Quasigroups and Substitution Permutation Networks: A Failed Experiment

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. We introduce a generalization of substitution permutation networks using quasigroups. Then, we prove that for quasigroups isotopic with a group $\mathbb{G}$, the complexity of mounting a differential attack against our generalization is the same as attacking a substitution permutation network based on $\mathbb{G}$. Although the result is negative, we believe that the design can be instructional for teaching students that failure is a natural part of research. Also, we hope to prevent others from making the same mistake by showing where such a path leads.

1 Introduction

In its most basic form, differential cryptanalysis [3] predicts how certain changes in the plaintext propagate through a cipher. When considering an ideally randomizing cipher, the probability of predicting these changes is $1/2^n$, where n is the number of input bits. Thus, in the ideal case, it is infeasible 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. Hence, differential cryptanalysis is often the most effective tool against symmetric key cryptographic algorithms [18].

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 [2, 6, 8, 9, 14, 15].

In this paper we introduce a straightforward generalization of substitution-permutation networks (SPN) and study its security. By replacing the group operation $\star$ between keys and (intermediary) plaintexts with a quasigroup operation $\otimes$ we aimed at extending the usage of quasigroups. Unfortunately, by means of differential cryptanalysis we prove that in the case of quasigroups isotopic with a group[3] the problem of breaking an SPN using $\otimes$ reduces to breaking an SPN using $\star$ and a substitution box (s-box) different from the initial one. Thus, if we initialize the SPN with a random secret s-box, replacing $\star$ with $\otimes$ brings

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

no extra security[4]. In the case of static s-boxes, changing $\star$ with $\otimes$ might even affect the SPN's security.

Although the design presented in this paper is not a successful one, we think that its usefulness is twofold. (1) Most scientific reports and papers published appear as sanitized accounts[5] and this gives people a distorted view of scientific research [12, 17, 24, 29]. This leads to a view that implies that failure, serendipity and unexpected results are not a normal part of science [12, 22]. Hence, this report provides students with an indication of the real processes of experimentation. (2) Negative results and false directions are rarely reported [12, 27] and, thus, people are bound to repeat the same mistakes. By presenting our results, we hope to provide an opportunity for others to learn where this path leads. Hence, preventing them to make the same mistakes[6].

Structure of the paper. We introduce notations and definitions in Section 2. An SPN generalization is introduced in Section 3 and its security is studied in Section 4. We conclude in Section 5.

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 [23].

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*

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

[4] *i.e.* we simply obtain another instantiation of the SPN

[5] Authors present their results as if they achieved them in a straightforward manner and not through a messy process.

[6] In [25], the author advises people to write down their mistakes so that they avoid making them again in the future.

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 isotopism exists, then $(\mathbb{G}, \otimes)$, $(\mathbb{H}, \star)$ are called isotopic.*

A popular method for constructing quasigroups [8, 9, 14, 28] is the following. Choose a group $(\mathbb{G}, \star)$ (*e.g.* $(\mathbb{Z}_{2^n}, \oplus)$ or $(\mathbb{Z}_{2^n}, +)$) and three random 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.

$\otimes$	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 $\rho(i) = n - i \bmod n$ [28].

2.2 Group Differential Cryptanalysis

Differential cryptanalysis was initially introduced in [3] for $(\mathbb{Z}_{2^n}, \oplus)$ and was extended to abelian groups in [16]. We further extend the notion to non-commutative groups.

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

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

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

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

Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher [11]. Thus, an attacker first computes the values of a round's LDPs (RDPs). Note that in the case of groups LDPs are dependent only on the round's non-linear layer. Hence, in the case of SPNs only the s-box's LDP values are needed. Once the LDPs are computed, the attacker examines likely differential characteristics. By a differential characteristic χ we understand a sequence of input and output differences such that the output difference of a round is the input difference of the next round. Using the most likely differential characteristic[7] an attacker exploits information coming into the last round of the cipher to derive parts of the last layer's subkey. More precisely, he partially decrypts the last round for each pair of ciphertexts[8] for all possible partial subkeys. When the difference for the input to the last round corresponds to the value expected from χ a counter incremented. The partial subkey value with the highest counter is assumed to be the correct partial subkey. For a concrete example of the whole process, we refer the reader to [11].

