Cryptographic Symmetric Structures Based on Quasigroups

George Teşeleanu[1,2]

[1] Advanced Technologies Institute
10 Dinu Vintilă, Bucharest, Romania
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy
21 Calea Grivitei, Bucharest, Romania
george.teseleanu@yahoo.com

Abstract. In our paper we study the effect of changing the commutative group operation used in Feistel and Lai-Massey symmetric structures into a quasigroup operation. We prove that if the quasigroup operation is isotopic with a group $\mathbb{G}$, the complexity of mounting a differential attack against our generalization of the Feistel structure is the same as attacking the unkeyed version of the general Feistel iteration based on $\mathbb{G}$. Also, when $\mathbb{G}$ is non-commutative we show that both versions of the Feistel structure are equivalent from a differential point of view. For the Lai-Massey structure we introduce four non-commutative versions, we argue for the necessity of working over a group and we provide some necessary conditions for the differential equivalency of the four notions.

Keywords: Feistel structure, Lai-Massey structure, quasigroups, block ciphers, differential cryptanalysis

1 Introduction

The most popular cryptographic symmetric structures used for constructing block ciphers are substitution-permutation networks (SPNs), Feistel and Lai-Massey. In its most basic form, an SPN uses a series of substitutions and permutations layers, while Feistel and Lai-Massey structures employ a random round function to construct a permutation [36].

One of the most effective tool against symmetric key cryptographic algorithms is differential cryptanalysis [23]. The basic idea of this attack is to investigate how certain changes in the plaintext propagate through a cipher [2]. When considering an ideal cipher, the probability of predicting these changes is $1/2^n$, where n is the number of input bits. Hence, in this case, it is not possible for an attacker to use these predictions when n is, for example, 128. Unfortunately, designers use theoretical estimates based on certain assumptions that do not always hold in practice and this makes ciphers far from ideal. Thus, security against differential cryptanalysis is one of the basic design criterion for symmetric primitives.

Quasigroups are group-like structures that, unlike groups, are not required to be associative and to possess an identity element. The usage of quasigroups as building blocks for cryptographic primitives is not very common. Regardless of that, various such cryptosystems can be found in the literature [1, 8, 9, 11, 14, 15, 19, 20].

In [32] the author introduces a straightforward generalization of SPNs and studies its security. The main ingredient of the generalisation was to replace the group operation between keys and (intermediary) plaintexts with a quasigroup operation. When the quasigroup operation is isotopic with a group operation[3], the author proves a negative result: the new SPN structure is equivalent from a differential point of view with an SPN using the group operation and a substitution box (s-box) different from the initial one. Hence, the generalization either brings no extra security, if we initialize the SPN with a random secret s-box, or it might affect the SPN's security, in the case of static s-boxes.

Another very recent approach [4–6, 10] uses commutative regular subgroups of the symmetric group to design SPN structures that appear secure against classical differential cryptanalysis, but are weaker with respect to a differential attack that uses a different group operation. More precisely, such an SPN has a security level, with respect to differential attacks, that is dependent on the considered operation. This methodology is similar to ours, since we also consider different operations to construct differential attacks against the proposed symmetric structures. Note that the scope of the papers [4–6, 10] is to show how a designer can embed a trapdoor into symmetric structures[4], while ours is to examine whether changing the group operation to a quasigroup one, one could reinforce the symmetric structures against differential cryptanalysis.

In this paper, using the results presented in [32], we prove that even if we use a non-commutative group, the two resulting SPN structures are differentially equivalent. Then, we generalize Feistel and Lai-Massey symmetric structures by employing the same technique of changing the group operations with a quasigroup ones. In the case of Feistel structures, we obtain equivalency with the unkeyed version of the general Feistel iteration that is described in [27, 36]. Note that the variations of the unkeyed general Feistel iteration are stable[5] under isotopies. Also, as in the case of SPNs, the two non-commutative Feistel structures are equivalent. When we tried to generalize the Lai-Massey structure we could not find a method that replaces the group operation with a quasigroup one and at the same time guarantees correct decryption. When the group operation is non-commutative we obtain four variations of the Lai-Massey structure. The only equivalence results that we obtained are when one layer is a group morphism or the group is commutative. Hence, we leave some open problems.

Although we present a series of negative results, we think that their usefulness is twofold. 1 In most scientific reports and papers, authors present their results as if they achieved them in a straightforward manner and not through a messy

[3] Note that this is the most popular method for generating quasigroups.

[4] The trapdoor consists in knowing the group operation that weakens the structure.

[5] *i.e* we obtain the same structure, but instantiated with different functions

process. This gives people a distorted view of scientific research [18,22,30,38] and leads to a view that implies that failure, serendipity and unexpected results are not a normal part of science [18,28]. Hence, this report provides readers with an indication of the real processes involved in the designing phase of a cryptographic primitive. 2 Negative results and false directions are rarely reported [18,34], and thus people are bound to repeat the same mistakes. By presenting our results, we hope to prevent others from making the same mistakes by showing them where these paths lead. This philosophy is based on an advise given in [31], where the author recommends that people write down their mistakes so that they avoid making them again in the future.

Structure of the paper. We introduce notations and definitions in Section 2. In Section 3 we generalize the Feistel structure and study its differential properties. A generic Lai-Massey structure is introduced in Section 4 and its security is analyzed. We conclude in Section 5.

2 Preliminaries

Notations. Throughout the paper $|\mathbb{G}|$ will denote the cardinality of a 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 π we further use the shorthand $\pi = \{a_0, a_1, \ldots, a_\ell\}$ which translates into $\pi(i) = a_i$ for all i. We also define the identity permutation $Id = \{0, \ldots, \ell\}$.

Let $X \in \mathbb{G}^2$. By X_l and X_r we understand the left and, respectively, right half of X. Additionally, let $\bullet$ and $\lhd$ be binary operators. We define the binary operators $\Delta_\bullet(X, Y) = X \bullet Y$ and $\Delta_{\bullet,\lhd}(X, Y) = (X_l \bullet Y_l, X_r \lhd Y_r)$.

2.1 Quasigroups

In this section we introduce a few basic notions about quasigroups. We base our exposition on [29].

Definition 1. *A quasigroup $(\mathbb{G}, \otimes)$ is a set $\mathbb{G}$ equipped with a binary operation of multiplication $\otimes\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}$, 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 $x \odot z = y$ 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*

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

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

Definition 3. *Let* $(\mathbb{G}, \otimes)$, $(\mathbb{H}, \star)$ *be two quasigroups. An ordered triple of bijections* π, ρ, ω *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 isotopy exists, then* $(\mathbb{G}, \otimes)$, $(\mathbb{H}, \star)$ *are called isotopic.*

A popular method for constructing quasigroups [14, 15, 19, 37] is the following. Choose a group $(\mathbb{G}, \star)$ (*e.g.* $(\mathbb{Z}_{2^n}, \oplus)$ or $(\mathbb{Z}_{2^n}, +)$) and three arbitrary permutations $\pi, \rho, \omega \colon \mathbb{G} \to \mathbb{G}$. Then, define the quasigroup operation as $x \otimes y = \omega^{-1}(\pi(x) \star \rho(y))$. To see why this leads to a quasigroup, we note that x, y and z are mapped uniquely to $\pi(x)$, $\rho(y)$ and $\omega(z)$, and thus any equation of the form $\pi(x) \star \rho(y) = \omega(z)$ is in fact uniquely resolved in the base group $\mathbb{G}$ given any of $\pi(x)$, $\rho(y)$ and $\omega(z)$.

2.2 Group Differential Cryptanalysis

Differential cryptanalysis was first introduced in [2] for $(\mathbb{Z}_{2^n}, \oplus)$. The notion was further extended to commutative groups in [21] and to non-commutative groups in [32]. Let $(\mathbb{G}, \star)$ be a group. We further present the notions of left and right differential probabilities for a permutation. Note that the 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 $\sigma \colon \mathbb{G} \to \mathbb{G}$ *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 σ be randomly chosen. When $(\mathbb{G}, \star) = (\mathbb{Z}_{2^n}, \star)$, the distribution of DP values is studied in [25, 26] and when $(\mathbb{G}, \star)$ is a generic commutative group in [17]. When σ is static[6], the distribution of DPs for $(\mathbb{Z}_{2^n}, \oplus)$ is studied for example in [7, 12, 24].

We further state, without proof, a lemma that will be useful later on. Intuitively, the lemma states that group differentials are key independent.

Lemma 3. *The following identities hold*

$$\Delta_\star((K \star X)^{-1}, K \star X') = \Delta_\star(X^{-1}, X')$$

$$\Delta_\star(X \star K, (X' \star K)^{-1}) = \Delta_\star(X, X'^{-1}).$$

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

The following lemma tells us that the notions of LDP and RDP are equivalent if we work with random secret permutations. Otherwise, the original static permutation is transformed into a different one, not necessary better. In the case of SPNs, this translates into the differential equivalence of the left and right SPNs. Note that this is not mentioned in [32].

