The Security of Quasigroups Based Substitution Permutation Networks

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. The study of symmetric structures based on quasigroups is relatively new and certain gaps can be found in the literature. In this paper, we want to fill one of these gaps. More precisely, in this work we study substitution permutation networks based on quasigroups that make use of permutation layers that are non-linear relative to the quasigroup operation. We prove that for quasigroups isotopic with a group $\mathbb{G}$, the complexity of mounting a differential attack against this type of substitution permutation network is the same as attacking another symmetric structure based on $\mathbb{G}$. The resulting structure is interesting and new, and we hope that it will form the basis for future secure block ciphers.

1 Introduction

When designing a block cipher, one of the main challenges is to construct a set of permutations that are easy to implement and at the same time behave as random permutations. Keeping this in mind, three main approaches can be found in the literature [22]. Substitution-permutation networks (SPNs) construct a large block random looking permutation using a series of substitution[3] and permutation layers iterated over several rounds. A different approach is used to construct Feistel and Lai-Massey symmetric structures. Instead of using invertible building blocks, these two structures construct permutations using non-invertible components.

One of the most powerful tools used to attack block ciphers is differential cryptanalysis [14]. Introduced by Biham and Shamir [2], this type of attack exploits the way certain plaintext changes propagate to the ciphertext. If we used truly random permutations, we could predict these changes with a probability of $1/2^n$, where n is the number of input bits. Therefore, if n was for example 128 bits the probability would be negligible. Nevertheless, as stated before we should be able to easily describe the permutation and this is not the case for ideal permutations. Hence, in order to build practical block ciphers, designers

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

need to use theoretical estimates based on certain assumptions that are not always valid in practice. In consequence, block ciphers are not ideal and this makes them susceptible to differential cryptanalysis. Because of that, security against differential cryptanalysis is one of the basic design criteria for symmetric primitives [18].

Latin squares are $\ell \times \ell$ matrices which contain only ℓ symbols and have the property that each symbol appears only once in each row and only once in each column [10]. A set endowed with a multiplication table that is a Latin square forms a quasigroup. These structures can be thought of as a group that is not associative and does not have an identity element. Although quasigroups are not a popular choice when constructing cryptographic primitives, various designs based can still be found in the literature [1, 6, 7, 11–13, 15, 16].

A very recent approach [3–5, 8] 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. Specifically, such a symmetrical structure has a level of security, in relation to differential attacks, which is dependent on the intended operation. This methodology is similar to the one used in this paper, because we also consider different operations to construct differential attacks against the proposed SPNs. Nevertheless, the scope of [3–5, 8] is to show how a designer can embed a trapdoor into a symmetric structure[4], while ours is to investigate whether changing the group operation to a quasigroup one could strengthen an SPN structure against differential cryptanalysis.

In [20, 21] the author introduces a straightforward generalization of the three main symmetric structures: SPNs, Feistel and Lai-Massey. Namely, instead of using a group operation between keys and (intermediary) plaintexts, the generalisations use a quasigroup one. When studying their security the author restricts the study to quasigroup operations that are isotopic with a group operation, since this is the most popular method for constructing quasigroups. We further discuss only the results concerning SPNs, since this is the topic of our paper. The result of the two studies is that in the case of isotopies the resulting symmetric structures are equivalent[5] with another structure that uses a group operation. Although the result is the same, the views considered in the two papers are different. In [21], the author implicitly considers that the permutation layer is linear with respect to the quasigroup operation. Therefore, differential probabilities are induced only by the s-boxes, since the permutation layer and the key mixing operation make differentials predictable with no uncertainty. Hence, we can reduce the analysis of the differential probabilities induced by the round function to those induced by the s-boxes. In the second paper [20], the view is changed from an element wise one to a global one. More precisely, in the first paper the key mixing operation between the key $k = k_1 \| \dots \| k_n$ and the plaintext $p = p_1 \| \dots \| p_n$ is $k_1 \otimes p_1 \| \dots \| k_n \otimes p_n$, while in the subsequent work is simply $k \otimes p$, where $\otimes$ is the quasigroup operation. Keep in mind that the

[4] The trapdoor consists in knowing the group operation that weakens the structure.
[5] from the point of view of differential attacks

results from [21] still apply since the whole round transformation can be seen as a permutation.