Example 3. Let $(\mathbb{G}, \star) = (\mathbb{Z}_8, \oplus)$ and $\sigma = \{5, 1, 0, 3, 4, 2, 6, 7\}$. The difference distribution table for the $\oplus$ operation and the σ s-box can be found in Table 2. For simplicity, we multiplied all the $LDP_{\oplus}(\sigma, \alpha, \beta)$ values by $|\mathbb{G}|$. Note that in this case $LDP_{\oplus} = RDP_{\oplus}$.

α \ β	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	2	0	2	2	0	2	0
2	0	0	4	0	0	4	0	0
3	0	2	0	2	2	0	2	0
4	0	2	0	2	2	0	2	0
5	0	0	0	0	0	4	0	4
6	0	2	0	2	2	0	2	0
7	0	0	4	0	0	0	0	4

Table 2: Difference distribution table for $\oplus$ and σ.

3 Quasigroup Substitution Permutation Network

Let n be a positive integer and $(\mathbb{G}, \otimes)$ a quasigroup. An SPN (see Figure 1) is an iterated structure that processes a plaintext for r rounds. Each round consist of a substitution layer $(S_1, \ldots, S_n)$, a permutation layer (P_i) and a key mixing

[7] When constructing differential trails we ignore the case $\alpha, \beta = e$, where e is the identity element of $\mathbb{G}$.

[8] corresponding to the pairs of plaintexts used to generate χ

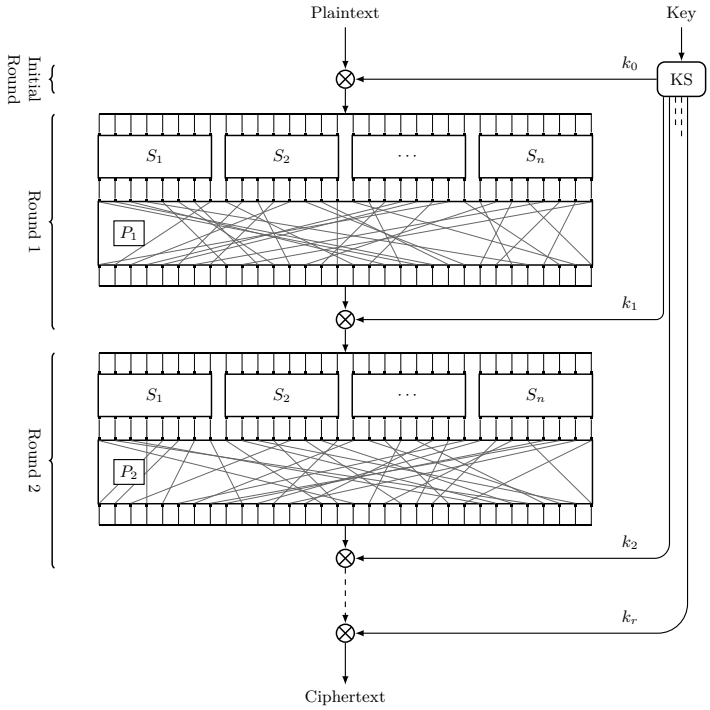

Fig. 1: Quasigroup substitution permutation network

operation. Also, the SPN has an initial round that consists only of a key mixing operation. Note that for each round i the key schedule algorithm (KS) derives the subkey k_i from the initial key.

Let $p_i = p_i^1 \| \dots \| p_i^n$ and $k_i = k_i^1 \| \dots \| k_i^n$ be the intermediary plaintext and, respectively, the subkey for round i[9]. Then, a left quasigroup SPN has as a key mixing operation $k_i \otimes p_i = k_i^1 \otimes p_i^1 \| \dots \| k_i^n \otimes p_i^n$, while a right quasigroup SPN has $p_i \otimes k_i = p_i^1 \otimes k_i^1 \| \dots \| p_i^n \otimes k_i^n$.

Remark 1. Let S_i be randomly chosen for all i values. When $(\mathbb{G}, \otimes) = (\mathbb{Z}_{2^n}, \oplus)$, the distribution of LDP values is studied in [20, 21]. These results are extended in [10], where the authors consider a generic abelian group $(\mathbb{G}, \otimes)$. When all the s-boxes are static[10], the distribution of LDPs for $(\mathbb{Z}_{2^n}, \oplus)$ is studied for example in [5, 7, 19].

