Improving Cryptography Based On Entropoids

Anisha Mukherjee[1] and Saibal K. Pal[2]

[1]University of Delhi, New Delhi
[2]DRDO & University of Delhi, New Delhi

November 11, 2021

Abstract

Entropic quasigroups or entropoids provide an attractive option for development of post-quantum cryptographic schemes. We elaborate on the mathematical properties of entropoids with modifications in the initial operation. The starting entropic quasigroups obtained by this process can be applied to generate higher-order structures suitable for cryptography. We also propose an encryption/decryption scheme analogous to the ElGamal scheme with quasigroup string transformations in the entropoid setting. We then move on to enumerate important properties that are beneficial in cryptographic use together with algorithms for their verification.

Introduction

It is a never-ending race to be one step ahead of adversaries in the pursuit of secure cryptographic algorithms and protocols. As quantum computing gains momentum, a number of cryptographic protocols relying on the mathematical concepts of number theory, group and field theory and Boolean algebra have become vulnerable to attacks. The focus is therefore shifting towards non-associative and non-commutative algebraic structures that may be able to withstand these attacks. In this paper, we discuss one such non-commutative and non-associative algebraic structure known as *entropic* groupoids [1] satisfying the *palintropic* property which is also a quasigroup. Quasigroups [15] have the ability to accommodate many cryptographically suitable properties (non-associativity, polynomial completeness to name a few) and especially, the number of possible quasigroups increases exponentially with an increase in their order, thus providing ample options to a cryptographer to choose the suitable ones for a particular cryptographic scheme. Quasigroup operations [17] are also useful in defining easy, fast and secure cryptographic functions.
First, we introduce the readers to the concept of entropoids and then describe a succint notation for exponentially large non-associative power indices as proposed by Gligoroski [1]. This is particularly interesting because it aids swift exponentiation and mimics the usual *'Logarithmetic'* (arithmetic of power indices) rules. We also give a list of a few cryptographic algorithms that can be formulated using this knowledge. Next, we mention Panny's work [2] on formulating a possible attack on the structure of entropoids by means of a hidden group structure contained in it. We also elaborate on the modifications introduced by Gligoroski [7] in order to refute the claims in [2]. In addition, we enumerate important properties that are desired in the newly generated entropic quasigroups to make them suitable for cryptographic implementations.

Our contribution: Section I provides definitions and concepts of entropic quasigroups along with their construction. In Section II, the process of power index computation is explained with the help of an example. Sections III and IV elaborate on the computational hard problems and cryptographic schemes based on entrapoid. The scheme analogous to the ElGamal cryptosystem and based on quasigroup string transformations in the entropoid setting is also presented in Section IV. Section V highlights the attacks published in literature. Modifications proposed in the initial structure of entropoids are highlighted in Section VI. Dealing with modifications in the initial operation, starting entropic quasigroups are presented that can be applied to generate higher order structures suitable for cryptography. Important properties that are beneficial in cryptographic use along with algorithms for their verification are also enumerated in this Section. The theory is supported by simple worked-out examples for the sake of clarity. All notations are consistent with those of the referred literature.

I. Some definitions and concepts

1. **Entropic binary operation:**A binary operation $'*'$ of the groupoid $(G, *)$ is called *entropic* if for every four elements x, y, z, w of G, the following condition holds true:

$$\text{If} \quad x * y = z * w \quad \Rightarrow \quad x * z = y * w \tag{1a}$$

Parallely, many authors also describe it as the *medial* or *restricted-commutativity*[16] identity and express it as follows:

$$(x * y) * (z * w) = (x * z) * (y * w) \tag{1b}$$

Quasigroup: A quasigroup $(Q, *)$ is a set with binary operation '$*$' : $Q^2 \to Q$, satisfying the law, for all $u, v \in$ Q, there exists unique $x, y \in$ Q such that

$$u * x = v \quad \text{and} \quad y * u = v \tag{1c}$$

To each quasigroup of finite order given by its multiplication table, one can associate a *Latin square*, *L*. A Latin Square on a finite set Q of cardinality n is an $n \times n$ matrix with elements from Q such that each row and each column is actually a permutation of Q.