In this paper we study the remaining case, namely SPN structures with a permutation layer that is non-linear with respect to the quasigroup operation. When this assumption holds, the results from [20,21] do not apply. Therefore, a new analysis is required. The results obtained using the techniques introduced in this paper are twofold. First of all we confirm the results[6] presented in [20,21] by using a different approach than the original one. Secondly, we show that when the permutation layer is non-linear relative to the quasigroup operation, then we cannot reduce its security to a group based SPN structure. More precisely, we obtain that the quasigroup based SPN is equivalent to a structure that has an extra substitution layer before the key mixing operation takes place and which uses a group based key mixing step. To the authors' knowledge, this design was never described in the literature. Therefore, we believe that this novel structure is worth attention for future research from both a theoretical and a design point of view.

Structure of the paper. We introduce notations and definitions in Section 2. SPNs with generic permutation layers are studied in Section 3. 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. 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 values. We also define the identity permutation $Id = \{0, \ldots, \ell\}$.

2.1 Quasigroups

In this section we introduce a few basic notions about quasigroups. We base our exposition on [19].

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*

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

[6] restricted to quasigroups isotopic to commutative groups

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

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 [12, 13, 15, 23] 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 $\pi, \rho, \omega : \mathbb{G} \to \mathbb{G}$. 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 $\omega(z)$.

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. [21]

$\otimes$	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 $\rho(i) = n - i \bmod n$. [23]

2.2 Quasigroup Differential Cryptanalysis

The notion of differential cryptanalysis was first introduced in [2] for analyzing the Data Encryption Standard block cipher. Since the key mixing layer was simply bitwise addition modulo 2 between the key and the (intermediary) plaintext, differential attacks where defined only for $(\mathbb{Z}_{2^n}, \oplus)$. Later on, the concept was extended to commutative groups [17], non-commutative groups [21] and quasigroups [20, 21]. We further present the notions of quasigroup differential probabilities for a permutation. Note that when the quasigroup is replaced with a (non-)commutative group the notions are in accordance with [17, 21]. Also, in the case of groups the KDP notions coincide with the corresponding DP probability (*i.e.* are key independent).

Definition 4. *Let* $\mathbb{G}$ *be a set equipped with a binary operation* $\bullet : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$. *The difference between two elements* $X, X' \in (\mathbb{G}, \bullet)$ *is defined as* $\Delta_\bullet(X, X') = X \bullet X'$.

Definition 5. *Let K be a key, $(\mathbb{G}, \otimes)$ a quasigroup and $\bullet \in \{\oslash, \oslash\}$. We define the quasigroup differential probabilities*

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

$$KDP_{\oslash}(\sigma, \alpha, \beta, K) = \frac{1}{|\mathbb{G}|} \sum_{\substack{X, X' \in \mathbb{G} \\ \Delta_{\oslash}(X, X') = \alpha}} [\Delta_{\oslash}(\sigma(K \otimes X), \sigma(K \otimes X')) = \beta],$$

$$KDP_{\oslash}(\sigma, \alpha, \beta, K) = \frac{1}{|\mathbb{G}|} \sum_{\substack{X, X' \in \mathbb{G} \\ \Delta_{\oslash}(X, X') = \alpha}} [\Delta_{\oslash}(\sigma(X \otimes K), \sigma(X' \otimes K)) = \beta],$$

where $\sigma : \mathbb{G} \to \mathbb{G}$ is a permutation and $\alpha, \beta \in \mathbb{G}$.

2.3 Quasigroup Substitution Permutation Network

Let n be a positive integer and $(\mathbb{G}, \otimes)$ a quasigroup. An SPN is an iterated structure that processes a plaintext for r rounds. Each round consist of a key mixing operation, a substitution layer and a permutation layer. Also, the SPN has a final round that consists only of a key mixing operation. Note that for each round i the key schedule algorithm derives the subkey k_i from the initial key. We refer the reader to Figure 1 for some SPN examples that have three rounds.[7]