Lemma 4. *Let $\sigma'(x) = \sigma(x^{-1})^{-1}$. Then*

$$LDP_\star(\sigma, \alpha, \beta) = RDP_\star(\sigma', \alpha, \beta).$$

Proof. Let $Y = X^{-1}$ and $Y' = X'^{-1}$. Then $\alpha = X^{-1} \star X' = Y \star Y'^{-1}$. Also, note that $\beta = \sigma(X)^{-1} \star \sigma(X') = \sigma(Y^{-1})^{-1} \star \sigma(Y'^{-1}) = \sigma'(Y) \star \sigma'(Y)^{-1}$. Hence, we obtain the equality. □

3 Feistel Structure

3.1 Description

Let $(\mathbb{G}, \otimes_l)$ and $(\mathbb{G}, \otimes_r)$ be two quasigroups. A quasigroup Feistel symmetric structure (see Figure 1) is an iterated structure that processes a plaintext $P \in \mathbb{G}^2$ for t rounds. Let F_i be random functions from $\mathbb{G}$ to $\mathbb{G}$. The first step is to break P into two halves L_0 and R_0. Then, for $i \in [1, t]$ compute

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

where $F_i(k_i, R_{i-1}) = F_i(k_i \otimes_r R_{i-1})$ or $F_i(k_i, R_{i-1}) = F_i(R_{i-1} \otimes_r k_i)$. These versions of the Feistel structure will further be called left Feistel structures. We can also define the right versions

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

Note that when $\otimes_l = \otimes_r$ and $\otimes_l$ is commutative, we obtain the standard Feistel structure. In this case, the structure's differential security can be reduced to the differential security of the non-linear F_is [2].

3.2 Analysis

In this section we extend the notion of differential cryptanalysis to quasigroup Feistel structures. Then, we show that our generalization is correct, study the security of Feistel structures based on quasigroups isotopic to a group and finally we study the equivalence between Feistel structures based on a non-commutative group.

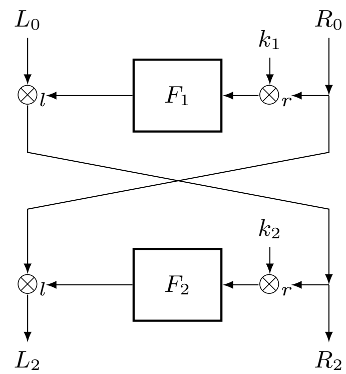


Fig. 1: Quasigroup Feistel structure

Definition 5. *Let K be a key, $X_l, X'_l \in (\mathbb{G}, \otimes_l)$ and $X_r, X'_r \in (\mathbb{G}, \otimes_r)$. We define the Feistel quasigroup differential probabilities*

$$FDP_{\obslash_l,\obslash_r}(F,\alpha,\beta,K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G}^2 \\ \Delta_{\obslash_l,\obslash_r}(X,X')=\alpha}} [\Delta_{\obslash_l}(X_l \otimes_l F(K \otimes_r X_r), \\ X'_l \otimes_l F(K \otimes_r X'_r)) = \beta],$$

$$FDP_{\obslash_l,\oslash_r}(F,\alpha,\beta,K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G}^2 \\ \Delta_{\obslash_l,\oslash_r}(X,X')=\alpha}} [\Delta_{\obslash_l}(X_l \otimes_l F(X_r \otimes_r K), \\ X'_l \otimes_l F(X'_r \otimes_r K)) = \beta],$$

$$FDP_{\oslash_l,\obslash_r}(F,\alpha,\beta,K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G}^2 \\ \Delta_{\oslash_l,\obslash_r}(X,X')=\alpha}} [\Delta_{\oslash_l}(F(K \otimes_r X_r) \otimes_l X_l, \\ F(K \otimes_r X'_r) \otimes_l X'_l) = \beta],$$

$$FDP_{\oslash_l,\oslash_r}(F,\alpha,\beta,K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G}^2 \\ \Delta_{\oslash_l,\oslash_r}(X,X')=\alpha}} [\Delta_{\oslash_l}(F(X_r \otimes_r K) \otimes_l X_l, \\ F(X'_r \otimes_r K) \otimes_l X'_l) = \beta],$$

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

Remark 2. In Definition 5 we only took into consideration the right half R_i, since any modification to R_{i-1} translates into $L_i = R_{i-1}$ with probability 1.

Lemma 5. *Let $(R, R') \in \{(K \otimes_r X_r, K \otimes_r X'_r), (X_r \otimes_r K, X'_r \otimes_r K)\}$. If $(\mathbb{G}, \otimes_l)$ forms a commutative group then the following identities hold*

$$\Delta_{\obslash_l}(X_l \otimes_l F(R), X'_l \otimes_l F(R')) = \Delta_{\otimes_l}(X_l^{-1}, {X'}_l) \otimes_l \Delta_{\otimes_l}(F(R), F(R')^{-1}).$$

Proof. Note that

$$
\begin{aligned}
\Delta_{\obslash_l}(X_l, X_l') = \alpha_l &\iff X_l \otimes_l \alpha_l = X_l' \\
&\iff X_l^{-1} \otimes_l X_l' = \alpha_l \iff \Delta_{\otimes_l}(X_l^{-1}, X_l') = \alpha_l.
\end{aligned}
$$

This relation leads to

$$
\begin{aligned}
\Delta_{\obslash_l}(X_l \otimes_l F(R), X_l' \otimes_l F(R')) = \beta \\
&\iff X_l \otimes_l F(R) \otimes_l \beta = X_l' \otimes_l F(R') \\
&\iff F(R) \otimes_l \beta \otimes_l X_l = F(R') \otimes_l X_l' \\
&\iff F(R)^{-1} \otimes_l F(R') = \alpha_l^{-1} \otimes_l \beta \\
&\iff \Delta_{\otimes_l}(X_l^{-1}, X_l') \otimes_l \Delta_{\otimes_l}(F(R)^{-1}, F(R')) = \beta.
\end{aligned}
$$

□

To see if Definition 5 is a generalization of the standard Feistel differential probability, we must recover DP when $\otimes_l = \otimes_r$ and $\otimes_l$ is commutative. This is proven in Corollary 1.

Corollary 1. *If $(\mathbb{G}, \otimes_l)$ forms a commutative group and $\otimes_r = \otimes_l = \otimes$ then the following identities hold*

$$
\begin{aligned}
FDP_{\obslash,\obslash}(F, \alpha, \beta, K) = FDP_{\oslash,\obslash}(F, \alpha, \beta, K) = LDP_{\obslash}(F, \alpha_r, \alpha_l^{-1} \otimes_l \beta), \\
FDP_{\obslash,\oslash}(F, \alpha, \beta, K) = FDP_{\oslash,\oslash}(F, \alpha, \beta, K) = RDP_{\oslash}(F, \alpha_r, \alpha_l^{-1} \otimes_l \beta).
\end{aligned}
$$

Proof. Using Lemmas 3 and 5 we obtain

$$
\begin{aligned}
&FDP_{\obslash,\obslash}(F, \alpha, \beta, K) = \\
&\quad = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X, X' \in \mathbb{G}^2 \\ \Delta_{\obslash,\obslash}(X, X') = \alpha}} [\Delta_{\obslash}(X_l \otimes F(K \otimes X_r), X_l' \otimes F(K \otimes X_r')) = \beta] \\
&\quad = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X, X' \in \mathbb{G}^2 \\ \Delta_{\obslash,\obslash}(X, X') = \alpha}} [\Delta_{\otimes}(X_l^{-1}, X'_l) \otimes \Delta_{\otimes}(F(K \otimes X_r)^{-1}, F(K \otimes X_r')) = \beta] \\
&\quad = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X_r, X_r' \in \mathbb{G} \\ \Delta_{\obslash}(X_r, X_r') = \alpha_r}} \sum_{X_l \in \mathbb{G}} [\Delta_{\otimes}(F(K \otimes X_r)^{-1}, F(K \otimes X_r')) = \alpha_l^{-1} \otimes \beta] \\
&\quad = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X_r, X_r' \in \mathbb{G} \\ \Delta_{\obslash}(X_r, X_r') = \alpha_r}} |\mathbb{G}| [\Delta_{\otimes}(F(K \otimes X_r)^{-1}, F(K \otimes X_r')) = \alpha_l^{-1} \otimes \beta] \\
&\quad = \frac{1}{|\mathbb{G}|} \sum_{\substack{X_r, X_r' \in \mathbb{G} \\ \Delta_{\obslash}(X_r, X_r') = \alpha_r}} [\Delta_{\otimes}(F(K \otimes X_r)^{-1}, F(K \otimes X_r')) = \alpha_l^{-1} \otimes \beta]
\end{aligned}
$$

$$= \frac{1}{|\mathbb{G}|} \sum_{\substack{Y_r, Y'_r \in \mathbb{G} \\ \Delta_\oslash(Y_r, Y'_r) = \alpha_r}} [\Delta_\otimes(F(Y_r)^{-1}, F(Y'_r)) = \alpha_l^{-1} \otimes \beta]$$
$$= LDP_\oslash(F, \alpha_r, \alpha_l^{-1} \otimes \beta).$$

The remaining equalities are proven in a similar way. $\square$

Let $i \in \{l, r\}$ and $x \otimes_i y = \omega_i^{-1}(\pi_i(x) \star_i \rho_i(y))$. We further study the impact of the ω_is, π_is and ρ_is permutations on FDP.

