Rebuttal to claims in Section 2.1 of the ePrint report 2021/583 "Entropoid-based cryptography is group exponentiation in disguise",

Danilo Gligoroski*

June 28, 2021

Abstract

In the recent ePrint report 2021/583 titled "Entropoid-based cryptography is group exponentiation in disguise" Lorenz Panny gave a cryptanalysis of the entropoid based instances proposed in our eprint report 2021/469. We acknowledge the correctness of his claims for the concrete instances described in our original report 2021/469.

However, we find that claims for the general applicability of his attack on the general Entropoid framework are misleading. Namely, based on the Theorem 1 in his report, which claims that for every entropic quasigroup $(G, *)$, there exists an Abelian group $(G, \cdot)$, commuting automorphisms σ, τ of $(G, \cdot)$, and an element $c \in G$, such that $x * y = \sigma(x) \cdot \tau(y) \cdot c$ the author infers that *"all instantiations of the entropoid framework should be breakable in polynomial time on a quantum computer."*

There are two misleading parts in these claim: **1.** It is implicitly assumed that all instantiations of the entropoid framework would define entropic quasigroups - thus fall within the range of algebraic objects addressed by Theorem 1. *We will show a construction of entropic groupoids that are not quasigroups*; **2.** It is implicitly assumed that finding the group $(G, \cdot)$, the commuting automorphisms σ and τ and the constant c *would be easy for every given entropic operation* $*$ and its underlying groupoid $(G, *)$. However, the provable existence of a mathematical object *does not guarantee an easy finding* of that object.

Treating the original entropic operation $* := *_1$ as a one-dimensional entropic operation, we construct multidimensional entropic operations $* := *_m$, for $m \geqslant 2$ and we show that newly constructed operations do not have the properties of $* = *_1$ that led to the recovery of the automorphism σ, the commutative operation $\cdot$ and the linear isomorphism ι and its inverse ι^{-1}.

We give proof-of-concept implementations in SageMath 9.2 for the new multidimensional entropic operations $* := *_m$ defined over several basic operations $* := *_1$ and we show how the non-associative and non-commutative exponentiation works for the key exchange and digital signature schemes originally proposed in report 2021/469.

1 Introduction

We would like to start this rebuttal by giving credits to Lorenz Panny for his ePrint report [7], where he showed how the instances proposed in our ePrint report [2] can be reduced to a polynomial number of discrete logarithm problems in Abelian groups - thus solvable efficiently on quantum computers. We give credit to his openness to discuss his findings and informing us before he published his result on ePrint. Actually, this rebuttal is the second version (where the first version had to be updated thanks to Lorenz Panny given feedback).

We would also like to give credit to Daniel Nager [5] who first mentioned the possibility to work with entropic groupoids (magmas) that are not quasigroups (only left quasigroups). In this rebuttal we propose concrete construction of such groupoids.

The entropic quasigroups in [2] are defined over the set $\mathbb{E} := \mathbb{F}_{(p-1)^2}$ with the operation $*$:

$$(x_1, x_2) * (y_1, y_2) = \Bigg(\frac{a_3(a_8 b_2 - b_7)}{a_8 b_7} + a_3 x_2 + \frac{a_8 b_2 y_1}{b_7} + a_8 x_2 y_1, \\ - \frac{b_2(a_8 - a_3 b_7)}{a_8 b_7} + \frac{a_3 b_7 y_2}{a_8} + b_2 x_1 + b_7 x_1 y_2 \Bigg), \tag{1}$$

where $a_3, a_8, b_2, b_7 \in \mathbb{F}_p$, $a_8 \neq 0$ and $b_7 \neq 0$, and the operations $-$ and $/$ are the operations of subtraction and division in $\mathbb{F}_p$.