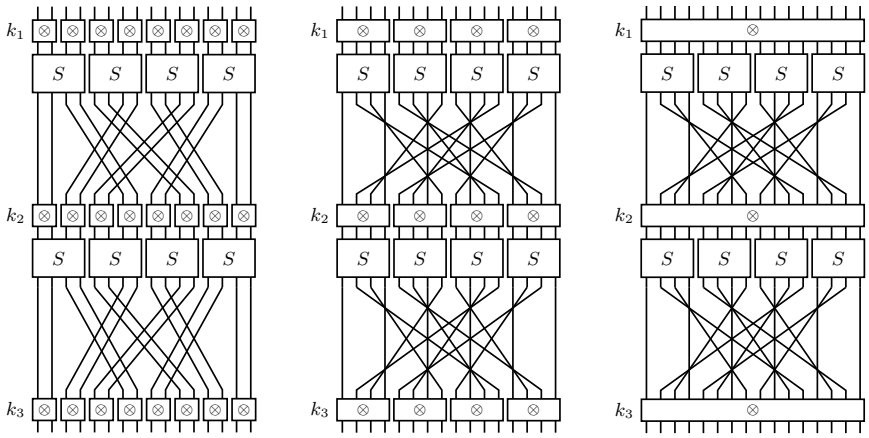
To exemplify the different types of possible generalisations of the SPN structure we will use Figure 1 as a reference. Let $p_i = \tilde{p}_i^1 \| \dots \| \tilde{p}_i^8 = \hat{p}_i^1 \| \dots \| \hat{p}_i^4$ and $k_i = \tilde{k}_i^1 \| \dots \| \tilde{k}_i^8 = \hat{k}_i^1 \| \dots \| \hat{k}_i^8$ be the intermediary plaintext and the subkey for round $i \in \{1, 2, 3\}$.

In Figure 1a we have an example of an element wise key mixing layer $\tilde{p}_i^1 \otimes \tilde{k}_i^1 \| \dots \| \tilde{p}_i^8 \otimes \tilde{k}_i^8$ (right quasigroup operation[8]) and a permutation layer that is linear with respect to $\otimes$. Therefore, is sufficient to study the differential properties of the s-box with respect to $x \bar{\otimes} y = x_1 \otimes y_1 \| x_2 \otimes y_2$, where $x = x_1 \| x_2$ and $y = y_1 \| y_2$. This variant was studied in [21].

In Figure 1b we have an example of an element wise key mixing layer $\hat{p}_i^1 \otimes \hat{k}_i^1 \| \dots \| \hat{p}_i^4 \otimes \hat{k}_i^4$ (right quasigroup operation) and a permutation layer that is non-linear with respect to $\otimes$. This is the version that we further study in our paper.

The last version is presented in Figure 1c and represents an example of a global key mixing layer $p_i \otimes k_i$ (right quasigroup operation). Here the permutation layer is inherently non-linear with respect to $\otimes$. This type of SPN was studied in [20].

[7] Figure 1 is based on the TikZ found in [9].
[8] left quasigroup operation: $\tilde{k}_i^1 \otimes \tilde{p}_i^1 \| \dots \| \tilde{k}_i^8 \otimes \tilde{p}_i^8$



(a) Linear permutation (b) Non-linear permutation (c) Global operation

Fig. 1: Variations of the SPN structure

3 Security Analysis

We further assume that the permutation layer P is non-linear with respect to $\otimes$. Since P shuffles b-bit blocks of data we further assume, without loss of generality, that it is linear with respect to addition modulo 2^b, further denoted by $\odot$. In the worse case, the permutation shuffles bits, and thus is linear with respect to $\oplus$. Note that since P shuffles blocks composed of bits that means that the quasigroup operation $\otimes$ must be isotopic to addition modulo some $2^{b'}$, for some $b' > b$.[9] We also assume, without loss of generality, that b' is a multiple of b.[10] In the worse case, we take $b = 1$ and this condition is fulfilled. To simplify our exposition we use the multiplicative notation for the inverse of an element modulo 2^b.

Since the permutation layer is $\odot$-linear, we have to study the following differential properties

$$LKDP_{\odot,\otimes}(\sigma,\alpha,\beta,K) = \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X'\in\mathbb{G} \\ X\odot X'^{-1}=\alpha}} [\sigma(K\otimes X)\odot\sigma(K\otimes X')^{-1}=\beta],$$

$$RKDP_{\odot,\otimes}(\sigma,\alpha,\beta,K) = \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X'\in\mathbb{G} \\ X\odot X'^{-1}=\alpha}} [\sigma(X\otimes K)\odot\sigma(X'\otimes K)^{-1}=\beta],$$

where $\sigma : \mathbb{G} \to \mathbb{G}$ is a permutation and $\alpha, \beta \in \mathbb{G}$.

[9] This condition is implied by the fact that the permutation is not linear.

[10] This condition implies that the sets $G = \mathbb{Z}_{2^{b'}}$ and $(\mathbb{Z}_{2^b})^{b'/b}$ are isomorphic.