[9] Note that $p_i^j, k_i^j \in \mathbb{G}$ for all j values.
[10] *i.e* are fixed and public for all of the SPN's implementations

4 Quasigroup Differential Cryptanalysis

In this section we extend the notion of differential cryptanalysis to quasigroup SPNs. After showing that our generalisation is correct, we use it to study the security of SPNs based on quasigroups isotopic to a group.

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

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

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

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

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

Example 4. Let $\omega^{-1} = \{4, 7, 0, 5, 1, 2, 3, 6\}$, $\pi = \{6, 1, 5, 2, 3, 0, 4, 7\}$ and $\rho = \{5, 1, 2, 6, 4, 0, 7, 3\}$. Using Example 3 as a starting point, in Table 3 we present the difference distribution tables for $\otimes$ and σ. To see that in general DP is

α \ β	0	1	2	3	4	5	6	7
0	5	0	0	1	1	0	1	0
1	0	2	1	1	1	1	2	0
2	1	1	3	1	2	0	0	0
3	0	1	0	3	0	1	1	2
4	0	1	1	0	3	0	1	2
5	1	1	0	2	1	3	0	0
6	1	2	1	0	0	1	3	0
7	0	0	2	0	0	2	0	4

(a) $|G| \cdot DP_\oslash(\sigma, \alpha, \beta)$

α \ β	0	1	2	3	4	5	6	7
0	3	2	1	0	0	0	1	1
1	1	3	0	0	1	2	1	0
2	0	0	3	1	1	2	1	0
3	0	1	2	3	0	0	1	1
4	1	0	0	1	3	0	2	1
5	2	0	0	2	0	4	0	0
6	1	1	1	1	2	0	2	0
7	0	1	1	0	1	0	0	5

(b) $|G| \cdot DP_\oslash(\sigma, \alpha, \beta)$

Table 3: Difference distribution tables for $\otimes$ and σ.

different from KDP, we also computed the keyed distribution tables for $K = 0$. The results are presented in Table 4.[11]

[11] The code used to generate Tables 2 to 5 can be found at https://github.com/teseleanu/quasigroup_differential_4_bit.

α \ β	0	1	2	3	4	5	6	7
0	1	0	2	1	0	1	0	3
1	2	0	0	2	1	1	1	1
2	0	0	4	0	0	2	2	0
3	1	0	2	1	3	0	1	0
4	1	1	0	0	1	3	0	2
5	2	1	0	3	0	1	1	0
6	1	1	0	0	2	0	3	1
7	0	5	0	1	1	0	0	1

(a) $|G| \cdot KDP_{\oslash}(\sigma, \alpha, \beta, K)$

α \ β	0	1	2	3	4	5	6	7
0	0	1	0	1	1	5	0	0
1	5	0	1	0	0	0	1	1
2	1	0	5	0	0	0	1	1
3	0	1	0	1	5	1	0	0
4	1	0	1	0	0	0	1	5
5	0	1	0	5	1	1	0	0
6	0	5	0	1	1	1	0	0
7	1	0	1	0	0	0	5	1

(b) $|G| \cdot KDP_{\oslash}(\sigma, \alpha, \beta, K)$

Table 4: Keyed difference distribution tables for $\otimes$ and σ.

When $\mathbb{G}$ is an associative quasigroup[12], we managed to prove (Lemma 2) that key bits K have no influence on the input difference value $\Delta_\bullet$, where $\bullet \in \{\oslash, \oslash\}$, and, thus, can be ignored. In other words, a keyed s-box has the same difference distribution table as an unkeyed s-box (Corollary 1).

Lemma 2. *If $\otimes$ is associative, then the following identities hold*

$$\Delta_{\oslash}(K \otimes X, K \otimes X') = \Delta_{\oslash}(X, X')$$
$$\Delta_{\oslash}(X \otimes K, X' \otimes K) = \Delta_{\oslash}(X, X').$$

Proof. Using Lemma 1 we obtain

$$X \otimes \Delta_{\oslash}(X, X') = X \otimes (X \oslash X') = X',$$

that leads to

$$\begin{aligned}\Delta_{\oslash}(K \otimes X, K \otimes X') &= (K \otimes X) \oslash (K \otimes X') \\ &= (K \otimes X) \oslash [K \otimes (X \otimes \Delta_{\oslash}(X, X'))] \\ &= (K \otimes X) \oslash [(K \otimes X) \otimes \Delta_{\oslash}(X, X')] \\ &= \Delta_{\oslash}(X, X').\end{aligned}$$

Similarly we prove the second equation. □

Corollary 1. *If $\otimes$ is associative, then the following identities hold*

$$KDP_{\oslash}(\sigma, \alpha, \beta, K) = DP_{\oslash}(\sigma, \alpha, \beta),$$
$$KDP_{\oslash}(\sigma, \alpha, \beta, K) = DP_{\oslash}(\sigma, \alpha, \beta).$$

[12] The need for associativity was pointed out to the author by one of the anonymous reviewers.