Lemma 6. *Let $i \in \{l, r\}$, $\pi'_i = \pi_i \circ \omega_i^{-1}$, $\rho'_i = \rho_i \circ \omega_i^{-1}$, $F' = \omega_l \circ F \circ \omega_r^{-1}$. We define $x *_i y = \pi'_i(x) \star_i \rho'_i(y) = z$, $x \backslash_i z = y$ and $z /_i y = x$. Then the following identities hold*

$$\begin{aligned}
FDP_{\oslash_l,\oslash_r}(F, \alpha, \beta, K) &= FDP_{\backslash_l,\backslash_r}(F', \omega_l(\alpha_l) \| \omega_r(\alpha_r), \omega_l(\beta), \omega_l(K)),\\
FDP_{\oslash_l,\oslash_r}(F, \alpha, \beta, K) &= FDP_{\backslash_l,/_r}(F', \omega_l(\alpha_l) \| \omega_r(\alpha_r), \omega_l(\beta), \omega_l(K)),\\
FDP_{\oslash_l,\oslash_r}(F, \alpha, \beta, K) &= FDP_{/_l,\backslash_r}(F', \omega_l(\alpha_l) \| \omega_r(\alpha_r), \omega_l(\beta), \omega_l(K)),\\
FDP_{\oslash_l,\oslash_r}(F, \alpha, \beta, K) &= FDP_{/_l,/_r}(F', \omega_l(\alpha_l) \| \omega_r(\alpha_r), \omega_l(\beta), \omega_l(K)).
\end{aligned}$$

Proof. Let $Z = X_l \otimes_l F(X_r \otimes_r K)$ and $Z' = X'_l \otimes_l F(X'_r \otimes_r K)$. First we rewrite

$$FDP_{\oslash_l,\oslash_r}(F, \alpha, \beta, K) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X_l, X'_l \in \mathbb{G} \\ \Delta_{\otimes_l}(X_l, \alpha_l) = X'_l}} \sum_{\substack{X_r, X'_r \in \mathbb{G} \\ \Delta_{\otimes_r}(\alpha_r, X'_r) = X_r}} [\Delta_{\otimes_l}(Z, \beta) = Z'].$$

Let $\omega_i(X_i) = Y_i$, $\omega_i(X'_i) = Y'_i$ and $\omega_i(\alpha_i) = A_i$. Then

$$\begin{aligned}
X_l \otimes_l \alpha_l = X'_l &\Longleftrightarrow \pi_l(X_l) \star_l \rho_l(\alpha_l) = \omega_l(X'_l)\\
&\Longleftrightarrow \pi'_l(\omega_l(X_l)) \star_l \rho'_l(\omega_l(\alpha_l)) = \omega_l(X'_l)\\
&\Longleftrightarrow \pi'_l(Y_l) \star_l \rho'_l(A_l) = Y'_l\\
&\Longleftrightarrow Y_l *_l A_l = Y'_l
\end{aligned} \tag{1}$$

and

$$\begin{aligned}
\alpha_r \otimes_r X'_r = X_r &\Longleftrightarrow \pi_r(\alpha_r) \star_r \rho_r(X'_r) = \omega_r(X_r)\\
&\Longleftrightarrow \pi'_r(A_r) \star_r \rho'_r(Y'_r) = Y_r\\
&\Longleftrightarrow A_r *_r Y'_r = Y_r.
\end{aligned} \tag{2}$$

Let $\omega_r(K) = K'$. Then we obtain

$$\begin{aligned}
F(X_r \otimes_r K) &= F(\omega_r^{-1}(\pi_r(X_r) \star_r \rho_r(K)))\\
&= \omega_l^{-1}(F'(\pi'_r(\omega_r(X_r)) \star_r \rho'_r(\omega_r(K))))\\
&= \omega_l^{-1}(F'(Y_r *_r K'))
\end{aligned}$$

and using this

$$
\begin{aligned}
Z &= \omega_l^{-1}(\pi_l(X_l) \star_l \rho_l(F(X_r \otimes_r K))) \\
&= \omega_l^{-1}(\pi_l'(\omega(X_l)) \star_l \rho_l'(F'(Y_r *_r K'))) \\
&= \omega_l^{-1}(Y_l *_l F'(Y_r *_r K')). \qquad (3)
\end{aligned}
$$

Similarly

$$
Z' = \omega_l^{-1}(Y_l' *_l F'(Y_r' *_r K')). \qquad (4)
$$

Let $\omega_l(\beta) = B$. Using Equations (3) and (4) we obtain

$$
\begin{aligned}
Z \otimes_l \beta = Z' &\iff \pi_l'(Y_l *_l F'(Y_r *_r K')) \star \rho_l'(\omega_l(\beta)) = Y_l' *_l F'(Y_r' *_r K') \\
&\iff (Y_l *_l F'(Y_r *_r K')) *_l B = Y_l' *_1 F'(Y_r' *_r K'). \qquad (5)
\end{aligned}
$$

Let $T = Y_l *_l F'(Y_r *_r K')$ and $T' = Y_l' *_l F'(Y_r' *_r K')$. Using Equations (1), (2) and (5) we obtain

$$
\begin{aligned}
FDP_{\otimes_l,\oslash_r}(F,\alpha,\beta,K) &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{Y_l,Y_l' \in \mathbb{G} \\ \Delta_{*_l}(Y_l,A_l)=Y_l'}} \sum_{\substack{Y_r,Y_r' \in \mathbb{G} \\ \Delta_{*_r}(A_r,Y_r')=Y_r}} [\Delta_{*_l}(T,B) = T'] \\
&= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{Y,Y' \in \mathbb{G}^2 \\ \Delta_{\backslash_l,/_r}(Y,Y')=A}} [\Delta_{\backslash_l}(T,T') = B] \\
&= FDP_{\backslash_l,/_r}(F',A,B,K').
\end{aligned}
$$

The remaining equalities are proven using similar techniques. $\square$

Lemma 6 tells us that it is irrelevant from a differential point of view[7] if we define the quasigroup operation with $\omega_i \neq Id$ or $\omega_i = Id$. Thus, we further restrict our study[8] to the quasigroup operations $x \otimes_i y = \pi_i(x) \star_i \rho_i(y)$.

Lemma 7. *Let $\rho_r' = \rho_r \circ \pi_r^{-1}$, $F' = \rho_l \circ F \circ \pi_r^{-1}$. We define $x *_{l1} y = \pi_l(x) \star_l y = z$, $x \backslash_{l1} z = y$ and $z /_{l1} y = x$. Also, let $x *_{r2} y = \pi_r(x \star_r \rho_r'(y)) = z$, $x \backslash_{r2} z = y$ and $z /_{r2} y = x$. Then the following identity holds*

$$
FDP_{\otimes_l,\oslash_r}(F,\alpha,\beta,K) = FDP_{\backslash_{l1},/_{r1}}(F',\pi_r(\alpha_r)\|\rho_l(\alpha_l),\rho_l(\beta),\pi_r(K)).
$$

Proof. Let $\rho_l(\alpha_l) = A_l$, $\pi_r(\alpha_r) = A_r$, $\pi_r(X_r) = Y_r$ and $\pi_r(X_r') = Y_r'$. Then

$$
\begin{aligned}
X_l \otimes_l \alpha_l = X_l' &\iff \pi_l(X_l) \star_l \rho_l(\alpha_l) = X_l' \\
&\iff \pi_l(X_l) \star_l A_l = X_l' \\
&\iff X_l *_{l1} A_l = X_l' \qquad (6)
\end{aligned}
$$

---

[7] *e.g.* we obtain the same differential probability FDP

[8] without loss of generality

and

$$\begin{aligned}\alpha_r \otimes_r X'_r = X_r &\iff \pi_r(\alpha_r) \star_r \rho_r(X'_r) = X_r \\ &\iff \pi_r(A_r \star_r \rho'_r(\pi_r(X'_r))) = \pi_r(X_r) \\ &\iff \pi_r(A_r \star_r \rho'_r(Y'_r)) = Y_r \\ &\iff A_r *_{r2} Y'_r = Y_r. \end{aligned} \tag{7}$$

Let $\pi_r(K) = K'$. Then we obtain

$$\begin{aligned}F(X_r \otimes_r K) &= F(\pi_r(X_r) \star_r \rho_r(K)) \\ &= F(\pi_r^{-1}(Y_r \star_r \rho'_r(\pi_r(K)))) \\ &= \rho_l^{-1}(F'(Y_r *_{r2} K'))\end{aligned}$$

and using this

$$\begin{aligned}Z &= \pi_l(X_l) \star_l \rho_l(F(X_r \otimes_r K)) \\ &= \pi_l(X_l) \star_l F'(Y_r *_{r2} K') \\ &= X_l *_{l1} F'(Y_r *_{r2} K'). \end{aligned} \tag{8}$$

Similarly

$$Z' = X'_l *_{l1} F'(Y'_r *_{r2} K'). \tag{9}$$

Let $\rho_l(\beta) = B$. Using Equations (8) and (9) we obtain

$$\begin{aligned}Z \otimes_l \beta = Z' &\iff \pi_l(X_l *_{l1} F'(Y_r *_{r2} K')) \star_l \rho_l(\beta) = X'_l *_{l1} F'(Y'_r *_{r2} K') \\ &\iff (X_l *_{l1} F'(Y_r *_{r2} K')) *_{l1} B = X'_l *_{l1} F'(Y'_r *_{r2} K'). \end{aligned} \tag{10}$$

Let $T = X_l *_{l1} F'(Y_r *_{r2} K')$ and $T' = X'_l *_{l1} F'(Y'_r *_{r2} K')$. Using Equations (6), (7) and (10) we obtain

$$\begin{aligned}FDP_{\otimes_l,\oslash_r}(F,\alpha,\beta,K) &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X_l, X'_l \in \mathbb{G} \\ \Delta_{*_{l1}}(X_l, A_l) = X'_l}} \sum_{\substack{Y_r, Y'_r \in \mathbb{G} \\ \Delta_{*_{r2}}(A_r, Y'_r) = Y_r}} [\Delta_{*_{l1}}(T,B) = T'] \\ &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S, S' \in \mathbb{G}^2 \\ \Delta_{\backslash_{l1},/_{r2}}(S,S') = A}} [\Delta_{\backslash_{l1}}(T,T') = B] \\ &= FDP_{\backslash_{l1},/_{r2}}(F', A, B, K'),\end{aligned}$$

where $S = Y_r \| X_r$ and $S' = Y'_r \| X'_r$. □

Lemmas 8 to 10 are proven similarly to Lemma 7 and thus their proofs are omitted.