Lemma 3. *Let $\sigma' = \sigma \circ \omega^{-1}$. We define $x * y = \pi(x) \star \rho(y)$. Then the following identities hold*

$$LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = LKDP_{\odot,*}(\sigma', \alpha, \beta, K),$$
$$RKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = RKDP_{\odot,*}(\sigma', \alpha, \beta, K).$$

Proof. First we rewrite

$$\begin{aligned}\beta &= \sigma(K \otimes X) \odot \sigma(K \otimes X')^{-1} \\ &= \sigma(\omega^{-1}(\pi(K) \star \rho(X))) \odot \sigma(\omega^{-1}(\pi(K) \star \rho(X')))^{-1} \\ &= \sigma'(\pi(K) \star \rho(X)) \odot \sigma'(\pi(K) \star \rho(X'))^{-1} \\ &= \sigma'(K * X) \odot \sigma'(K * X')^{-1}.\end{aligned}$$

Then we obtain

$$\begin{aligned}LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) &= \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} [\sigma(K \otimes X) \odot \sigma(K \otimes X')^{-1} = \beta] \\ &= \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} [\sigma'(K * X) \odot \sigma'(K * X')^{-1} = \beta] \\ &= LKDP_{\odot,*}(\sigma', \alpha, \beta, K).\end{aligned}$$

Similarly, we obtain $RKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = RKDP_{\odot,*}(\sigma', \alpha, \beta, K)$. □

Lemma 3 tells us that it is irrelevant from a differential point of view if we define the quasigroup operation with $\omega \neq Id$ or $\omega = Id$. Thus, we further restrict our study to the quasigroup operation $x \otimes y = \pi(x) \star \rho(y)$.

A closer analysis of $LKDP$ and $RKDP$ shows some interesting properties. These are presented in the following lemma.

Lemma 4. *The following equalities hold*

$$LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = LKDP_{\odot,\otimes}(Id, \alpha, \gamma, K) \cdot DP_{\odot}(\sigma, \gamma, \beta),$$
$$RKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = RKDP_{\odot,\otimes}(Id, \alpha, \gamma, K) \cdot DP_{\odot}(\sigma, \gamma, \beta).$$

Proof. We only prove the lemma for $LKDP$, since the proof for $RKPD$ is similar. Therefore, we have

$$\begin{aligned}LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) &= \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} [\sigma(K \otimes X) \odot \sigma(K \otimes X')^{-1} = \beta] \\ &= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} \sum_{\substack{Y,Y'^{-1} \in \mathbb{G} \\ Y \odot Y'^{-1} = \gamma}} [(K \otimes X) \odot (K \otimes X')^{-1} = \gamma]\end{aligned}$$

$$
\begin{aligned}
&\cdot [\sigma(Y) \odot \sigma(Y')^{-1} = \beta] \\
&= \left\{ \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} [(K \otimes X) \odot (K \otimes X')^{-1} = \gamma] \right\} \\
&\cdot \left\{ \frac{1}{|\mathbb{G}|} \sum_{\substack{Y,Y' \in \mathbb{G} \\ Y \odot Y'^{-1} = \gamma}} [\sigma(Y) \odot \sigma(Y')^{-1} = \beta] \right\} \\
&= LKDP_{\odot,\otimes}(Id, \alpha, \gamma, K) \cdot DP_{\odot}(\sigma, \gamma, \beta),
\end{aligned}
$$

as desired. □

Looking more closely at Lemma 4 we can observe that $DP_{\odot}(\sigma, \gamma, \beta)$ is independent of $\otimes$. Hence, the only components that need to be studied further are $LKDP_{\odot,\otimes}(Id, \alpha, \gamma, K)$ and $RKDP_{\odot,\otimes}(Id, \alpha, \gamma, K)$. Using a similar argument as in Lemma 4 we can further breakdown the two differential probabilities.

Lemma 5. *We define $x *_1 y = \pi(x) \star y$ and $x *_2 y = x \star \rho(y)$. Then the following identities hold*

$$
\begin{aligned}
LKDP_{\odot,\otimes}(Id, \alpha, \gamma, K) &= DP_{\odot}(\rho, \alpha, \delta) \cdot LKDP_{\odot,*_1}(Id, \delta, \gamma, K), \\
RKDP_{\odot,\otimes}(Id, \alpha, \gamma, K) &= DP_{\odot}(\rho, \alpha, \delta) \cdot RKDP_{\odot,*_2}(Id, \delta, \gamma, K).
\end{aligned}
$$