Isotopy in quasigroups: Two quasigroups $(K, *)$ and $(Q, \bullet)$ are said to be isotopic if there exists bijections α, β, γ from K to Q such that

$$\gamma\,(x * y) = \alpha(x) \bullet \beta(y) \tag{1d}$$

for each $x, y \in$ K.
The triple (α, β, γ) is called an isotopism from $(K, *)$ to $(Q, \bullet)$
Given a quasigroup $(Q, *)$ five new operations (called parastrophes) denoted by $\backslash, /, \bullet, \backslash\backslash, //$ can be derived from $*$.
We can define the operations according to the relations,

$$x * y = z \Leftrightarrow y = x \setminus z \Leftrightarrow x = z/y \Leftrightarrow y \bullet x = z \Leftrightarrow y = z \setminus \backslash x \Leftrightarrow x = y//z \tag{1e}$$

Thus $(Q, \backslash)$, (Q, /), $(Q, \bullet)$,$(Q, \backslash\backslash)$, (Q, //) are quasigroups too.

Quasigroup $e-$ and $d-$ type string transformations: We give here a type of string transformation [17] that we will make use of in a later section. Consider a finite set (called the alphabet) Q, and denote by $Q^+ = \{a_1, a_2, \cdots, a_n | a_i \in Q\}$ to be the set of all finite strings formed by the elements of Q. Let us also consider a quasigroup $(Q, *)$. For each $a \in Q$ we define two functions $e_{a,*}$, $d_{a,*} : Q^+ \to Q^+$ as:
Let $a_i \in Q$, $\alpha = a_1 a_2 \cdots a_n$. Then,

$$e_{a,*}(\alpha) = b_1 b_2 \cdots b_n \Leftrightarrow b_1 = a * a_1,\, b_2 = b_1 * a_2, \cdots, b_n = b_{n-1} * a_n \tag{1f}$$

$$d_{a,*}(\alpha) = c_1 c_2 \cdots c_n \Leftrightarrow c_1 = a * a_1, c_2 = a_1 * a_2, \cdots, c_n = a_{n-1} * a_n \tag{1g}$$

.
These functions $e_{a,*}, d_{a,*}$ are called e- and d-transformation of Q^+ with respect to the quasigroup operation $*$ and a is called the leader.
As a generalisation, we may define more than one quasigroup operation, say, a sequence of opearations $*_1, *_2, \cdots, *_k$ such that for a sequence of leaders $a_1, a_2, \cdots, a_k$ in Q, the composition maps E_k, D_k and T_k are the given by,

$$E_k = E_{a_1 \cdots a_k} = e_{a_1} \circ e_{a_2} \circ \cdots \circ e_{a_k} \tag{1h}$$
$$D_k = D_{a_1 \cdots a_k} = d_{a_1} \circ d_{a_2} \circ \cdots \circ d_{a_k} \tag{1i}$$
$$T_k = T_{a_1 \cdots a_k} = t_{a_1} \circ t_{a_2} \circ \cdots \circ t_{a_k} \tag{1j}$$

where t_{a_i} is either an e- or a d-transformation determined according to some rule specific to a cryptographic primitive. We must also note here that e_{a_i} is actually $e_{a_{i*_1}}$.
The transformations E_k, D_k and T_k are clearly transformations on Q^+ and any E_k or D_k is essentially a T_k transformation.
Next we mention here an important theorem from [17] as a fact:

For a finite quasigroup, $(Q, *, \backslash, /)$, each string α in the alphabet Q^+ and each leader l in Q, the $e_{l,*}$ and $d_{l,\backslash}$ transformations turn out to be inverse transformation of each other. In other words,

$$d_{l,\backslash}(e_{l,*}(\alpha)) = \alpha = e_{l,*}(d_{l,\backslash}(\alpha)). \tag{1k}$$

2. **Bracketing shapes:** When a binary operation is associative, the number or combination of brackets in an expression involving the operation has no effect on its evaluation. However, in algebraic structures where the property of associativity is not inherent, the placement of brackets in the expression is crucial, and may give different results.
Let us consider an element x of the groupoid $(G, *)$ (recall that the binary operation in a groupoid is not assumed to have any additional properties) and let $a \in \mathbb{N}$. A *bracketing shape/pattern* for multiplying x by itself, $'a'$ times is denoted by a_s i.e.,

$$a_s : \underbrace{(x * \cdots (x * x) \cdots)}_{'a' \text{ copies of } x} \tag{2}$$

We call the pair, $\mathbf{A} = (a, a_s)$ a *power index.* Writing $x^{\mathbf{A}}$ will refer to the expression (2) for some bracketing shape a_s.