Lemma 8. *Let $\pi'_r = \pi_r \circ \rho_r^{-1}$, $F' = \rho_l \circ F \circ \rho_r^{-1}$. We define $x *_{l1} y = \pi_l(x) \star_l y = z$, $x \backslash_{l1} z = y$ and $z /_{l1} y = x$. Also, let $x *_{r1} y = \rho_r(\pi'_r(x) \star_r y) = z$, $x \backslash_{r1} z = y$ and $z /_{r1} y = x$. Then the following identity holds*

$$FDP_{\otimes_l,\otimes_r}(F,\alpha,\beta,K) = FDP_{\backslash_{l1},\backslash_{r2}}(F', \rho_r(\alpha_r) \| \rho_l(\alpha_l), \rho_l(\beta), \rho_r(K)).$$

Lemma 9. *Let* $\rho'_r = \rho_r \circ \pi_r^{-1}$, $F' = \pi_l \circ F \circ \pi_r^{-1}$. *We define* $x *_{l2} y = x \star_l \rho_l(y) = z$, $x \backslash_{l2} z = y$ *and* $z /_{l2} y = x$. *Also, let* $x *_{r2} y = \pi_r(x \star_r \rho'_r(y)) = z$, $x \backslash_{r2} z = y$ *and* $z /_{r2} y = x$. *Then the following identity holds*

$$FDP_{\oslash_l, \oslash_r}(F, \alpha, \beta, K) = FDP_{/_{l2}, /_{r1}}(F', \pi_r(\alpha_r) \| \pi_l(\alpha_l), \pi_l(\beta), \pi_r(K)).$$

Lemma 10. *Let* $\rho'_r = \pi_r \circ \rho_r^{-1}$, $F' = \pi_l \circ F \circ \rho_r^{-1}$. *We define* $x *_{l2} y = x \star_l \rho_l(y) = z$, $x \backslash_{l2} z = y$ *and* $z /_{l2} y = x$. *Also, let* $x *_{r1} y = \rho_r(\pi'_r(x) \star_r y) = z$, $x \backslash_{r1} z = y$ *and* $z /_{r1} y = x$. *Then the following identity holds*

$$FDP_{\oslash_l, \otimes_r}(F, \alpha, \beta, K) = FDP_{/_{l2}, \backslash_{r2}}(F', \rho_r(\alpha_r) \| \pi_l(\alpha_l), \pi_l(\beta), \rho_r(K)).$$

Remark 3. We also tried to define a series of the differential probabilities in which $\otimes_l$ is changed into $\oslash_l$ and vice versa, but we could not find a method for removing π_l or ρ_l.

We can easily see that Lemmas 7 to 10 reduce the right side of the Feistel structure to either $F \circ \rho_r(\pi_r(K) \star_r X_R)$ or $F \circ \pi_r(X_R \star_r \rho(K))$, for some π_r, ρ_r and F. Hence, we can consider a much simpler approach. Define F' as $F \circ \rho_r$ in the first case and $F \circ \pi_r$ in the second case. Then, study the differential properties of F' instead of F. Using this approach we can restrict our study to $x \otimes_r y = \pi_r(x) \star_r y$ and, respectively, $x \otimes_r y = x \star_r \rho_r(y)$.

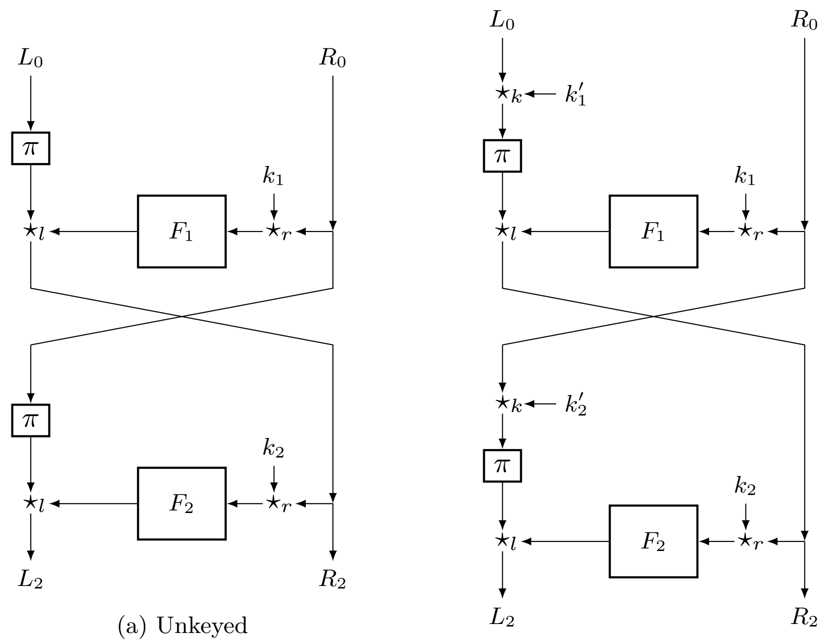
Since K and, for example, π_r are generated as a pair, for a differential attack to work we do not really need to know K. The value $\pi_r(K)$ suffices. Thus, the right side operation of the Feistel structure can be replaced with $\star_r$.

Let $x \otimes_1 y = \pi(x) \star_l y$ and $x \otimes_2 y = x \star_l \rho(y)$ and $\otimes_1$, $\oslash_1$ and, respectively, $\otimes_2$, $\oslash_2$ the associated divisions. Also, let $\otimes_i = \star_i$, where $i \in \{l, r\}$. Using Lemmas 3 and 7 to 10 we can redefine the FDP differential probabilities as

$$FDP_{\otimes_1, \otimes_r}(F, \alpha, \beta) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X, X' \in \mathbb{G}^2 \\ \Delta_{\otimes_1, \otimes_r}(X, X') = \alpha}} [\Delta_{\otimes_1}(X_l \otimes_1 F(X_r), X'_l \otimes_1 F(X'_r)) = \beta],$$

$$FDP_{\oslash_2, \oslash_r}(F, \alpha, \beta) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X, X' \in \mathbb{G}^2 \\ \Delta_{\oslash_2, \oslash_r}(X, X') = \alpha}} [\Delta_{\oslash_2}(F(X_r) \otimes_2 X_l, F(X'_r) \otimes_2 X'_l) = \beta].$$

The Feistel structure we obtained is depicted in Figure 2a and represents the unkeyed version of the general Feistel iteration (UGF) described in [36]. The keyed version (KGF) [27] is depicted in Figure 2b.



(a) Unkeyed

(b) Keyed

Fig. 2: Variations of the Feistel structure

A different point of view of studying the Feistel variations is to redefine the probabilities as

$$
\begin{aligned}
FDP_{\oslash_l,\oslash_r}(F,\alpha,\beta) &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G}^2 \\ \Delta_{\oslash_l,\oslash_r}(X,X')=\alpha}} [\Delta_{\oslash_l}(\pi(X_l) \otimes_l F(X_r), \\
&\qquad\qquad\qquad\qquad\qquad\qquad \pi(X'_l) \otimes_l F(X'_r)) = \beta], \\
FDP_{\oslash_l,\oslash_r}(F,\alpha,\beta) &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G}^2 \\ \Delta_{\oslash_l,\oslash_r}(X,X')=\alpha}} [\Delta_l \oslash (F(X_r) \otimes_l \rho(X_l), \\
&\qquad\qquad\qquad\qquad\qquad\qquad F(X'_r) \otimes_l \rho(X'_l)) = \beta].
\end{aligned}
$$

Lemma 11. *Let $G(x) = F(x)^{-1}$ and $\rho(x) = \pi(x^{-1})^{-1}$. Then*

$$FDP_{\oslash_l,\oslash_r}(F,\alpha,\beta) = FDP_{\oslash_l,\oslash_r}(G,\alpha,\beta).$$

Proof. Let $Y_r = X_r$, $Y_l = X_l^{-1}$, $Y'_r = X'_r$ and $Y'_l = {X'}_l^{-1}$. Then

$$\alpha_l = X_l^{-1} \otimes_l X'_l = Y_l \otimes_l {Y'}_l^{-1} = Y_l \oslash_l Y'_l$$

and

$$\begin{aligned}\beta &= (\pi(X_l) \otimes_l F(X_r))^{-1} \otimes_l \pi(X_l') \otimes_l F(X_r') \\ &= F(X_r)^{-1} \otimes_l \pi(X_l)^{-1} \otimes_l \pi(X_l') \otimes_l F(X_r') \\ &= G(Y_r) \otimes_l \rho(Y_l) \otimes_l \rho(Y_l')^{-1} \otimes_l G(Y_r')^{-1} \\ &= \Delta_{\oslash_l}(G(Y_r) \otimes_l \rho(Y_l), G(Y_r') \otimes_l \rho(Y_l')).\end{aligned}$$

Hence, we obtain the desired equality. $\square$

The next corollary tells us that the left and the right versions of the classical non-commutative Feistel structure are equivalent from a differential point of view.