Proof. For $LKDP$ the following relations hold

$$
\begin{aligned}
LKDP_{\odot,\otimes}(Id, \alpha, \gamma, K) &= \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} [(K \otimes X) \odot (K \otimes X')^{-1} = \gamma] \\
&= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} \sum_{\substack{Y,Y'^{-1} \in \mathbb{G} \\ Y \odot Y'^{-1} = \delta}} [\rho(X) \odot \rho(X')^{-1} = \delta] \\
&\cdot [(\pi(K) \star Y) \odot (\pi(K) \star Y')^{-1} = \gamma] \\
&= \left\{ \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} [\rho(X) \odot \rho(X')^{-1} = \delta] \right\} \\
&\cdot \left\{ \frac{1}{|\mathbb{G}|} \sum_{\substack{Y,Y' \in \mathbb{G} \\ Y \odot Y'^{-1} = \delta}} [(K *_1 Y) \odot (K *_1 Y')^{-1} = \gamma] \right\} \\
&= DP_{\odot}(\rho, \alpha, \delta) \cdot LKDP_{\odot,*_1}(Id, \delta, \gamma, K).
\end{aligned}
$$

Similarly, we obtain the result for $RKDP$. □

Corollary 1. *The following properties are true*

$$
\begin{aligned}
LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) &= DP_{\odot}(\rho, \alpha, \delta) \cdot LKDP_{\odot,*_1}(Id, \delta, \gamma, K) \cdot DP_{\odot}(\sigma, \gamma, \beta), \\
RKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) &= DP_{\odot}(\rho, \alpha, \delta) \cdot RKDP_{\odot,*_2}(Id, \delta, \gamma, K) \cdot DP_{\odot}(\sigma, \gamma, \beta).
\end{aligned}
$$

The following corollary tell us that if P is linear with respect to $\star$ then $LKDP$ and $RKDP$ are key independent.

Corollary 2. *If $\star = \odot$, then following properties are true*

$$LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = RKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = DP_{\odot}(\rho, \alpha, \delta) \cdot DP_{\odot}(\sigma, \delta, \beta).$$

Proof. Let $X \odot X' = \delta$. Then

$$\begin{aligned}\gamma &= (K *_1 X) \odot (K *_1 X')^{-1} \\ &= \pi(K) \odot X \odot \pi(K)^{-1} \odot X'^{-1} \\ &= X \odot X'^{-1} \\ &= \delta,\end{aligned}$$

and thus $LKDP_{\odot,*_1}(Id, \delta, \gamma, K) = 1$ if and only if $\gamma = \delta$. Similarly, we have $RKDP_{\odot,*_2}(Id, \delta, \gamma, K) = 1$ if and only if $\gamma = \delta$. Therefore, we obtain the desired results. □

According to Corollary 2 the notions of $LKDP$ and $RKDP$ coincide if $\star = \odot$. A consequence of this is the following result from [20]. Note that our proof is different from the one given in the original paper.

Corollary 3. *The left and right quasigroup SPNs derived from a commutative group SPN using an isotopy are equivalent from a differential point of view.*

Corollary 4. *Let $\sigma' = \sigma \circ \rho$. If $\star = \odot$, then following equalities hold*

$$LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = RKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = DP_{\odot}(\sigma, \alpha, \beta).$$

Proof. From Corollary 2 we know that

$$LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = DP_{\odot}(\rho, \alpha, \delta) \cdot DP_{\odot}(\sigma, \delta, \beta).$$

Rewriting the right hand side RHS term of the equality we obtain

$$\begin{aligned}RHS = &\left\{\frac{1}{|\mathbb{G}|} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} [\rho(X) \odot \rho(X')^{-1} = \delta]\right\} \\ &\cdot \left\{\frac{1}{|\mathbb{G}|} \sum_{\substack{Y,Y' \in \mathbb{G} \\ Y \odot Y'^{-1} = \delta}} [\sigma(Y) \odot \sigma(Y')^{-1} = \beta]\right\} \\ = &\frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} \sum_{\substack{\rho(X),\rho(X') \in \mathbb{G} \\ \rho(X) \odot \rho(X')^{-1} = \delta}} [\sigma(\rho(X)) \odot \sigma(\rho(X'))^{-1} = \beta] \\ &\cdot [\rho(X) \odot \rho(X')^{-1} = \delta] \\ = &\frac{1}{|\mathbb{G}|} \sum_{\substack{X,X' \in \mathbb{G} \\ X \odot X'^{-1} = \alpha}} [\sigma'(X) \odot \sigma(X')^{-1} = \beta],\end{aligned}$$

which leads to

$$LKDP_{\odot,\otimes}(\sigma,\alpha,\beta,K) = DP_{\odot}(\sigma',\alpha,\beta),$$

as desired. □

When $\otimes = \odot$, Corollary 4 tells us that is irrelevant from a differential point of view if we replace the group operation with a quasigroup one isotopic to a commutative group operation. Therefore, using different techniques we arrive at the main result from [21].