Proof. According to Definition 1, given X and K there exists an unique element Y such that $X = K \otimes Y$. Thus, we have

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

where for the third equality we use Lemma 2. Similarly, we prove the second equation. □

To see if our definition is a generalization for the group differential probability, we must recover LDP and RDP when $(\mathbb{G}, \otimes)$ is a group. We prove this in Corollary 2. Note that any group is associative and, according to Corollary 1, equivalence to DP suffices.

Lemma 3. *If $(\mathbb{G}, \otimes)$ forms a group then the following identities hold*

$$\begin{aligned}
\Delta_{\oslash}(X, X') &= \Delta_{\otimes}(X^{-1}, X'), \\
\Delta_{\oslash}(X, X') &= \Delta_{\otimes}(X', X^{-1}).
\end{aligned}$$

Proof. Note that

$$\begin{aligned}
\Delta_{\oslash}(X, X') = \alpha &\iff X \otimes \alpha = X' \\
&\iff X^{-1} \otimes X' = \alpha \iff \Delta_{\otimes}(X^{-1}, X') = \alpha.
\end{aligned}$$

Similarly, we prove the second equation. □

Corollary 2. *If $(\mathbb{G}, \otimes)$ forms a group then $DP_{\oslash}(\sigma, \alpha, \beta) = LDP_{\otimes}(\sigma, \alpha, \beta)$ and $DP_{\oslash}(\sigma, \alpha, \beta) = RDP_{\otimes}(\sigma, \alpha, \beta)$.*

Proof. Note that

$$\begin{aligned}
DP_{\oslash}(\sigma, \alpha, \beta) &= \frac{1}{|\mathbb{G}|} \sum_{\substack{X, X' \in \mathbb{G} \\ \Delta_{\oslash}(X, X') = \alpha}} [\Delta_{\oslash}(\sigma(X), \sigma(X')) = \beta] \\
&= \frac{1}{|\mathbb{G}|} \sum_{\substack{X, X' \in \mathbb{G} \\ \Delta_{\otimes}(X^{-1}, X') = \alpha}} [\Delta_{\otimes}(\sigma(X)^{-1}, \sigma(X')) = \beta] \\
&= LDP_{\otimes}(\sigma, \alpha, \beta).
\end{aligned}$$

Similarly we prove the second equation. □

The action of deriving $\otimes$ from $\star$ gives rise to a natural question: what happens if we derive a new quasigroup operation $\hat{\otimes}$ from $\otimes$? Unfortunately, according to Lemma 4 we end up with another isotopy of $\star$. Thus, the problem of studying KDP for a chain of isotopies is reduced to studying KDP for an isotopy of the base operation $\star$.

Lemma 4. *We define $x \,\hat{\otimes}\, y = \hat{\omega}^{-1}(\hat{\pi}(x) \otimes \hat{\rho}(y))$. Then there exist ω', π', ρ' such that $x \,\hat{\otimes}\, y = \omega'^{-1}(\pi'(x) \star \rho'(y))$.*

Proof. Remark that

$$\begin{aligned} x \,\hat{\otimes}\, y &= \hat{\omega}^{-1}(\hat{\pi}(x) \otimes \hat{\rho}(y)) \\ &= \hat{\omega}^{-1}(\omega^{-1}(\pi(\hat{\pi}(x)) \star \rho(\hat{\rho}(y)))) \\ &= \omega'^{-1}(\pi'(x) \star \rho'(y)), \end{aligned}$$

where $\omega' = \hat{\omega} \circ \omega$, $\pi' = \hat{\pi} \circ \pi$ and $\rho' = \hat{\rho} \circ \rho$. □

When the base group $(\mathbb{G}, \star)$ is commutative we observe (Lemma 5) that taking into consideration both $\oslash$ and $\ocirc$ for designing an SPN does not make sense.