The core success of the Lorenz' attack described in the first part of Section 2 of [7] relies on the following properties of the instances of the entropic quasigroups proposed in [2]:

*Department of Information Security and Communication Technologies, Norwegian University of Science and Technology - NTNU

1. The algebraic degree of operation $*$ is 2;
2. The entropic operation $*$ is quasigroup;
3. There exists an element $\mathbf{1} = \left(\frac{1}{b_7} - \frac{a_3}{a_8}, \frac{1}{a_8} - \frac{b_2}{b_7}\right)$ which is a multiplicative left unit for the groupoid $(\mathbb{E}, *)$;
4. Due to Theorem 1 and Theorem 2 from [9], it is easy to find an automorpism $\sigma : \mathbb{E} \to \mathbb{E}$, $\sigma(x) = x * \mathbf{1}$ such that $x * y = \sigma(x) \cdot y$, where $\cdot$ is a commutative operation

$$(x_1, x_2) \cdot (y_1, y_2) = \Bigg(b_7 x_1 y_1 + \frac{a_3 b_7}{a_8} x_1 + \frac{a_3 b_7}{a_8} y_1 + \frac{a_3^2 b_7 - a_3 a_8}{a_8^2}, \\ a_8 x_2 y_2 + \frac{a_8 b_2}{b_7} x_2 + \frac{a_8 b_2}{b_7} y_2 + \frac{a_8 b_2^2 - b_2 b_7}{b_7^2}\Bigg), \tag{2}$$

   i.e. the algebraic structure $(\mathbb{E}, \cdot)$ is an Abelian group;
5. Instead of being represented in the most general form by two commuting automorphisms σ, τ of $(G, \cdot)$, and an element $c \in G$, such that $x * y = \sigma(x) \cdot \tau(y) \cdot c$, the instances of the operation $*$ are represented in a simpler way as $x * y = \sigma(x) \cdot y$;
6. The group $(\mathbb{E}, \cdot)$ can be seen as a direct product of two affine algebraic groups (there is no mix of components x_1 and y_2 and of components x_2 and y_1);
7. It is easy to find a linear isomorphism between $(\mathbb{E}, \cdot)$ and $(\mathbb{F}_p^\times)^2$, $\iota : \mathbb{E} \to (\mathbb{F}_p^\times)^2$ (and its inverse ι^{-1}) where

$$\iota(x_1, x_2) = (b_7 x_1 + \frac{a_3 b_7}{a_8}, a_8 x_2 + \frac{a_8 b_2}{b_7}).$$

Then the attack on the instances proposed in [2] uses the isomorphism ι to map g, $\sigma(g)$ and $g^{\mathbf{A}}$ into $(\mathbb{F}_p^\times)^2$, solve 6 discrete logarithm problems in $\mathbb{F}_p$ and one 2×2 linear system in $\mathbb{Z}^2$, and use that solution to construct an equivalent private key that computes $x^{\mathbf{A}}$ for any $x \in \mathbb{E}$.

Thus, we praise the author for constructing very efficient attack on this specific instance of the Entropic Based Cryptography.

What about the general case? Do all instances of the entropoid-based cryptography framework produce algebraic structures that are quasigroups with the properties 1 - 7 discussed above?

2 Rebuttal to the claims in the General attack

In the subsection 2.1 of [7], there is a proposal for a generic attack on every instance of the entropoid framework. The attack relies on a proposed theorem that the author composed from three related works by Murdoch [4], Toyoda [9] and Bruck [1]. We give here the original theorem as it is given in [7] (with a slight notation change - instead of notation x^σ and y^τ we use the notation $\sigma(x)$ and $\tau(y)$):

Theorem 1 (Theorem 1 in [7]) *For every entropic quasigroup $(G, *)$, there exists an abelian group $(G, \cdot)$, commuting automorphisms σ, τ of $(G, \cdot)$, and an element $c \in G$, such that*

$$x * y = \sigma(x) \cdot \tau(y) \cdot c$$

Based on this theorem the author of [7] infers that *"all instantiations of the entropoid framework should be breakable in polynomial time on a quantum computer."*

Rebuttal arguments

1. The author of [7] implicitly infers that all instantiations of the entropoid framework will operate with the algebraic structures that are quasigroups, and thus are addressable by the works of Murdoch, Toyoda and Bruck. That is not necessary true. In what follows we give a construction of multidimensional entropic operations based on previously defined simpler entropic operations, that are not quasigroup operations. They are groupoids (magmas) with only a left cancellation property (left quasigroups).
2. The author of [7] implicitly infers that finding the commuting automorphisms σ, τ of $(G, \cdot)$ as well as the operation $\cdot$ would be easy for every given entropic quasigroup $(G, *)$. Ignoring for a moment the fact that we do not have a constructive proof of that theorem by which we can measure the complexity of the proposed attack, we can only point to the fact that a provable existence of a mathematical object *does not guarantee an easy finding* of that object. One simple example of this universal principle comes from the design of cryptographic hash functions: it is easy to prove that there exist infinitely many colliding pairs of inputs, but for a carefully designed cryptographic hash function, finding a single colliding pair is hard.

