265 (2021)
10. Civino, R., Blondeau, C., Sala, M.: Differential attacks: using alternative operations. Des. Codes Cryptogr. **87**(2-3), 225–247 (2019)
11. Dénes, J., Keedwell, A.D.: Latin Squares: New Developments in the Theory and Applications, Annals of Discrete Mathematics, vol. 46. Elsevier (1991)
12. Dénes, J., Keedwell, A.D.: A New Authentication Scheme Based on Latin Squares. Discrete Mathematics **106**, 157–161 (1992)
13. Dobbertin, H.: One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. Appl. Algebra Eng. Commun. Comput. **9**(2), 139–152 (1998)
14. Dudek, W.: Parastrophes of Quasigroups. Quasigroups and Related Systems **23**(2), 221–230 (2015)
15. Falcón, R.M., Falcón, Ó.J., Núñez, J.: A Historical Perspective of the Theory of Isotopisms. Symmetry **10**(8), 322 (2018)
16. Gligoroski, D., Markovski, S., Knapskog, S.J.: The Stream Cipher Edon80. In: New Stream Cipher Designs, Lecture Notes in Computer Science, vol. 4986, pp. 152–169. Springer (2008)

17. Gligoroski, D., Markovski, S., Kocarev, L.: Edon-R, An Infinite Family of Cryptographic Hash Functions. I.J. Network Security **8**(3), 293–300 (2009)
18. Hawkes, P., O'Connor, L.: XOR and Non-XOR Differential Probabilities. In: EUROCRYPT 1999. Lecture Notes in Computer Science, vol. 1592, pp. 272–285. Springer (1999)
19. Howitt, S.M., Wilson, A.N.: Revisiting "Is the Scientific Paper a Fraud?". EMBO Reports **15**(5), 481–484 (2014)
20. Hulpke, A., Kaski, P., Östergård, P.: The Number of Latin Squares of Order 11. Mathematics of Computation **80**(274), 1197–1219 (2011)
21. Knudsen, L.R., Robshaw, M.: The Block Cipher Companion. Springer Science & Business Media (2011)
22. Kościelny, C.: A Method of Constructing Quasigroup-Based Stream-Ciphers. Applied Mathematics and Computer Science **6**, 109–122 (1996)
23. Lai, X., Massey, J.L.: A Proposal for a New Block Encryption Standard. In: EUROCRYPT 1990. Lecture Notes in Computer Science, vol. 473, pp. 389–404. Springer (1991)
24. Lai, X., Massey, J.L., Murphy, S.: Markov Ciphers and Differential Cryptanalysis. In: EUROCRYPT 1991. Lecture Notes in Computer Science, vol. 547, pp. 17–38. Springer (1991)
25. McKay, B.D., Meynert, A., Myrvold, W.: Small Latin Squares, Quasigroups, and Loops. Journal of Combinatorial Designs **15**(2), 98–119 (2007)
26. McKay, B.D., Wanless, I.M.: On the Number of Latin Squares. Annals of Combinatorics **9**(3), 335–344 (2005)
27. Medawar, P.: Is the Scientific Paper a Fraud? The Listener **70**(12), 377–378 (1963)
28. Mouha, N.: On Proving Security against Differential Cryptanalysis. In: CFAIL 2019 (2019)
29. Nyberg, K.: Perfect Nonlinear S-boxes. In: EUROCRYPT 1991. Lecture Notes in Computer Science, vol. 547, pp. 378–386. Springer (1991)
30. O'Connor, L.: On the Distribution of Characteristics in Bijective Mappings. Journal of Cryptology **8**(2), 67–86 (1995)
31. O'Connor, L.: On the Distribution of Characteristics in Bijective Mappings. In: EUROCRYPT 1993. Lecture Notes in Computer Science, vol. 765, pp. 360–370. Springer (1994)
32. Schwartz, M.A.: The Importance of Stupidity in Scientific Research. Journal of Cell Science **121**(11), 1771–1771 (2008)
33. Smith, J.D.: Four Lectures on Quasigroup Representations. Quasigroups Related Systems **15**, 109–140 (2007)
34. Tao, T.: Ask Yourself Dumb Questions - and Answer Them! https://terrytao.wordpress.com/career-advice/ask-yourself-dumb-questions-and-answer-them/
35. Tao, T.: Use The Wastebasket. https://terrytao.wordpress.com/career-advice/use-the-wastebasket/
36. Teşeleanu, G.: Quasigroups and Substitution Permutation Networks: A Failed Experiment. Cryptologia **45**(3), 266–281 (2021)
37. Teşeleanu, G.: The Security of Quasigroups Based Substitution Permutation Networks. In: SecITC 2022. Lecture Notes in Computer Science, vol. 13809, pp. 306–319. Springer (2022)
38. Teşeleanu, G.: Cryptographic Symmetric Structures Based on Quasigroups. Cryptologia **47**(4), 365–392 (2023)
39. Truran, P.: Practical Applications of the Philosophy of Science: Thinking About Research. Springer Science & Business Media (2013)

40. Vaudenay, S.: A Classical Introduction to Cryptography: Applications for Communications Security. Springer Science & Business Media (2005)
41. Vojvoda, M., Sỳs, M., Jókay, M.: A Note on Algebraic Properties of Quasigroups in Edon80. Tech. rep., eSTREAM report 2007/005 (2007)
42. Weidman, D.R.: Emotional Perils of Mathematics. Science **149**(3688), 1048–1048 (1965)