Corollary 2. *Let $G(x) = F(x)^{-1}$. If $\pi = \rho = Id$ then*

$$FDP_{\obslash_l, \obslash_r}(F, \alpha, \beta) = FDP_{\oslash_l, \oslash_r}(G, \alpha, \beta).$$

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

Proposition 1. *A quasigroup Feistel structure derived from a group Feistel structure using an isotopy has the same differential security as a UGF based on the same group. Also, the left and right versions of the non-commutative unkeyed version of the general Feistel iteration are equivalent from a differential point of view.*

4 Lai-Massey Structure

4.1 Description

In this section we describe four generalizations of the Lai-Massey structure. Before doing that, we start with Lemma 12 that guarantees correct decryption. When we tried to generalize the Lai-Massey structure, the only condition that seemed to guarantee correct decryption was that $(\mathbb{G}, \otimes)$ should be group. Hence, we further impose this restriction.

Lemma 12. *Let $t \in \mathbb{G}$. If $(\mathbb{G}, \otimes)$ is a group, then the following properties hold*

1. *If $y_0 = x_0 \otimes t$ and $y_1 = x_1 \otimes t$, then $y_0 \oslash y_1 = x_0 \oslash x_1$;*
2. *If $y_0 = t \otimes x_0$ and $y_1 = t \otimes x_1$, then $y_1 \obslash y_0 = x_1 \obslash x_0$;*
3. *If $y_0 = x_0 \otimes t$ and $y_1 = t \obslash x_1$, then $y_0 \otimes y_1 = x_0 \otimes x_1$;*
4. *If $y_0 = t \otimes x_0$ and $y_1 = x_1 \oslash t$, then $y_1 \otimes y_0 = x_1 \otimes x_0$.*

Proof. Since $\mathbb{G}$ is a group we have $x \obslash z = x^{-1} \otimes z$ and $z \oslash y = z \otimes y^{-1}$. Thus,

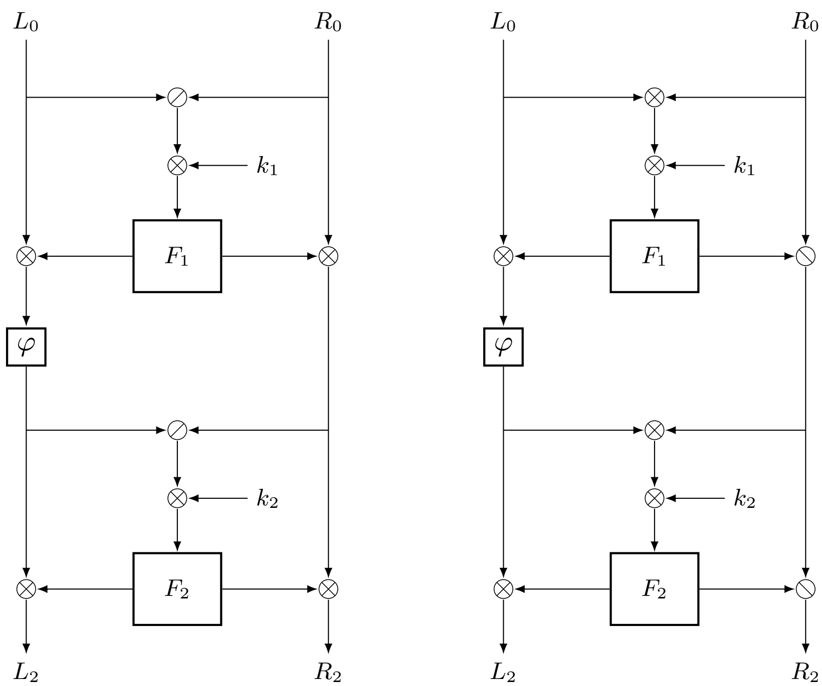
$$y_0 \oslash y_1 = y_0 \otimes y_1^{-1} = x_0 \otimes t \otimes t^{-1} \otimes x_1^{-1} = x_0 \otimes x_1^{-1} = x_0 \oslash x_1.$$

Similarly we can prove the remaining properties. $\square$

Remark 4. If we want, for example, $y_0 \oslash y_1 = x_0 \oslash x_1$ to hold, we obtain

$$\begin{aligned}\alpha \otimes y_1 = y_0 &\iff \alpha \otimes (x_1 \otimes t) = x_0 \otimes t \\ &\iff (\alpha \otimes (x_1 \otimes t)) \oslash t = (x_0 \otimes t) \oslash t \\ &\iff (\alpha \otimes (x_1 \otimes t)) \oslash t = x_0.\end{aligned}$$

Hence, without associativity we could not see how the relation could hold. But, if $\otimes$ is associative then $(\mathbb{G}, \otimes)$ forms a group [29]. That is the reason why we impose the restriction that $(\mathbb{G}, \otimes)$ should be a group.



(a) Symmetric version (b) Asymmetric version

Fig. 3: Non-commutative group Lai-Massey structures

Based on the Lemma 12 we introduce two non-commutative versions of the Lai-Massey structure: a symmetric one Figure 3a and an asymmetric one Figure 3b. Using Lemma 12 it is easy to see that all the structures are correctly defined.

Hence, in both cases the first step is to parse the plaintext into two halves L_0 and R_0. In the symmetric case, for t rounds we compute

$$L_i = \varphi(L_{i-1} \otimes F_i(k_i, L_{i-1} \oslash R_{i-1})) \text{ and } R_i = R_{i-1} \otimes F_i(k_i, L_{i-1} \oslash R_{i-1}),$$

where $\varphi\colon \mathbb{G} \to \mathbb{G}$ is a permutation and we define $F_i(k_i, x)$ as $F_i(k_i \otimes x)$ or $F_i(x \otimes k_i)$. We further call these versions the left symmetric Lai-Massey structures. We can also define the right symmetric Lai-Massey structures as follows

$$L_i = \varphi(F_i(k_i, L_{i-1} \obslash R_{i-1}) \otimes L_{i-1}) \text{ and } R_i = F_i(k_i, L_{i-1} \obslash R_{i-1}) \otimes R_{i-1}.$$

In the asymmetric case we define the outer versions as

$$L_i = \varphi(L_{i-1} \otimes F_i(k_i, L_{i-1} \otimes R_{i-1})) \text{ and } R_i = F_i(k_i, L_{i-1} \otimes R_{i-1}) \obslash R_{i-1}$$

and the inner versions as

$$L_i = \varphi(F_i(k_i, L_{i-1} \otimes R_{i-1}) \otimes L_{i-1}) \text{ and } R_i = R_{i-1} \oslash F_i(k_i, L_{i-1} \otimes R_{i-1}).$$

Let $\varphi = Id$. Then the Lai-Massey structure can be easily distinguished from a random permutation by simply checking if, for example, $L_2 \oslash R_2 = L_0 \oslash R_0$. In the case of commutative groups, Vaudeney [35, 36] introduced the usage of an orthomorphism φ to prevent this vulnerability. Following his approach, we extend the Lai-Massey structure to non-commutative groups.

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

Lemma 13. *Let t be the output of F. If $(\mathbb{G}, \otimes)$ is a group, then the following properties hold*

1. *If $y_0 = \varphi(x_0 \otimes t)$ and $y_1 = x_1 \otimes t$, then $y_0 \oslash y_1 = [\varphi(x_0 \otimes t) \oslash (x_0 \otimes t)] \otimes (x_0 \oslash x_1)$;*
2. *If $y_0 = \varphi(t \otimes x_0)$ and $y_1 = t \otimes x_1$, then $y_1 \obslash y_0 = (x_1 \obslash x_0) \otimes [(x_0 \otimes t) \obslash \varphi(x_0 \otimes t)]$;*
3. *If $y_0 = \varphi(x_0 \otimes t)$ and $y_1 = t \obslash x_1$, then $y_0 \otimes y_1 = [\varphi(x_0 \otimes t) \oslash (x_0 \otimes t)] \otimes (x_0 \otimes x_1)$;*
4. *If $y_0 = \varphi(t \otimes x_0)$ and $y_1 = x_1 \oslash t$, then $y_1 \otimes y_0 = (x_1 \otimes x_0) \otimes [(x_0 \otimes t) \obslash \varphi(x_0 \otimes t)]$.*

Proof. The first equality is proven as follows

$$\begin{aligned} y_0 \oslash y_1 = y_0 \otimes y_1^{-1} &= \varphi(x_0 \otimes t) \otimes t^{-1} \otimes x_0^{-1} \otimes x_0 \otimes x_1^{-1} \\ &= [\varphi(x_0 \otimes t) \otimes (x_0 \otimes t)^{-1}] \otimes (x_0 \otimes x_1^{-1}) \\ &= [\varphi(x_0 \otimes t) \oslash (x_0 \otimes t)] \otimes (x_0 \oslash x_1). \end{aligned}$$

Similarly we can prove the remaining properties. ∎

According to Lemma 13 we have, for example,

$$\begin{aligned} L_1 \oslash R_1 &= [\varphi(L_0 \otimes F(k, L_0 \oslash R_0)) \oslash (L_0 \otimes F(k, L_0 \oslash R_0))] \otimes (L_0 \oslash R_0) \\ &= \varphi'(L_0 \otimes F(k, L_0 \oslash R_0)) \otimes (L_0 \oslash R_0). \end{aligned}$$

If φ' is a permutation and $F(k, \cdot)$ is a random round function, then $L_1 \oslash R_1$ is uniformly distributed. Hence, we require that φ is a right orthomorphism.

According to the Hall-Paige theorem [16] a finite group admits an orthomorphism if its Sylow-2 subgroup is trivial or noncyclic. The converse was proven in [13, 39]. In particular $\mathbb{Z}_{2^m}$ has no orthomorphism [35]. To overcome this restriction, Vaudney relaxed the orthomorphism requirement for φ into a δ-almost orthomorphism requirement. To be consistent with the structure introduced by Vaudney, we further consider that φ is a non-commutative δ-almost orthomorphism (see Definition 7).