2.1 Construction of entropic operations that are not quasigroups

Let us first update the notation about the operation $*$ used in equation (1) and in [2]. Since it is designed for a "one-dimensional" $\mathbb{E}$ we will denote that operation as $*_1$:

$$(x_1, x_2) *_1 (y_1, y_2) = \Bigg(\frac{a_3(a_8 b_2 - b_7)}{a_8 b_7} + a_3 x_2 + \frac{a_8 b_2 y_1}{b_7} + a_8 x_2 y_1, \\ - \frac{b_2(a_8 - a_3 b_7)}{a_8 b_7} + \frac{a_3 b_7 y_2}{a_8} + b_2 x_1 + b_7 x_1 y_2 \Bigg), \tag{3}$$

Next, to give a definition of an entropic operation $* := *_m$ over $\mathbb{E}^m = ((\mathbb{F}_p^\times)^2)^m$ we will adapt the ideas for building multidimensional entropic operations from simpler entropic operations given in a recent ePrint report 2021/444 [6] by Nager and Jianfang, but with the style of D-transformations as defined in [3].

Definition 1 *Let $x, y \in \mathbb{E}^m$, i.e., $x = (x_0 \ldots, x_{m-1})$ and $y = (y_0, \ldots, y_{m-1})$. A component-wise product Π of x and y is defined as:*

$$z = \Pi(x, y) = (z_0, \ldots, z_{m-1}), \tag{4}$$

where $z_i = x_i *_1 y_i$ for $i \in \mathbb{Z}_m$.

Definition 2 *Let $x \in \mathbb{E}^m$, i.e., $x = (x_0 \ldots, x_{m-1})$ and let $l \in \mathbb{E}^*$ is a nonzero element of $\mathbb{E}$. A D-transformation $\mathcal{D}$ of x with the respect of the leader element l is defined as:*

$$z = \mathcal{D}_l(x) = (z_0, \ldots, z_{m-1}), \tag{5}$$

where $z_0 = l * x_0$, and $z_i = x_{i-1} *_1 x_i$ for $i \in \{1, \ldots, m-1\}$.

Let we denote by $\mathbf{\Delta}_m$ a derangement permutation (a permutation without a fixed element) on indices $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. In other words $\mathbf{\Delta}_m(0, 1, \ldots, m-1) = (\delta(0), \ldots, \delta(m-1))$, where $\delta(i) \neq i$ for all $i \in \mathbb{Z}_m$.

By overloading the notation, let us denote the permutation of elements of $x = (x_0 \ldots, x_{m-1})$ with the derangement $\mathbf{\Delta}_m$ as $\mathbf{\Delta}_m(x) = \mathbf{\Delta}_m(x_0 \ldots, x_{m-1}) = (x_{\delta(0)}, \ldots x_{\delta(m-1)})$.

Definition 3 *A one round generalized Feistel transformation $\mathcal{F}_{m,l} : \mathbb{E}^m \to \mathbb{E}^m$ of an element $x \in \mathbb{E}^m$ with the respect of a leader l is defined as:*

$$\mathcal{F}_{m,l}(x) := \Delta_m(\mathcal{D}_l(x)), \tag{6}$$

and a Rounds generalized Feistel transformation $\mathcal{F}_m^{(Rounds)} : \mathbb{E}^m \to \mathbb{E}^m$ with the respect of a list of leaders $L = \{l_1, l_2, \ldots, l_{Rounds}\}$ is defined as:

$$\mathcal{F}_{m,L}^{(Rounds)}(x) := \mathcal{F}_{m,l_{Rounds}}(x) \circ \ldots \circ \mathcal{F}_{m,l_1}(x). \tag{7}$$

Definition 4 *Let $m \geqslant 2$, $Rounds \geqslant 1$, and let $x, y \in \mathbb{E}^m$. The operation $* := *_{m,Rounds}$ is defined as:*

$$x * y = \Pi\Big(y, \mathcal{F}_{m,L}^{(Rounds)}\big(\Pi(x, y)\big)\Big). \tag{8}$$

Proposition 1 *Operation $*$ is entropic operation i.e. $\forall x, y, z, w \in \mathbb{E}^m$,*

$$(x * y) * (z * w) = (x * z) * (y * w).$$

We can easily check that this multidimensional entropic operation $*$ does not have the properties that were crucial for easily finding the automorphism σ, the abelian operation $\cdot$, the linear isomorphism ι and its inverse ι^{-1} in [7]. Even for the smallest dimension beyond 1, i.e. for the dimension $m = 2$, the degree of the multivariate polynomials grows with the pace of the Fibonacci sequence (thus exponentially with the number of Rounds).