Lemma 5. *We define $x \,\bar{\otimes}\, y = \omega^{-1}(\rho(x) \star \pi(y)) = z$, $x \,\bar{\oslash}\, z = y$ and $z \,\bar{\ocirc}\, y = x$. If $\star$ is commutative then the following identities hold*

$$\begin{aligned} KDP_{\oslash}(\sigma, \alpha, \beta, K) &= KDP_{\bar{\ocirc}}(\sigma, \alpha, \beta, K), \\ KDP_{\ocirc}(\sigma, \alpha, \beta, K) &= KDP_{\bar{\oslash}}(\sigma, \alpha, \beta, K). \end{aligned}$$

Proof. The lemma's hypothesis implies that

$$\begin{aligned} x \otimes y &= \omega^{-1}(\pi(x) \star \rho(y)) \\ &= \omega^{-1}(\rho(x) \star \pi(y)) \\ &= y \,\bar{\otimes}\, x. \end{aligned}$$

Thus, $\Delta_{\oslash}(x, y) = \Delta_{\bar{\ocirc}}(y, x)$ for any $x, y \in \mathbb{G}$. Hence, $KDP_{\oslash}(\sigma, \alpha, \beta, K) = KDP_{\bar{\ocirc}}(\sigma, \alpha, \beta, K)$. The second statement is proven similarly. □

Corollary 3. *If $\star$ is commutative and $\pi = \rho$ then we have $KDP_{\oslash}(\sigma, \alpha, \beta, K) = KDP_{\ocirc}(\sigma, \alpha, \beta, K)$.*

We further study the impact of the ω, π, ρ permutations on KDP.

Lemma 6. *Let $\pi' = \omega^{-1} \circ \pi$, $\rho' = \omega^{-1} \circ \rho$, $\sigma' = \omega^{-1} \circ \sigma \circ \omega$. We define $x * y = \pi'(x) \star \rho'(y) = z$, $x \backslash z = y$ and $z / y = x$. Then the following identities hold*

$$\begin{aligned} KDP_{\oslash}(\sigma, \alpha, \beta, K) &= KDP_{\backslash}(\sigma', \omega(\alpha), \omega(\beta), \omega(K)) \\ KDP_{\ocirc}(\sigma, \alpha, \beta, K) &= KDP_{/}(\sigma', \omega(\alpha), \omega(\beta), \omega(K)). \end{aligned}$$

Proof. First we rewrite

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

Let $\omega(X)=Y$, $\omega(X')=Y'$ and $\omega(\alpha)=A$. Then

$$\begin{aligned}X\otimes\alpha=X' &\iff \pi(X)\star\rho(\alpha)=\omega(X')\\ &\iff \pi'(\omega(X))\star\rho'(\omega(\alpha))=\omega(X')\\ &\iff \pi'(Y)\star\rho'(A)=Y'\\ &\iff Y*A=Y'. \end{aligned}\tag{1}$$

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

$$\begin{aligned}\sigma(K\otimes X)&=\sigma(\omega^{-1}(\pi(K)\star\rho(X))\\ &=\sigma(\omega^{-1}(\pi'(\omega(K))\star\rho'(\omega(X))))\\ &=\omega^{-1}(\sigma'(\pi'(K')\star\rho'(Y)))\\ &=\omega^{-1}(\sigma'(K'*Y))\end{aligned}\tag{2}$$

and similarly

$$\sigma(K\otimes X')=\omega^{-1}(\sigma'(K'*Y')).\tag{3}$$

Let $\omega(\beta)=B$. Using Equations (2) and (3) we obtain

$$\begin{aligned}\sigma(K\otimes X)\otimes\beta=\sigma(K\otimes X') &\iff \omega^{-1}(\sigma'(K'*Y))\otimes\beta=\omega^{-1}(\sigma'(K'*Y'))\\ &\iff \pi'(\sigma'(K'*Y))\star\rho(\beta)=\sigma'(K'*Y')\\ &\iff \pi'(\sigma'(K'*Y))\star\rho'(\omega(\beta))=\sigma'(K'*Y')\\ &\iff \sigma'(K'*Y)*B=\sigma'(K'*Y').\end{aligned}\tag{4}$$