Corollary 5. *A quasigroup SPN derived from a commutative group SPN using an isotopy has the same differential security as the same group SPN instantiated with a different s-box.*

Remark that in $LKDP_{\odot,*_1}$ and $RKDP_{\odot,*_2}$ we apply a permutation to the key K. Since K and, for example, π are generated as a pair, it suffices from a differential point of view to simply consider $K' = \pi(K)$ 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 block cipher. As a consequence, it suffices to study $LKDP_{\odot,\star}$ and $RKDP_{\odot,\star}$. Therefore, we can rewrite the results presented in Corollary 1 as follows

$$LKDP_{\odot,\otimes}(\sigma,\alpha,\beta,K) = DP_{\odot}(\rho,\alpha,\delta) \cdot LKDP_{\odot,\star}(Id,\delta,\gamma,K') \cdot DP_{\odot}(\sigma,\gamma,\beta),$$
$$RKDP_{\odot,\otimes}(\sigma,\alpha,\beta,K) = DP_{\odot}(\rho,\alpha,\delta) \cdot RKDP_{\odot,\star}(Id,\delta,\gamma,K') \cdot DP_{\odot}(\sigma,\gamma,\beta).$$

Using the results obtained so far the SPN construction shown in Figure 1b is equivalent with the symmetric structure presented in Figure 2. To summarise all the lemmas and observations we provide the reader with Proposition 1.

Proposition 1. *Let $(\mathbb{G},\otimes)$ be a quasigroup isotopic with a group $(\mathbb{G},\star)$. Then, in the case of SPNs that use element wise key mixing based on $\otimes$ and a permutation that is non-linear relative to $\otimes$, the equivalent structure[11] is composed of*

a. $r-1$ rounds consisting of a substitution layer, a key mixing operation based on $\star$, a substitution layer and a permutation layer,
b. a final round consisting only of a substitution layer and a key mixing operation based on $\star$.

The last thing we will prove is that it does not matter if we use the left or right differential probability. As a consequence, the left and right versions of structure presented in Figure 2 are equivalent from a differential point of view.

Lemma 6. *Let $i(x) = x^{-1}$, where the inverse is with respect to $\star$. Then*

$$LKDP_{\odot,\star}(Id,\delta,\gamma,K) = RKDP_{\odot,\star}(i,\delta,\gamma,i(K)),$$
$$RKDP_{\odot,\star}(Id,\delta,\gamma,K) = LKDP_{\odot,\star}(i,\delta,\gamma,i(K)).$$

[11] from a differential point of view

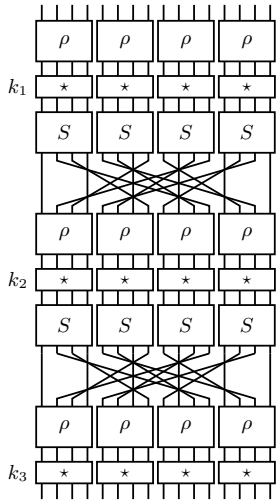


Fig. 2: Equivalent symmetric structure

Proof. Let $Z = i(Y)$, $Z' = i(Y')$ and $K' = i(K)$. Then we have

$$\begin{aligned}
LKDP_{\odot,\star}(Id,\delta,\gamma,K) &= \frac{1}{|\mathbb{G}|} \sum_{\substack{Y,Y'\in\mathbb{G} \\ Y\odot Y'^{-1}=\delta}} [(K\star Y)\odot(K\star Y')^{-1}=\gamma] \\
&= \frac{1}{|\mathbb{G}|} \sum_{\substack{Y,Y'\in\mathbb{G} \\ Y\odot Y'^{-1}=\delta}} [i(i(Y)\star i(K))\odot(i(i(Y')\star i(K)))^{-1}=\gamma] \\
&= \frac{1}{|\mathbb{G}|} \sum_{\substack{Z,Z'\in\mathbb{G} \\ Z\odot Z'^{-1}=\delta}} [i(Z\star K')\odot(i(Z'\star K'))^{-1}=\gamma] \\
&= RKDP_{\odot,\star}(i,\delta,\gamma,K'),
\end{aligned}$$

as desired. □

Corollary 6. *Let $i(x) = x^{-1}$, where the inverse is with respect to $\star$. Then*

$$\begin{aligned}
LKDP_{\odot,\otimes}(\sigma,\alpha,\beta,K) &= DP_{\odot}(\rho,\alpha,\delta)\cdot RKDP_{\odot,\star}(i,\delta,\gamma,i(K))\cdot DP_{\odot}(\sigma,\gamma,\beta), \\
RKDP_{\odot,\otimes}(\sigma,\alpha,\beta,K) &= DP_{\odot}(\rho,\alpha,\delta)\cdot LKDP_{\odot,\star}(i,\delta,\gamma,i(K))\cdot DP_{\odot}(\sigma,\gamma,\beta).
\end{aligned}$$