Proposition 2 *For $m = 2$, the minimal degree of the multivariate polynomial describing the operation $*$, internally having Rounds Feistel rounds, is $a(Rounds + 3)$; the maximal degree is $a(Rounds + 4)$, where*

$$a(n) = 2\ Fibonacci(n) + 1, \tag{9}$$

and where $Fibonacci(n)$ is the n-th Fibonacci number.

With higher dimensions, the degree of the multivariate polynomials that describe the operation $*$ grows even faster. So, having analytical expressions that could help finding the commuting automorphisms σ, τ of $(G, \cdot)$ as well as the commutative group operation $\cdot$ becomes infeasible even with $m = 2$ and with number of rounds $Rounds \geqslant 16$.

Another observation is that for the dimension $m = 2$ and even with the the smallest number of rounds $Rounds = 1$, it is easy to prove (it is just a simple polynomial algebra) that there are neither left nor right unit elements in $\mathbb{E}^2$.

Proposition 3 *For $m = 2$ and Rounds $= 1$, there are leader values l, such that operation $* := *_{m,Rounds} := *_{2,1}$ has neither left nor right unit elements, i.e., there is no element $e \in \mathbb{E}^2$ such that $\forall x \in \mathbb{E}^2$ it holds that $e * x = x$, or it holds that $x * e = x$.*

Once having the operation $* := *_m$, all the principles for raising to the non-associative and non-commutative powers described in our original paper "Entropoid Based Cryptography" still hold.

We want to emphasize here that Definition 4 and equation (8) can be used with any entropic operation $*_1$, not necessarily only the defined operation in equation (3). The following example illustrates that.

Example 1. Let us use one tiny entropic quasigroup operation $*_1$ of size 4×4.

$*_1$	0	1	2	3
0	1	3	0	2
1	0	1	2	3
2	3	2	1	0
3	2	0	3	1

(10)

If we take $m = 2$ and the list of leaders to be $L = \{2, 3, 1, 1, 0, 1, 0, 0\}$, then the operation $*$ obtained by the equation (8) is described by the following Cayley 16×16 table:

$*$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	9	13	1	5	0	8	4	12	15	7	11	3	6	2	14	10
1	0	8	4	12	6	2	14	10	9	13	1	5	15	7	11	3
2	15	7	11	3	9	13	1	5	6	2	14	10	0	8	4	12
3	6	2	14	10	15	7	11	3	0	8	4	12	9	13	1	5
4	7	3	15	11	13	5	9	1	2	10	6	14	8	12	0	4
5	13	5	9	1	8	12	0	4	7	3	15	11	2	10	6	14
6	2	10	6	14	7	3	15	11	8	12	0	4	13	5	9	1
7	8	12	0	4	2	10	6	14	13	5	9	1	7	3	15	11
8	4	0	12	8	14	6	10	2	1	9	5	13	11	15	3	7
9	14	6	10	2	11	15	3	7	4	0	12	8	1	9	5	13
10	1	9	5	13	4	0	12	8	11	15	3	7	14	6	10	2
11	11	15	3	7	1	9	5	13	14	6	10	2	4	0	12	8
12	10	14	2	6	3	11	7	15	12	4	8	0	5	1	13	9
13	3	11	7	15	5	1	13	9	10	14	2	6	12	4	8	0
14	12	4	8	0	10	14	2	6	5	1	13	9	3	11	7	15
15	5	1	13	9	12	4	8	0	3	11	7	15	10	14	2	6

(11)

Apparently, the operation $*$ in (11) is a quasigroup (the Cayley 16×16 table is a Latin Square). It is also an entropic quasigroup.