Using Equations (1) and (4) we obtain

$$\begin{aligned}KDP_{\oslash}(\sigma,\alpha,\beta,K)&=\frac{1}{|\mathbb{G}|}\sum_{\substack{X\in\mathbb{G}\\ \Delta_{\otimes}(X,\alpha)=X'}}[\Delta_{\otimes}(\sigma(K\otimes X),\beta)=\sigma(K\otimes X')]\\ &=\frac{1}{|\mathbb{G}|}\sum_{\substack{Y\in\mathbb{G}\\ \Delta_{*}(Y,A)=Y'}}[\Delta_{*}(\sigma'(K'*Y),B)=\sigma'(K'*Y')]\\ &=\frac{1}{|\mathbb{G}|}\sum_{\substack{Y,Y'\in\mathbb{G}\\ \Delta_{\backslash}(Y,Y')=A}}[\Delta_{\backslash}(\sigma'(K'*Y),\sigma'(K'*Y'))=B]\\ &=KDP_{\backslash}(\sigma',A,B,K').\end{aligned}$$

Similarly, we obtain $KDP_{\oslash}(\sigma,\alpha,\beta,K)=KDP_{/}(\sigma',A,B,K)$. □

Lemma 6 tells us that it is irrelevant from a differential point of view[13] if we define the quasigroup operation with $\omega \neq Id$ or $\omega = Id$. Thus, we further restrict our study[14] to the quasigroup operation $x \otimes y = \pi(x) \star \rho(y)$.

Lemma 7. *Let $\pi' = \rho^{-1} \circ \pi$, $\sigma' = \rho^{-1} \circ \sigma \circ \rho$. We define $x *_1 y = \rho(\pi'(x) \star y) = z$, $x \backslash_1 z = y$ and $z /_1 y = x$. Then the following identity holds*

$$KDP_{\oslash}(\sigma, \alpha, \beta, K) = KDP_{\backslash_1}(\sigma', \rho(\alpha), \rho(\beta), \rho(K)).$$

Proof. Let $\rho(X) = Y$, $\rho(X') = Y'$ and $\rho(\alpha) = A$. Then

$$\begin{aligned} X \otimes \alpha = X' &\iff \pi(X) \star \rho(\alpha) = X' \\ &\iff \rho(\pi'(\rho(X)) \star A) = \rho(X') \\ &\iff \rho(\pi'(Y) \star A) = Y' \\ &\iff Y *_1 A = Y'. \end{aligned} \tag{5}$$

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

$$\begin{aligned} \sigma(K \otimes X) &= \sigma(\pi(K) \star \rho(X)) \\ &= \sigma(\pi'(\rho(K)) \star Y) \\ &= \rho^{-1}(\sigma'(\rho(\pi'(K') \star Y))) \\ &= \rho^{-1}(\sigma'(K' *_1 Y)) \end{aligned} \tag{6}$$

and similarly

$$\sigma(K \otimes X') = \rho^{-1}(\sigma'(K' *_1 Y')). \tag{7}$$

Let $\omega(\beta) = B$. Using Equations (6) and (7) we obtain

$$\begin{aligned} \sigma(K \otimes X) \otimes \beta = \sigma(K \otimes X') &\iff \rho^{-1}(\sigma'(K' *_1 Y)) \otimes \beta = \rho^{-1}(\sigma'(K' *_1 Y')) \\ &\iff \pi'(\sigma'(K' *_1 Y)) \star \rho(\beta) = \rho^{-1}(\sigma'(K' *_1 Y')) \\ &\iff \rho(\pi'(\sigma'(K' *_1 Y)) \star B) = \sigma'(K' *_1 Y') \\ &\iff \sigma'(K' *_1 Y) *_1 B = \sigma'(K' *_1 Y'). \end{aligned} \tag{8}$$

Using Equations (5) and (8) we obtain

$$\begin{aligned} KDP_{\oslash}(\sigma, \alpha, \beta, K) &= \frac{1}{|\mathbb{G}|} \sum_{\substack{X \in \mathbb{G} \\ \Delta_{\otimes}(X, \alpha) = X'}} [\Delta_{\otimes}(\sigma(K \otimes X), \beta) = \sigma(K \otimes X')] \\ &= \frac{1}{|\mathbb{G}|} \sum_{\substack{Y \in \mathbb{G} \\ \Delta_{*_1}(Y, A) = Y'}} [\Delta_{*_1}(\sigma'(K' *_1 Y), B) = \sigma'(K' *_1 Y')] \\ &= KDP_{\backslash_1}(\sigma', A, B, K'). \end{aligned}$$