2.1 The set of all possible bracketing shapes a_s of an element x multiplied a times with itself is given by,

$$S_a(x) = \{a_s \mid a_s \text{ is a bracketing shape with } a \text{ instances of an element } x\}. \tag{3}$$

2.2 Let $\mathbf{A} = (a, a_s)$ be a bracketing shape. The cardinality of the set S_a has the following expression in terms of the $(a-1)$*th Catalan number*, C_{a-1},

$$|S_a(x)| = C_{a-1} = \frac{1}{a}\binom{2a-2}{a-1} \tag{4}$$

Two members of the set S_a of bracketing shapes are intuitive or *primary*: they can be visualised with an iterative process strarting with $x * x$ and sequentially absorbing the rest of the factors x at a time either from left to right or from right to left.

2.3 The *left-to-right* bracketing shape of $'a'$ instances of an element x with power index, $\mathbf{A} = (a, a_s)$ is given by,

$$a_s : \underbrace{((\cdots((x{*}x) * x) \cdots){*}x)}_{a \text{ copies of } x} \tag{5}$$

In compact from, it is denoted by, $\mathbf{A} \equiv x_{(a-1,x)to-right}$ (starting with x and following a sequnce of $a-1$ right multiplications by x).
For a generic bracketing shape s the notation used is, $s_{(k,x)to-right}$ and it denotes a sequential extension of s by k right multiplications by x. Thus, $s \equiv s_{(0,x)to-right}$ would mean the shape s itself extended with zero right multiplications by x.
Similarly, the *right-to-left* bracketing shape of a power index, $\mathbf{A} = (a, a_s)$ is given by,

$$a_s : \underbrace{(x{*}(\cdots(x * (x * x) \cdots))}_{a \text{ copies of } x} \tag{6}$$

In compact from, it is denoted by, $\mathbf{A} \equiv x_{(x,a-1)to-left}$.
With a generic bracketing shape s we use the short notation $s_{(x,k)to-left}$ to denote a sequential extension of s by k left multiplications by x and the notation $s \equiv s_{(x,0)to-right}$ means the shape s itself extended with zero left multiplications by x.

2.4 *The sum and product of power indices:* Since ia a groupoid operation $*$ in $(G, *)$ is a (closed) binary operation, therefore every power index $\mathbf{A} = (a, a_s)$ may be considered as an endomorphism on G,

$$\mathbf{A} : x \rightarrow x^{\mathbf{A}}. \tag{7}$$

Let us consider two power indices, $\mathbf{A} = (a, a_s)$ and $\mathbf{B} = (b, b_s)$, then their *sum*, $\mathbf{A} + \mathbf{B}$ is defined as the power index of the product of two powers,

$$x^{\mathbf{A}+\mathbf{B}} = x^{\mathbf{A}} * x^{\mathbf{B}} \tag{8}$$

and, their *product*, $\mathbf{A} \times \mathbf{B}$ (or simply $\mathbf{AB}$) is defined as the power index of an expression obtained by replacing every factor in the expression of the shape b_s by a complete shape a_s,

$$x^{\mathbf{AB}} = (x^{\mathbf{A}})^{\mathbf{B}} \tag{9}$$

Take for example, $\mathbf{A} \equiv x_{(x,a-1)to-left}$ and $\mathbf{B} \equiv x_{(b-1,x)to-right}$, then, $(x^{\mathbf{A}})^{\mathbf{B}}$ is just,

$$\underbrace{((\cdots((x_{(x,a-1)to-left}*x_{(x,a-1)to-left}) * x_{(x,a-1)to-left})\cdots)*x_{(x,a-1)to-left})}_{b \text{ copies of } x_{(x,a-1)to-left}}$$

which would in turn mean,

$$((\cdots((\overbrace{(x*(\cdots(x*(x*x)\cdots))}^{a \text{ copies of } x})*\overbrace{(x*(\cdots(x*(x*x)\cdots)))}^{a \text{ copies of } x}) * \overbrace{(x*(\cdots(x*(x*x)\cdots)))}^{a \text{ copies of } x})\cdots)*$$
$$\overbrace{(x*(\cdots(x*(x*x)\cdots)))}^{a \text{ copies of } x}$$

2.5 Two power indices, $\mathbf{A} = (a, a_s)$ and $\mathbf{B} = (b, b_s)$ are *equal* iff $x^{\mathbf{A}} = x^{\mathbf{B}}$ for all $x \in (G, *)$.
The *Logarithmetic*, $(L(G), +, \times)$ is the algebra over the equated indices from 2.5 with operations $+$ and $\times$ as defined in 2.4.