However, if we put one more leader element i.e. if we set the list of leaders to be $L = \{2, 3, 1, 1, 0, 1, 0, 0, 1\}$, then Cayley 16×16 table is the following:

$*$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	13	13	2	1	14	14	1	1	14	14	1	2	13	13	2
1	12	3	3	12	15	0	0	15	15	0	0	15	12	3	3	12
2	15	0	0	15	12	3	3	12	12	3	3	12	15	0	0	15
3	1	14	14	1	2	13	13	2	2	13	13	2	1	14	14	1
4	9	6	6	9	10	5	5	10	10	5	5	10	9	6	6	9
5	7	8	8	7	4	11	11	4	4	11	11	4	7	8	8	7
6	4	11	11	4	7	8	8	7	7	8	8	7	4	11	11	4
7	10	5	5	10	9	6	6	9	9	6	6	9	10	5	5	10
8	5	10	10	5	6	9	9	6	6	9	9	6	5	10	10	5
9	11	4	4	11	8	7	7	8	8	7	7	8	11	4	4	11
10	8	7	7	8	11	4	4	11	11	4	4	11	8	7	7	8
11	6	9	9	6	5	10	10	5	5	10	10	5	6	9	9	6
12	14	1	1	14	13	2	2	13	13	2	2	13	14	1	1	14
13	0	15	15	0	3	12	12	3	3	12	12	3	0	15	15	0
14	3	12	12	3	0	15	15	0	0	15	15	0	3	12	12	3
15	13	2	2	13	14	1	1	14	14	1	1	14	13	2	2	13

(12)

We see that now we do not have a 16×16 quasigroup, but a groupoid that is an entropic left quasigroup.

Let us now carefully analyze the existing techniques given in the works of Toyoda [9], Murdoch [4], and Bruck [1] for constructing the Abelian group $(G, \cdot)$ with its commuting automorphisms σ, τ.

A common assumption in the works of Toyoda, Bruck and Murdoch: A common assumption in the works of Toyoda, Bruck and Murdoch is that the underlying entropic algebraic structure $(G, *)$ is a quasigroup. Then, with different techniques commutative groups are constructed, by finding certain automorphisms and constants. As we showed so far, the constructed entropic operations $* = *_m$ are not necessarily quasigroup operations.

Toyoda's paper: In the paper of Toyoda, the entropic operation is given in the field of real numbers. More concretely, for the conditions of Theorem 1 in Toyoda's paper, the entropic operation $\cdot$ is constructed as a linear (affine) function of two variables x and y, i.e. $x \cdot y = \lambda x + \mu y + \nu$. In our initial ePrint paper "Entropoid Based Cryptography" we constructed initially just a little bit more complex quadratic functions for the entropic operation. Thus, it not hard to find the corresponding group operation following the steps described in Toyoda's paper. Namely, having a simple linear form, Toyoda constructs a new operation $+$ under which $(G, +)$ is an Abelian group. The operation $+$ is defined as $a \cdot b = a \cdot s + r \cdot b$. Furthermore, Theorem 1 obtains that the operation $\cdot$ in G can be expressed as $x \cdot y = Ax + By + c$ for some automorphisms A and B on G and for some fixed element $c \in G$.

There is no direct algorithmic approach for finding explicitly the Abelian group (and the accompanied automorphisms) for the newly constructed multidimensional entropic operation $* = *_m$, that now has an unknown analytic form of multivariate polynomials with degrees higher than few millions.

Toyoda's approach to find the corresponding Abelian group, followed in Theorem 2, relies on the existence of a unit element for the entropic operation, and the existence of such a unit element for the newly defined multidimensional variant of the operation $* := *_m$ is not guaranteed.

Bruck's paper (viewed as extension of Murdoch's work): In Section 10 of his work, Bruck shows with Lemma 13 how to construct an entropic quasigroups (which he calls Abelian quasigroups) with a unique right or left unit element which is isotopic to any given entropic quasigroup $(Q, \cdot)$. For constructing the isotope with the unique right unit element, first he fixes an element $g \in Q$, then he uses the inverse map R_g^{-1} of the right mapping R_g where $R_g(x) = x \cdot g$. Then an isotopic quasigroup $(Q, \circ)$ is constructed as $a \circ b = R_g^{-1}(a) \cdot b$. Now for the operation $\circ$ the element g is a unique right unit i.e. $a \circ g = a$. A similar technique is applied for obtaining an isotopic operation with a unique left unit with the use of the inverse L_g^{-1} of the left mapping where $L_g(x) = g \cdot x$.