□

[13] *e.g.* we obtain the same differential probability KDP

[14] without loss of generality

Lemma 8. *Let $\rho' = \pi^{-1} \circ \rho$, $\sigma' = \pi^{-1} \circ \sigma \circ \pi$. We define $x *_2 y = \pi(x \star \rho'(y)) = z$, $x \backslash_2 z = y$ and $z /_2 y = x$. Then the following identity holds*

$$KDP_{\oslash}(\sigma, \alpha, \beta, K) = KDP_{/_2}(\sigma', \rho(\alpha), \rho(\beta), \rho(K)).$$

Lemma 8 is proven similarly to Lemma 7 and, thus, its proof is omitted. Remark that our scope is to see how certain differences in the input affect the output of the non-linear layer. But our non-linear has either the form $\sigma(\rho(\pi(x) \star y))$ or the form $\sigma(\pi(x \star \rho(y)))$. Thus, a simpler strategy would be to study directly $\sigma_1 = \rho \circ \sigma$ and $\sigma_2 \pi \circ \sigma$ instead of σ. Taking into account the previous remark, we further restrict our study to $x \otimes_1 y = \pi(x) \star y$ and $x \otimes_2 y = x \star \rho(y)$.

Example 5. Using Examples 3 and 4 as starting points, in Table 5 we present the difference distribution tables for $\otimes_1$ and $\otimes_2$.

α \ β	0	1	2	3	4	5	6	7
0	2	2	0	0	0	0	2	2
1	0	2	0	2	2	0	0	2
2	0	0	2	2	0	0	2	2
3	2	0	2	0	2	0	0	2
4	2	0	0	2	2	0	2	0
5	0	0	0	0	0	8	0	0
6	2	2	2	2	0	0	0	0
7	0	2	2	0	2	0	2	0

(a) $|G| \cdot KDP_{\otimes_1}(\sigma, \alpha, \beta, K)$

α \ β	0	1	2	3	4	5	6	7
0	2	2	2	2	0	0	0	0
1	2	0	0	2	2	0	0	2
2	0	0	2	2	2	0	2	0
3	0	2	0	2	0	0	2	2
4	2	2	0	0	2	0	2	0
5	0	0	0	0	0	8	0	0
6	2	0	2	0	0	0	2	2
7	0	2	2	0	2	0	0	2

(b) $|G| \cdot KDP_{\oslash_2}(\sigma, \alpha, \beta, K)$

Table 5: Difference distribution tables for $\otimes_1$ and $\otimes_2$.

Example 6. Let $\mathbb{G} = \mathbb{Z}_{256}$. To see how the maximum values for $LDP_{\oplus}$, $KDP_{\otimes_1}$ and $KDP_{\oslash_2}$ are distributed, we run the following experiment 10000 times[15]. We randomly generated π, ρ and then we computed the maximum values of $256 \cdot LDP_{\oplus}$[16]. Then we generated 1000 keys and for each π and ρ we computed the mean value of the maximum values of $256 \cdot KDP_{\otimes_1}$ and $256 \cdot KDP_{\oslash_2}$. After gathering data from these experiments we computed the expected value $E[x]$ and the median absolute deviation MAD for each differential probability. The results are presented in Example 6.

We can see from Examples 3 and 5 that the difference distribution tables for $\oplus$, $\otimes_1$ and $\otimes_2$ have nothing in common. Also, Example 6 tells us that the

[15] The associated code can be found at https://github.com/teseleanu/quasigroup_differential_8_bit.

[16] In this case we excluded the value 256.

	$LDP_{\oplus}$	$KDP_{\oslash_1}$	$KDP_{\oslash_2}$
$E[x]$	11.3550	7.56167	7.56204
MAD	1.067740	0.036824	0.036817

Table 6: Distribution of maximal differential probabilities.

average probability of success for a differential attack is lower in the case of $\otimes_1$ and $\otimes_2$ than in the case of $\oplus$. Thus, it might seem that we discovered a new method for improving SPNs.

Unfortunately, this is not the case. Let's review what we want to do. We want to study how input differences affect the output differences of a keyed s-box σ_K. Since K and, for example, π are generated as a pair, for a differential attack to work we do not really need to know K. The value $\pi(K)$ suffices. Thus, another way of studying the output differences of S_K is by using $\Delta_\star$. According to Lemma 9 the resulting differential probability is independent of $\pi(K)$. Hence, the choice for the permutation that acts on the key is irrelevant. This leads to the fact that using an isotopy is identical[17] to using the base operation.