Definition 7. *A permutation φ is a δ-almost right orthomorphism if at most δ elements from $\mathbb{G}$ that have no preimage by the function $\varphi'(x) = \varphi(x) \oslash x$. If we change $\varphi'(x)$ to $x \owns \varphi(x)$, then φ is called a δ-almost left orthomorphism.*

4.2 Symmetric Structure Analysis

In this subsection we extend the differential probabilities to the symmetric Lai-Massey structures. Then, we study what happens when φ is a morphism or $\otimes$ is commutative and finally we show that our generalizations are correct.

Definition 8. *Let K be a key and $X^i, Y^i \in \mathbb{G}^2$ for $i \in \{0, 1\}$. We define the symmetric Lai-Massey quasigroup differential probabilities*

1. *Let $Z^i = X^i_l \oslash X^i_r$, $Y^i_l = \varphi(X^i_l \otimes F(K \otimes Z^i))$ and $Y^i_r = X^i_r \otimes F(K \otimes Z^i)$. Then*

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

2. *Let $Z^i = X^i_l \oslash X^i_r$, $Y^i_l = \varphi(X^i_l \otimes F(Z^i \otimes K))$ and $Y^i_r = X^i_r \otimes F(Z^i \otimes K)$. Then*

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

3. *Let $Z^i = X^i_r \owns X^i_l$, $Y^i_l = \varphi(F(K \otimes Z^i) \otimes X^i_l)$ and $Y^i_r = F(K \otimes Z^i) \otimes X^i_r$. Then*

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

4. *Let $Z^i = X^i_r \owns X^i_l$, $Y^i_l = \varphi(F(Z^i \otimes K) \otimes X^i_l)$ and $Y^i_r = F(Z^i \otimes K) \otimes X^i_r$. Then*

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

where $F\colon \mathbb{G} \to \mathbb{G}$ is a function, $\varphi\colon \mathbb{G} \to \mathbb{G}$ is a δ-almost orthomorphism, $\alpha, \beta \in \mathbb{G}^2$ and $\gamma \in \mathbb{G}$.

We further study the impact of φ on the symmetric Lai-Massey structures, when φ is a morphism, not just a δ-almost orthomorphism. Note that some φ examples provided in [35, 36] satisfy this property.

Lemma 14. *Let $\bullet \in \{\otimes, \oslash\}$. If φ is a morphism*[9]*, then we can rewrite the symmetric Lai-Massey differential probabilities as follows*

1. *Let $T^i = S^i_l \oslash S^i_r$, $Y^i_l = \varphi(S^i_l \otimes F(T^i))$ and $Y^i_r = S^i_r \otimes F(T^i)$. Then*

$$LLM_{\otimes,\bullet}(F,\alpha,\beta,\gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0,S^1 \in \mathbb{G}^2 \\ \Delta_{\otimes,\otimes}(S^0,S^1)=\alpha \\ \Delta_\bullet(T^0,T^1)=\gamma}} [\Delta_{\otimes,\otimes}(Y^0,Y^1)=\beta];$$

2. *Let $T^i = S^i_r \otimes S^i_l$, $Y^i_l = \varphi(F(T^i) \otimes S^i_l)$ and $Y^i_r = F(T^i) \otimes S^i_r$. Then*

$$RLM_{\oslash,\bullet}(F,\alpha,\beta,\gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0,S^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(S^0,S^1)=\alpha \\ \Delta_\bullet(T^0,T^1)=\gamma}} [\Delta_{\oslash,\oslash}(Y^0,Y^1)=\beta].$$

Proof. Lets consider $LLM_{\otimes,\otimes}$. We begin by rewriting $X^i_l = K^{-1} \otimes S^i_l$ and $X^i_r = S^i_r$. Then

$$\alpha_l = (X^0_l)^{-1} \otimes X^1_l = (S^0_l)^{-1} \otimes K \otimes K^{-1} \otimes S^1_l = (S^0_l)^{-1} \otimes S^1_l \tag{11}$$

and

$$Z^i = X^i_l \otimes (X^i_r)^{-1} = K^{-1} \otimes S^i_l \otimes (S^i_r)^{-1}. \tag{12}$$

Let $T^i = S^i_l \oslash S^i_r$, for some S^i_l, S^i_r. Using Equations (11) and (12) we obtain

$$\begin{aligned}
\gamma = (Z^0)^{-1} \otimes Z^1 &= (K^{-1} \otimes S^0_l \otimes (S^0_r)^{-1})^{-1} \otimes (K^{-1} \otimes S^1_l \otimes (S^1_r)^{-1}) \\
&= S^0_r \otimes (S^0_l)^{-1} \otimes K \otimes K^{-1} \otimes S^1_l \otimes (S^1_r)^{-1} \\
&= S^0_r \otimes (S^0_l)^{-1} \otimes S^1_l \otimes (S^1_r)^{-1} \\
&= (T^0)^{-1} \otimes T^1
\end{aligned} \tag{13}$$

and

$$F(K \otimes Z^i) = F(K \otimes K^{-1} \otimes S^i_l \otimes (S^i_r)^{-1}) = F(S^i_l \otimes (S^i_r)^{-1}) = F(T^i). \tag{14}$$

From Equation (14) we derive

$$Y^i_r = X^i_r \otimes F(K \otimes Z^i) = S^i_r \otimes F(T^i) \tag{15}$$

[9] Although for $LLM_{\otimes,\oslash}$ and $RLM_{\oslash,\otimes}$ this is not necessary, we leave it for uniformity.

and

$$\begin{aligned} Y_l^i &= \varphi(X_l^i \otimes F(K \otimes Z^i)) \\ &= \varphi(K^{-1} \otimes S_l^i \otimes F(T^i)) \\ &= \varphi(K)^{-1} \otimes \varphi(S_l^i \otimes F(T^i)). \end{aligned} \tag{16}$$

Hence, we have

$$Y_l^0 \oslash Y_l^1 = (\varphi(S_l^0 \otimes F(T^0)))^{-1} \otimes \varphi(S_l^1 \otimes F(T^1)) \tag{17}$$

$$Y_r^0 \oslash Y_r^1 = (S_r^0 \otimes F(T^0))^{-1} \otimes (S_r^1 \otimes F(T^1)). \tag{18}$$

Using Equations (11), (13), (17) and (18) we obtain the desired equality. The remaining relations are proven similarly. ☐

Lemma 15. *Let $\beta' = \varphi^{-1}(\beta_l)\|\beta_r$. If φ is a morphism then the following properties hold*

1. *Let $T^i = S_l^i \oslash S_r^i$, $V_l^i = S_l^i \otimes F(T^i)$ and $V_r^i = S_r^i \otimes F(T^i)$. Then*

$$LLM_{\oslash,\bullet}(F, \alpha, \beta, \gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0, S^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(S^0, S^1) = \alpha \\ \Delta_\bullet(T^0, T^1) = \gamma}} [\Delta_{\oslash,\oslash}(V^0, V^1) = \beta'];$$

2. *Let $T^i = S_r^i \oslash S_l^i$, $V_l^i = F(T^i) \otimes S_l^i$ and $V_r^i = F(T^i) \otimes S_r^i$. Then*

$$RLM_{\oslash,\bullet}(F, \alpha, \beta, \gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0, S^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(S^0, S^1) = \alpha \\ \Delta_\bullet(T^0, T^1) = \gamma}} [\Delta_{\oslash,\oslash}(V^0, V^1) = \beta'].$$

Proof. Since φ is a morphism then

$$\begin{aligned} \beta_l = (Y_l^0)^{-1} \otimes Y_l^1 &= \varphi(S_l^0 \otimes F(T^0))^{-1} \otimes \varphi(S_l^1 \otimes F(T^1)) \\ &= \varphi((S_l^0 \otimes F(T^0))^{-1}) \otimes \varphi(S_l^1 \otimes F(T^1)) \\ &= \varphi((S_l^0 \otimes F(T^0))^{-1} \otimes (S_l^1 \otimes F(T^1)) \\ &= \varphi(V_l^0 \oslash V_l^1). \end{aligned}$$

This is equivalent with $V_l^0 \oslash V_l^1 = \varphi^{-1}(\beta_l)$. The second equality is proven similarly. ☐

Lemma 15 tell us that when φ is a morphism it does not influence the symmetric Lay-Massey differential probabilities. Thus, the differential study of one round reduces to studying, for example, $F(Z^0)^{-1} \otimes \alpha_j \otimes F(Z^1)$, where $j \in \{l, r\}$.

Corollary 3. *Let $G(x) = F(x)^{-1}$. If φ is a morphism then*

$$LLM_{\oslash,\bullet}(F, \alpha, \beta, \gamma) = RLM_{\oslash,\bullet}(G, \alpha, \beta, \gamma).$$

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

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

and

$$\begin{aligned}T_j^0 \oslash T_j^1 &= F(Z^0)^{-1} \otimes (X_j^0)^{-1} \otimes X_j^1 \otimes F(Z^1) \\ &= G(Z^0) \otimes S_j^0 \otimes (S_j^1)^{-1} \otimes G(Z^1)^{-1} \\ &= \Delta_{\oslash}(G(Z^0) \otimes S_j^0, G(Z^1) \otimes S_j^1).\end{aligned}$$

Thus, we obtain the desired equality. □

In this last part, we consider $(\mathbb{G}, \otimes)$ to be a commutative group and see what properties hold for the symmetric Lai-Massey structures.