Then, in Theorem 11 Bruck gives the construction of the Abelian group $(G, \circ)$ isomorphic to the isotopes of $(Q, \cdot)$ that poses unit elements. The group is $G \equiv Q(R_g^{-1}, L_f^{-1})$ i.e. where $a \circ b = R_g^{-1}(a) \cdot L_f^{-1}(b)$ for some fixed elements f and g in G. Finally, in Theorem 12 Bruck shows that every entropic quasigroup $(G, \cdot)$, that is isotopic to an Abelian group, is isomorphic to some other quasigroup $(G, \circ)$, where $a \circ b = f \cdot S(a) \cdot T(b)$ where $f \in G$ is a fixed element, and where S and T are commutative automorphisms of G.

Note that the construction of $(G, \circ)$ in Theorem 11 assumes the knowledge of two inverse mappings R_g^{-1} and L_f^{-1}. Note also that the isomorphism in Theorem 12 is between two quasigroups, and the construction of the automorphisms S and T of the group G assumes the knowledge of the inverse elements in G and the knowledge of two isomorphisms U and V for the isotopes with unit elements.

3 Conclusions

Being entropic operation $*$ that is not a quasigroup, without having explicit analytical expressions for it, without having a unit element for that operation, without the knowledge of the hidden corresponding Abelian group $(G, \cdot)$ (if existing at all), without the knowledge of its commuting automorphisms σ and τ and without the knowledge of the isomorphism ι and its inverse ι^{-1}, we can say that

Entropid Based Cryptography is cryptography with hidden sub-quasigroup and hidden sub-group exponentiation

As with the initial publication of the paper "Entropoid Based Cryptography", we accompany this rebuttal with proof-of-the-concept Jupyter notebook implementations in Sagemath 9.2 which can be taken from the following link: `http://people.item.ntnu.no/~danilog/EntropoidBasedCryptography/`.

For the key exchange the implementation uses a small but convenient prime number: the fourth Fermat prime number $F_4 = p = 2^{2^4} + 1$ and defines an operation $*_1$ defined over the entropoid $\mathbb{E}_p$. To reach the magma structures with $2^{256}, 2^{384}$ and 2^{512} elements, the dmensions defined by m should be $m = 8, 12, 16$. We use $Rounds = 14$ or $Rounds = 21$.

The signatures implementation are still with the big prime numbers and the proof-of-concept implementation is just to show that signing and verification work well with the newly defined multi-dimensional entropic operations.

Several open research questions are raising with this rebuttal:

- What is the size of the underlying entropic sub-quasigroup?
- How the number of rounds and the used derangement permutation are related in respect to the newly obtained groupoids? What are the guarantees that the structure is (is not) a quasigroup?
- What are the optimal practical parameters?

We hope that the implementation and this rebuttal will inspire further interest and further analysis of the strengths and weaknesses of the Entropoid Based Cryptography. We also plan soon to update the initial paper "Entropoid Based Cryptography" with the proposed multi-dimensional entropic operations.

Acknowledgements

I would like to thank Lorenz Panny for his kind emails and the discussions we had. I would also like to thank Daniel Nager and "Danny" Niu Jianfang for their email inputs and suggestions.

I would also like to thank Mattia Veroni for his numerous suggestions how to improve the quality of this text.

References

[1] Richard H Bruck. Some results in the theory of quasigroups. *Transactions of the American Mathematical Society*, 55:19–52, 1944.

[2] Danilo Gligoroski. Entropoid Based Cryptography. 2021. `https://eprint.iacr.org/2021/469`.

[3] Danilo Gligoroski, Hristina Mihajloska, Daniel Otte, and M El-Hadedy. GAGE and InGAGE V1. 03. *NIST lightweight competition round*, 1:114, 2019.

[4] DC Murdoch. Quasi-groups which satisfy certain generalized associative laws. *American Journal of Mathematics*, 61(2):509–522, 1939.

[5] Daniel Nager. Private email communications, May 2021.

[6] Daniel Nager and "Danny" Niu Jianfang. Xifrat - Compact Public-Key Cryptosystems based on Quasigroups. 2021. `https://eprint.iacr.org/2021/444`.

[7] Lorenz Panny. Entropoid-based cryptography is group exponentiation in disguise. 2021. `https://eprint.iacr.org/2021/583`.

[8] Lorenz Panny. Private email communications, May 2021.

[9] Kôshichi Toyoda. On Axioms of Linear Functions. *Proceedings of the Imperial Academy*, 17(7):221–227, 1941.