Lemma 9. *The following identities hold*

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

Proof. We simply remark that

$$\begin{aligned}\Delta_\star((\pi(K) \star X)^{-1}, \pi(K) \star X') &= X^{-1} \star \pi(K)^{-1} \star \pi(K) \star X' \\ &= X^{-1} \star X' = \Delta_\star(X, X').\end{aligned}$$

Similarly we obtain the second equation. □

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

Proposition 1. *A quasigroup SPN derived from a group SPN using an isotopy has the same differential security as the same group SPN instantiated with a different s-box.*

5 Conclusions

In this paper we studied the effect of using quasigroups isotopic to groups when designing SPNs. According to Lemmas 6 to 9, the problem of studying an SPN based on an isotopic quasigroup reduces to studying an SPN based on the base group. When we consider SPNs with random secret s-boxes (*e.g.* [4, 26]) using an isotopic quasigroup does not pose a problem, since studying its security reduces

[17] from a differential point of view

to studying the security of an SPN with a different s-box than the original one. Thus, in this case, the extension is 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 operation might lead to cryptographic weaknesses unforeseen by the designers of the static s-box.

Although this experiment failed from a cryptographic point of view, in our opinion it can still be useful as a teaching tool, as well as for preventing others from making the same mistake. Also, our analysis might serve as a stepping stone to a security analysis of generic quasigroup SPNs.

References

1. CFAIL 2019. https://www.cfail2019.com/ (2019)
2. Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J.: A Message Authentication Code Based on Latin Squares. In: ACISP 1997. Lecture Notes in Computer Science, vol. 1270, pp. 194–203. Springer (1997)
3. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: CRYPTO 1990. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1991)
4. 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)
5. 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)
6. Dénes, J., Keedwell, A.D.: A New Authentication Scheme Based on Latin Squares. Discrete Mathematics **106**, 157–161 (1992)
7. Dobbertin, H.: One-to-One Highly Nonlinear Power Functions on GF(2^n). Appl. Algebra Eng. Commun. Comput. **9**(2), 139–152 (1998)
8. 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)
9. Gligoroski, D., Markovski, S., Kocarev, L.: Edon-R, An Infinite Family of Cryptographic Hash Functions. I.J. Network Security **8**(3), 293–300 (2009)
10. 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)
11. Heys, H.M.: A Tutorial on Linear and Differential Cryptanalysis. Cryptologia **26**(3), 189–221 (2002)
12. Howitt, S.M., Wilson, A.N.: Revisiting "Is the Scientific Paper a Fraud?". EMBO reports **15**(5), 481–484 (2014)
13. Jean, J.: TikZ for Cryptographers. https://www.iacr.org/authors/tikz/ (2016)
14. Kościelny, C.: A Method of Constructing Quasigroup-Based Stream-Ciphers. Applied Mathematics and Computer Science **6**, 109–122 (1996)
15. 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)

16. 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)
17. Medawar, P.: Is the Scientific Paper a Fraud? The Listener pp. 377–378 (1963)
18. Mouha, N.: On Proving Security against Differential Cryptanalysis. In: CFAIL 2019 (2019)
19. Nyberg, K.: Perfect Nonlinear S-boxes. In: EUROCRYPT 1991. Lecture Notes in Computer Science, vol. 547, pp. 378–386. Springer (1991)
20. O'Connor, L.: On the Distribution of Characteristics in Bijective Mappings. Journal of Cryptology **8**(2), 67–86 (1995)
21. 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)
22. Schwartz, M.A.: The Importance of Stupidity in Scientific Research. Journal of Cell Science **121**(11), 1771–1771 (2008)
23. Smith, J.D.: Four Lectures on Quasigroup Representations. Quasigroups Related Systems **15**, 109–140 (2007)
24. Tao, T.: Ask Yourself Dumb Questions - and Answer Them! https://terrytao.wordpress.com/career-advice/ask-yourself-dumb-questions-and-answer-them/
25. Tao, T.: Use The Wastebasket. https://terrytao.wordpress.com/career-advice/use-the-wastebasket/
26. 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)
27. Truran, P.: Practical Applications of the Philosophy of Science: Thinking About Research. Springer Science & Business Media (2013)
28. Vojvoda, M., Sỳs, M., Jókay, M.: A Note on Algebraic Properties of Quasigroups in Edon80. In: SASC 2007 (2007)
29. Weidman, D.R.: Emotional Perils of Mathematics. Science **149**(3688), 1048–1048 (1965)