Lemma 16. *The following properties hold*

$$\begin{aligned}\Delta_{\oslash}(X_l^0 \oslash X_r^0, X_l^1 \oslash X_r^1) &= X_r^0 \otimes \Delta_{\oslash}(X_l^0, X_l^1) \otimes (X_r^1)^{-1}, \\ \Delta_{\oslash}(X_l^0 \oslash X_r^0, X_l^1 \oslash X_r^1) &= X_l^0 \otimes \Delta_{\oslash}(X_r^0, X_r^1) \otimes (X_l^1)^{-1}, \\ \Delta_{\oslash}(X_r^0 \oslash X_l^0, X_r^1 \oslash X_l^1) &= (X_l^0)^{-1} \otimes \Delta_{\oslash}(X_r^0, X_r^1) \otimes X_l^1, \\ \Delta_{\oslash}(X_r^0 \oslash X_l^0, X_r^1 \oslash X_l^1) &= (X_r^0)^{-1} \otimes \Delta_{\oslash}(X_l^0, X_l^1) \otimes X_r^1.\end{aligned}$$

Proof. By rewriting the left hand side of the equality we obtain

$$\begin{aligned}\Delta_{\oslash}(X_l^0 \oslash X_r^0, X_l^1 \oslash X_r^1) &= (X_l^0 \otimes (X_r^0)^{-1})^{-1} \otimes (X_l^1 \otimes (X_r^1)^{-1}) \\ &= X_r^0 \otimes ((X_l^0)^{-1} \otimes X_l^1) \otimes (X_r^1)^{-1} \\ &= X_r^0 \otimes \Delta_{\oslash}(X_l^0, X_l^1) \otimes (X_r^1)^{-1}.\end{aligned}$$

The remaining equalities are proven similarly. □

Corollary 4. *If* $(\mathbb{G}, \otimes)$ *is a commutative group then*

$$\begin{aligned}\Delta_{\oslash}(X_l^0 \oslash X_r^0, X_l^1 \oslash X_r^1) &= \Delta_{\oslash}(X_l^0, X_l^1) \otimes (\Delta_{\oslash}(X_r^0, X_r^1))^{-1}, \\ \Delta_{\oslash}(X_l^0 \oslash X_r^0, X_l^1 \oslash X_r^1) &= (\Delta_{\oslash}(X_l^0, X_l^1))^{-1} \otimes \Delta_{\oslash}(X_r^0, X_r^1), \\ \Delta_{\oslash}(X_r^0 \oslash X_l^0, X_r^1 \oslash X_l^1) &= (\Delta_{\oslash}(X_l^0, X_l^1))^{-1} \otimes \Delta_{\oslash}(X_r^0, X_r^1), \\ \Delta_{\oslash}(X_r^0 \oslash X_l^0, X_r^1 \oslash X_l^1) &= \Delta_{\oslash}(X_l^0, X_l^1) \otimes (\Delta_{\oslash}(X_r^0, X_r^1))^{-1}.\end{aligned}$$

Corollary 5 tells us that when φ is a morphism and $(\mathbb{G}, \otimes)$ is a commutative group, the problem of studying the differential security of the symmetric Lay-Massey structure is reduced to studying the security of F. Hence, our definitions are well defined.

Corollary 5. *If $(\mathbb{G}, \otimes)$ is a commutative and φ is a morphism then the following properties hold*

$$\begin{aligned} LLM_{\obslash,\bullet}(F, \alpha, \beta, \gamma) &= DP_{\otimes}(F, A^l_\bullet, B^l_\bullet), \\ RLM_{\obslash,\bullet}(F, \alpha, \beta, \gamma) &= DP_{\otimes}(F, A^r_\bullet, B^r_\bullet), \end{aligned}$$

for some As and Bs.

Proof. According to Corollary 4 $LLM_{\obslash,\obslash}$ is 0, unless $\gamma = \alpha_l \otimes \alpha_r^{-1}$. Thus, the differential probability makes sense only when $\gamma = \alpha_l^{-1} \otimes \alpha_r = A$.

Using the notations from Lemma 15, we have

$$\begin{aligned} \beta'_l = (V_l^0)^{-1} \otimes V_l^1 &= F(T^0)^{-1} \otimes (S_l^0)^{-1} \otimes S_l^1 \otimes F(T^1) \\ &= F(T^0)^{-1} \otimes \alpha_l \otimes F(T^1) \\ &= \alpha_l \otimes \Delta_{\obslash}(F(T^0), F(T^1)). \end{aligned}$$

This is equivalent with $\Delta_{\obslash}(F(T^0), F(T^1)) = \alpha_l^{-1} \otimes \beta'_l$. Similarly we obtain $\Delta_{\obslash}(F(T^0), F(T^1)) = \alpha_r^{-1} \otimes \beta'_r$. Thus, $LLM_{\obslash,\obslash}$ makes sense only when $\alpha_l^{-1} \otimes \beta'_l = \alpha_r^{-1} \otimes \beta'_r = B$. Hence, we obtain

$$\begin{aligned} LLM_{\obslash,\obslash}(F, \alpha, \beta, \gamma) &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0, S^1 \in \mathbb{G}^2 \\ \Delta_{\obslash,\obslash}(S^0, S^1) = \alpha \\ \Delta_{\obslash}(T^0, T^1) = \alpha_l \otimes \alpha_r^{-1}}} [\Delta_{\obslash}(F(T^0), F(T^1)) = B] \\ &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{T^0, T^1 \in \mathbb{G} \\ \Delta_{\obslash}(T^0, T^1) = A}} \sum_{S_r^0 \in \mathbb{G}} [\Delta_{\obslash}(F(T^0), F(T^1)) = B] \\ &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{T^0, T^1 \in \mathbb{G} \\ \Delta_{\obslash}(T^0, T^1) = A}} |\mathbb{G}| [\Delta_{\obslash}(F(T^0), F(T^1)) = B] \\ &= DP_{\otimes}(F, A, B). \end{aligned}$$

The remaining probabilities are reduced to DP using similar techniques. □

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

Proposition 2. *If φ is a morphism, then the left and right symmetric versions are equivalent from a differential point of view. Moreover, if $(\mathbb{G}, \otimes)$ is commutative we recover that LLM and RLM are equal to DP.*

4.3 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 $\otimes$ is equivalent[10] with $\otimes$ and then we study the impact of the morphism φ-property and the commutativity $\otimes$-property on the asymmetric structure.

[10] from a differential point of view

Definition 9. *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 $Z^i = X_l^i \otimes X_r^i$, $Y_l^i = \varphi(X_l^i \otimes F(K \otimes Z^i))$ and $Y_r^i = F(K \otimes Z^i) \otimes X_r^i$. Then*

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

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

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

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

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

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

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

where $F\colon \mathbb{G} \to \mathbb{G}$ is a function, $\varphi\colon \mathbb{G} \to \mathbb{G}$ is a δ-almost orthomorphism, $\alpha, \beta \in \mathbb{G}^2$ and $\gamma \in \mathbb{G}$.

The next lemma allows us to remove the key from the differential probabilities. Note that the Lemma 17 is proven similarly to Lemma 14 and hence we omit its proof.

Lemma 17. *Let $\bullet \in \{\obslash, \oslash\}$. If φ is a morphism*[11]*, then we can rewrite the asymmetric Lai-Massey differential probabilities as follows*

1. *Let $T^i = S_l^i \otimes S_r^i$, $Y_l^i = \varphi(S_l^i \otimes F(T^i))$ and $Y_r^i = F(T^i) \otimes S_r^i$. Then*

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

[11] Although for $OLM_{\obslash,\oslash}$ and $ILM_{\oslash,\oslash}$ this is not necessary, we leave it for uniformity.

2. *Let* $T^i = S^i_r \otimes S^i_l$, $Y^i_l = \varphi(F(T^i) \otimes S^i_l)$ *and* $Y^i_r = S^i_r \otimes F(T^i)$. *Then*

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

As in the symmetric case, if φ is a morphism the differential study is reduced to studying, for example, $F(Z^0)^{-1} \otimes \alpha_r \otimes F(Z^1)$ and $F(Z^0) \otimes \alpha_l \otimes F(Z^1)^{-1}$. This is stated formally in the next lemma.

Lemma 18. *Let* $\beta' = \varphi^{-1}(\beta_l) \| \beta_r$. *If* φ *is a morphism then the following properties hold*

1. *Let* $T^i = S^i_l \otimes S^i_r$, $V^i_l = S^i_l \otimes F(T^i)$ *and* $V^i_r = F(T^i) \otimes S^i_r$. *Then*

$$OLM_{\otimes,\bullet}(F,\alpha,\beta,\gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0,S^1 \in \mathbb{G}^2 \\ \Delta_{\otimes,\oslash}(S^0,S^1)=\alpha \\ \Delta_\bullet(T^0,T^1)=\gamma}} [\Delta_{\otimes,\oslash}(V^0,V^1) = \beta'];$$

2. *Let* $T^i = S^i_r \otimes S^i_l$, $V^i_l = F(T^i) \otimes S^i_l$ *and* $V^i_r = S^i_r \otimes F(T^i)$. *Then*

$$ILM_{\oslash,\bullet}(F,\alpha,\beta,\gamma) = \frac{1}{|\mathbb{G}|^2} \sum_{\substack{S^0,S^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\otimes}(S^0,S^1)=\alpha \\ \Delta_\bullet(T^0,T^1)=\gamma}} [\Delta_{\oslash,\otimes}(V^0,V^1) = \beta'].$$

Corollary 6. *Let* $G(x) = F(x)^{-1}$. *If* φ *is a morphism then*

$$OLM_{\otimes,\bullet}(F,\alpha,\beta,\gamma) = ILM_{\oslash,\bullet}(G,\alpha,\beta,\gamma).$$

When $\otimes$ is commutative we obtain that all the Lai-Massey structures are equivalent. This is stated formally in the following lemma.