Lemma 7. *Let $i(x) = x^{-1}$, where the inverse is with respect to $\star$. Then*

$$\begin{aligned}
LKDP_{\odot,\star}(i,\delta,\gamma,K) &= LKDP_{\odot,\star}(Id,\delta,\eta,K)\cdot DP_{\odot}(i,\eta,\gamma), \\
RKDP_{\odot,\star}(i,\delta,\gamma,K) &= RKDP_{\odot,\star}(Id,\delta,\eta,K)\cdot DP_{\odot}(i,\eta,\gamma).
\end{aligned}$$

Proof. For the left version, we have

$$\begin{aligned}
LKDP_{\odot,\star}(i,\delta,\gamma,K) &= \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X'\in\mathbb{G}\\ X\odot X'^{-1}=\delta}} [i(K\star X)\odot i(K\star X')^{-1}=\gamma] \\
&= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X'\in\mathbb{G}\\ X\odot X'^{-1}=\delta}} \sum_{\substack{Y,Y'^{-1}\in\mathbb{G}\\ Y\odot Y'^{-1}=\eta}} [(K\star X)\odot (K\star X')^{-1}=\eta] \\
&\cdot [i(Y)\odot i(Y')^{-1}=\gamma] \\
&= \left\{\frac{1}{|\mathbb{G}|} \sum_{\substack{X,X'\in\mathbb{G}\\ X\odot X'^{-1}=\delta}} [(K\star X)\odot (K\star X')^{-1}=\eta]\right\} \\
&\cdot \left\{\frac{1}{|\mathbb{G}|} \sum_{\substack{Y,Y'\in\mathbb{G}\\ Y\odot Y'^{-1}=\eta}} [i(Y)\odot i(Y')^{-1}=\gamma]\right\} \\
&= LKDP_{\odot,\star}(Id,\delta,\eta,K)\cdot DP_{\odot}(i,\eta,\gamma),
\end{aligned}$$

as desired. Similarly, we obtain the relation for the right version. □

Lemma 8. *Let $i(x)=x^{-1}$, where the inverse is with respect to $\star$. Also, let $\sigma'=i\circ\sigma$. Then*

$$\begin{aligned}
DP_{\odot}(i,\eta,\gamma)\cdot DP_{\odot}(\sigma,\gamma,\beta) &= DP_{\odot}(\sigma',\eta,\beta), \\
DP_{\odot}(i,\eta,\gamma)\cdot DP_{\odot}(\sigma,\gamma,\beta) &= DP_{\odot}(\sigma',\eta,\beta).
\end{aligned}$$

Proof. For the first relation we have

$$\begin{aligned}
LHS &= \left\{\frac{1}{|\mathbb{G}|} \sum_{\substack{X,X'\in\mathbb{G}\\ X\odot X'^{-1}=\eta}} [i(X)\odot (i(X'))^{-1}=\gamma]\right\} \\
&\cdot \left\{\frac{1}{|\mathbb{G}|} \sum_{\substack{Y,Y'\in\mathbb{G}\\ Y\odot Y'^{-1}=\gamma}} [\sigma(Y)\odot \sigma(Y')^{-1}=\beta]\right\} \\
&= \frac{1}{|\mathbb{G}|^2} \sum_{\substack{X,X'\in\mathbb{G}\\ X\odot X'^{-1}=\eta}} \sum_{\substack{i(X),i(X')\in\mathbb{G}\\ i(X)\odot i(X')^{-1}=\gamma}} [\sigma(i(X))\odot \sigma(i(X'))^{-1}=\beta] \\
&\cdot [i(X)\odot i(X')^{-1}=\gamma] \\
&= \frac{1}{|\mathbb{G}|} \sum_{\substack{X,X'\in\mathbb{G}\\ X\odot X'^{-1}=\eta}} [\sigma'(X)\odot \sigma'(X')^{-1}=\beta],
\end{aligned}$$

as desired. The second relation is proven similarly. □

Corollary 7. *Let $i(x) = x^{-1}$, where the inverse is with respect to $\star$. Also, let $\sigma' = i \circ \sigma$. Then*

$$LKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = DP_{\odot}(\rho, \alpha, \delta) \cdot RKDP_{\odot,\star}(Id, \delta, \gamma, i(K)) \cdot DP_{\odot}(\sigma', \gamma, \beta),$$
$$RKDP_{\odot,\otimes}(\sigma, \alpha, \beta, K) = DP_{\odot}(\rho, \alpha, \delta) \cdot LKDP_{\odot,\star}(Id, \delta, \gamma, i(K)) \cdot DP_{\odot}(\sigma', \eta, \beta).$$

Proof. We only prove the corollary for the first equality. Using Corollary 6 and Lemmas 6 and 7 we obtain

$$\begin{aligned} LHS &= DP_{\odot}(\rho, \alpha, \delta) \cdot RKDP_{\odot,\star}(i, \delta, \gamma, i(K)) \cdot DP_{\odot}(\sigma, \gamma, \beta) \\ &= DP_{\odot}(\rho, \alpha, \delta) \cdot RKDP_{\odot,\star}(Id, \delta, \eta, i(K)) \cdot DP_{\odot}(i, \eta, \gamma) \cdot DP_{\odot}(\sigma, \gamma, \beta) \\ &= DP_{\odot}(\rho, \alpha, \delta) \cdot RKDP_{\odot,\star}(Id, \delta, \eta, i(K)) \cdot DP_{\odot}(\sigma', \eta, \beta). \end{aligned}$$

Hence, we obtain the equality. □

4 Conclusions

In this paper we filled a gap found in the literature. Namely, the study of SPN structures that use a quasigroup operation to mix keys and plaintexts, and a permutation layer that is non-linear relative to the quasigroup operation. Therefore, we studied the effect of quasigroups isotopic to groups in the design of these SPN structures. We managed to link their security to another symmetric structure that has an extra substitution layer before key mixing takes place. Also, in the case of the equivalent structure, the key and the plaintext are combined using the initial group operation. Note that, to our knowledge, the resulting structure is novel, and thus can lead to a new designs of secure block ciphers.

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. Brunetta, C., Calderini, M., Sala, M.: On Hidden Sums Compatible with a Given Block Cipher Diffusion Layer. Discret. Math. **342**(2), 373–386 (2019)
4. 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)
5. 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)
6. Chauhan, D., Gupta, I., Verma, R.: Construction of Cryptographically Strong S-boxes from Ternary Quasigroups of Order 4. Cryptologia **569**, 658–680 (2021)
7. Chauhan, D., Gupta, I., Verma, R.: Quasigroups and Their Applications in Cryptography. Cryptologia **45**(3), 227–265 (2021)

8. Civino, R., Blondeau, C., Sala, M.: Differential attacks: using alternative operations. Des. Codes Cryptogr. **87**(2-3), 225–247 (2019)
9. Delporte, F.: TikZ for Cryptographers. https://www.iacr.org/authors/tikz/ (2016)
10. Dénes, J., Keedwell, A.D.: Latin Squares: New Developments in the Theory and Applications, Annals of Discrete Mathematics, vol. 46. Elsevier (1991)
11. Dénes, J., Keedwell, A.D.: A New Authentication Scheme Based on Latin Squares. Discrete Mathematics **106**, 157–161 (1992)
12. 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)
13. Gligoroski, D., Markovski, S., Kocarev, L.: Edon-R, An Infinite Family of Cryptographic Hash Functions. I.J. Network Security **8**(3), 293–300 (2009)
14. Knudsen, L.R., Robshaw, M.: The Block Cipher Companion. Springer Science & Business Media (2011)
15. Kościelny, C.: A Method of Constructing Quasigroup-Based Stream-Ciphers. Applied Mathematics and Computer Science **6**, 109–122 (1996)
16. 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)
17. 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)
18. Mouha, N.: On Proving Security against Differential Cryptanalysis. In: CFAIL 2019 (2019)
19. Smith, J.D.: Four Lectures on Quasigroup Representations. Quasigroups Related Systems **15**, 109–140 (2007)
20. Teşeleanu, G.: Cryptographic Symmetric Structures Based on Quasigroups. Cryptologia (2021), To appear. https://eprint.iacr.org/2021/1676
21. Teşeleanu, G.: Quasigroups and Substitution Permutation Networks: A Failed Experiment. Cryptologia **45**(3), 266–281 (2021)
22. Vaudenay, S.: A Classical Introduction to Cryptography: Applications for Communications Security. Springer Science & Business Media (2005)
23. Vojvoda, M., Sỳs, M., Jókay, M.: A Note on Algebraic Properties of Quasigroups in Edon80. Tech. rep., eSTREAM report 2007/005 (2007)