Lemma 19. *If* $(\mathbb{G},\otimes)$ *is a commutative group then the following properties hold*

$$OLM_{\otimes,\bullet}(F,\alpha,\beta,\gamma) = LLM_{\otimes,\bullet}(F,\alpha,\beta_l \| (\alpha_r)^2 \otimes \beta_r^{-1},\gamma,K),$$
$$ILM_{\oslash,\bullet}(F,\alpha,\beta,\gamma) = RLM_{\oslash,\bullet}(F,\alpha,\beta_l \| (\alpha_r)^2 \otimes \beta_r^{-1},\gamma,K).$$

Proof. Let $T^i_l = X^i_l$ and $T^i_r = (X^i_r)^{-1}$. Then $Z^i = T^i_l \otimes (T^i_r)^{-1} = T^i_l \oslash T^i_r$ and $X^0_r \oslash X^1_r = (T^0_r)^{-1} \otimes T^1_r = T^0_r \otimes T^1_r$. Since $\otimes$ is commutative we obtain

$$\beta_r = Y^0_r \oslash Y^1_r = F(Z^0) \otimes X^0_r \otimes (X^1_r)^{-1} \otimes F(Z^1)^{-1} = \alpha_r \otimes F(Z^0) \otimes F(Z^1)^{-1}.$$

This is equivalent with

$$\begin{aligned}(\alpha_r)^2 \otimes \beta_r^{-1} &= \alpha_r \otimes F(Z^0)^{-1} \otimes F(Z^1) \\ &= F(Z^0)^{-1} \otimes (T^0_r)^{-1} \otimes T^1_r \otimes F(Z^1) \\ &= \Delta_\otimes(T^0_r \otimes F(Z^0), T^1_r \otimes F(Z^1)).\end{aligned}$$

Let $S_l^i = Y_l^i$ and $S_r^i = T_r^i \otimes F(Z^i)$. Hence, we obtain

$$\begin{aligned} OLM_{\oslash,\bullet}(F,\alpha,\beta,\gamma) &= \frac{1}{\mathbb{G}} \sum_{\substack{T^0,T^1 \in \mathbb{G}^2 \\ \Delta_{\oslash,\oslash}(T^0,T^1)=\alpha \\ \Delta_{\bullet}(Z^0,Z^1)=\gamma}} [\Delta_{\oslash,\oslash}(S^0,S^1) = \beta_l \| (\alpha_r)^2 \otimes \beta_r^{-1}] \\ &= LLM_{\oslash,\bullet}(F,\alpha,\beta_l\|(\alpha_r)^2 \otimes \beta_r^{-1},\gamma). \end{aligned}$$

The second equality is proven in a similar fashion. □

By using some results obtained in the symmetric case, Corollary 7 shows the correctness of our definitions.

Corollary 7. *If* $(\mathbb{G},\otimes)$ *is a commutative and* φ *is a morphism then the following properties hold*

$$\begin{aligned} OLM_{\oslash,\bullet}(F,\alpha,\beta,\gamma) &= DP_{\otimes}(F,A_{\bullet}^l,B_{\bullet}^l), \\ ILM_{\oslash,\bullet}(F,\alpha,\beta,\gamma) &= DP_{\otimes}(F,A_{\bullet}^r,B_{\bullet}^r), \end{aligned}$$

for some As *and* Bs.

Proof. Using Lemma 19 we reduce the notions of OLM and ILM to LLM and RLM. Then, using Corollary 5 we collapse the notions to DP. Hence, we obtain the corollary. □

We further summarise the results obtained for the asymmetric Lai-Massey structures in Proposition 3.

Proposition 3. *When* φ *is a morphism, then the inner and outer asymmetric versions are equivalent from a differential point of view. Also, if* $\otimes$ *is commutative, then the symmetric and asymmetric structures are equivalent.*

5 Conclusions

In this paper we studied the effect of quasigroups isotopic to groups in the design of cryptographic symmetric structures. We first show that for SPNs based on non-commutative groups, the left and right versions are equivalent (Lemma 4). Then, we study Feistel structures and we prove that the problem of studying a Feistel structure based on an isotopic quasigroup reduces to studying an unkeyed version of the general Feistel iteration based on the initial group (Lemmas 6 to 10). As in the SPN case, left and right Feistel structures are equivalent (Corollary 2). For the Lai-Massey structure we argue that the operation should be a group operation (Lemma 12 and Remark 4). When the δ-almost orthomorphism is a morphism then the left and right Lai-Massey versions are equivalent (Corollary 3). The same statement is true for the inner and outer Lai-Massey versions (Corollary 6).

When we consider SPN and Feistel symmetric structures with random secret s-boxes (*e.g.* [3, 33]) using an isotopic quasigroup or a non-commutative group does not pose a problem, since studying its security reduces to studying the security of a symmetric structure with a different s-box than the original one. Thus, in this case, the extensions are secure, but, nevertheless, useless. When we consider static s-boxes we encounter a security problem. Since the resulting new s-box might not have the cryptographic properties of the initial s-box, using a quasigroup/non-commutative group operation might lead to cryptographic weaknesses unforeseen by the designers of the static s-box.

Future work. We showed the stability of the UGF, but not of the KGF. Hence, we leave this as an open problem. An interesting problem is to (dis)prove that the left and inner versions of the Lai-Massey structure are equivalent when φ is a morphism. Another open problem is to find a sufficient condition for the differential equivalency of the four Lai-Massey structures.

References

1. 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)
2. 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)
3. Borghoff, J., Knudsen, L.R., Leander, G., Thomsen, S.S.: Cryptanalysis of PRESENT-Like Ciphers with Secret S-Boxes. In: FSE 2011. Lecture Notes in Computer Science, vol. 6733, pp. 270–289. Springer (2011)
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 (2020)
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 (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.: A New Authentication Scheme Based on Latin Squares. Discret. Math. **106**, 157–161 (1992)
12. Dobbertin, H.: One-to-One Highly Nonlinear Power Functions on $\mathrm{GF}(2^n)$. Appl. Algebra Eng. Commun. Comput. **9**(2), 139–152 (1998)

13. Evans, A.B.: The Admissibility of Sporadic Simple Groups. Journal of Algebra **321**(1), 105–116 (2009)
14. 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)
15. Gligoroski, D., Markovski, S., Kocarev, L.: Edon-R, An Infinite Family of Cryptographic Hash Functions. I.J. Network Security **8**(3), 293–300 (2009)
16. Hall, M., Paige, L.J.: Complete Mappings of Finite Groups. Pacific Journal of Mathematics **5**(4), 541–549 (1955)
17. 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)
18. Howitt, S.M., Wilson, A.N.: Revisiting "Is the Scientific Paper a Fraud?". EMBO Reports **15**(5), 481–484 (2014)
19. Kościelny, C.: A Method of Constructing Quasigroup-Based Stream-Ciphers. Applied Mathematics and Computer Science **6**, 109–122 (1996)
20. 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)
21. 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)
22. Medawar, P.: Is the Scientific Paper a Fraud? The Listener **70**(12), 377–378 (1963)
23. Mouha, N.: On Proving Security against Differential Cryptanalysis. In: CFAIL 2019 (2019)
24. Nyberg, K.: Perfect Nonlinear S-boxes. In: EUROCRYPT 1991. Lecture Notes in Computer Science, vol. 547, pp. 378–386. Springer (1991)
25. O'Connor, L.: On the Distribution of Characteristics in Bijective Mappings. Journal of Cryptology **8**(2), 67–86 (1995)
26. 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)
27. Schneier, B.: Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). In: FSE 1993. Lecture Notes in Computer Science, vol. 809, pp. 191–204. Springer (1994)
28. Schwartz, M.A.: The Importance of Stupidity in Scientific Research. Journal of Cell Science **121**(11), 1771–1771 (2008)
29. Smith, J.D.: Four Lectures on Quasigroup Representations. Quasigroups Related Systems **15**, 109–140 (2007)
30. Tao, T.: Ask Yourself Dumb Questions - and Answer Them! https://terrytao.wordpress.com/career-advice/ask-yourself-dumb-questions-and-answer-them/
31. Tao, T.: Use The Wastebasket. https://terrytao.wordpress.com/career-advice/use-the-wastebasket/
32. Teşeleanu, G.: Quasigroups and Substitution Permutation Networks: A Failed Experiment. Cryptologia **45**(3), 266–281 (2021)
33. Tiessen, T., Knudsen, L.R., Kölbl, S., Lauridsen, M.M.: Security of the AES with a Secret S-Box. In: FSE 2015. Lecture Notes in Computer Science, vol. 9054, pp. 175–189. Springer (2015)
34. Truran, P.: Practical Applications of the Philosophy of Science: Thinking About Research. Springer Science & Business Media (2013)

35. Vaudenay, S.: On the Lai-Massey Scheme. In: ASIACRYPT 1999. Lecture Notes in Computer Science, vol. 1716, pp. 8–19. Springer (1999)
36. Vaudenay, S.: A Classical Introduction to Cryptography: Applications for Communications Security. Springer Science & Business Media (2005)
37. Vojvoda, M., Sỳs, M., Jókay, M.: A Note on Algebraic Properties of Quasigroups in Edon80. Tech. rep., eSTREAM report 2007/005 (2007)
38. Weidman, D.R.: Emotional Perils of Mathematics. Science **149**(3688), 1048–1048 (1965)
39. Wilcox, S.: Reduction of the Hall-Paige Conjecture to Sporadic Simple Groups. Journal of Algebra **321**(5), 1407–1428 (2009)