2.6 *Palintropic groupoids:* If $x^{\mathbf{AB}} = x^{\mathbf{BA}}$ for all $x \in G$ and for all power indices $\mathbf{A}$ and $\mathbf{B}$, then the groupoid $(G, *)$ is called *palintropic*.

2.7 *(Theorem 2, [1])* If the groupoid $(G, *)$ is entropic, then for every $x, y \in G$

$$(x * y)^{\mathbf{A}} = x^{\mathbf{A}} * y^{\mathbf{A}} \tag{10}$$

and,

$$x^{\mathbf{AB}} = (x^{\mathbf{A}})^{\mathbf{B}} = (x^{\mathbf{B}})^{\mathbf{A}} \tag{11}$$

Since the operation $*$ is entropic, the corresponding operands of every factor $(x * y)$ in the expression of $(x * y)^{\mathbf{A}}$ can be clubbed together, that is, the $x's$ are multiplied with themselves and so are the $y's$ according to the power index $\mathbf{A}$ and this gives us the expression on the RHS of (10).

2.8 *Generator:* $g \in G$ is a generator of the groupoid $(G, *)$ if for all $x \in G$, there exists a power index $\mathbf{A}$, such that

$$x = g^{\mathbf{A}} \tag{12}$$

We may write G in terms of its generator g as, $G = \langle g \rangle$.

The notation $(\mathbb{F}_p)^L$: Let us denote by $(\mathbb{F}_p)^L$ the direct product G of L, $(L \geq 2)$ copies of a finite field $\mathbb{F}_p$, i.e.,

$$G = \underbrace{\mathbb{F} \times \cdots \times \mathbb{F}}_{L \text{ times}}, \quad G = (\mathbb{F}_p)^L, \quad L \geq 2$$

3. **Criteria for constructing entropic groupoids over $(\mathbb{F}_p)^L$:**
Let the elements $x, y, z, w \in G = (\mathbb{F}_p)^L$ be represented by the tuples $x = (x_1, \cdots, x_L)$, $y = (y_1, \cdots, y_L)$, $z = (z_1, \cdots, z_L)$ and $w = (w_1, \cdots w_L)$.

3.1 The binary operation $*$ over G should be, **(i)** ***entropic*** as per definition (1), **(ii)** ***non-linear*** with repsect to the operations of addition and multiplication of the finite field $\mathbb{F}_p$, **(iii)** ***non-commutative*** and **(iv)** ***non-associative***.
As suggested in (Gligoroski), defining an operation $*$ for $L = 2$ with the help of general quadratic $2L$-variate polynomials and choosing suitable coefficients from $\mathbb{F}_p$ such that all the conditions (i)-(iv) are met could be one possible way. However, in their most general form, these $2L$-variate polynomials would possess almost 30 coefficients and determining feasible relations among them will become herculean.
A simplified form of defining $*$ for $L = 2$ is given as follows:

$$\begin{aligned} x * y = (x_1, x_2) * (y_1, y_2) &= (P_1(x_1, x_2, y_1, y_2), P_2(x_1, x_2, y_1, y_2)) \\ P_1(x_1, x_2, y_1, y_2) &= a_1 + a_2x_1 + a_3x_2 + a_4y_1 + a_6x_1y_1 + a_8x_2y_1 \\ P_2(x_1, x_2, y_1, y_2) &= b_1 + b_2x_1 + b_3x_2 + b_5y_2 + b_7x_1y_2 + b_9x_2y_2 \end{aligned} \tag{13}$$

where, P_1 and P_2 are $2L$-variate polynomials with some monomial terms removed so as to make the definition of $*$ simpler.

3.2 The following can be viewed as a solution of the system (13):

$$\begin{aligned} (x_1, x_2) * (y_1, y_2) = \Big(&\frac{a_3(a_8b_2 - b_7)}{a_8b_7} + a_3x_2 + \frac{a_8b_2}{b_7}y_1 + a_8x_2y_1, \\ &\frac{-b_2(a_8 - a_3b_7)}{a_8b_7} + \frac{a_3b_7}{a_8}y_2 + b_2x_1 + b_7x_1y_2 \Big) \end{aligned} \tag{14}$$

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

3.3 *A few observations for a groupoid $(G, *)$ with the operation $*$ as defined in (14) :*

- (14) satisfies all the design criteria from (i)-(iv). It is clearly non-linear, non-commutative and non-associative. A closer inspection and some replacements, we can verify that the operation is entropic too.

- Let us take into account the additive inverses of the constants a_3, a_8, b_2 and b_7, that is, since for observational purposes we have considered the operations in the underlying field $\mathbb{F}_p^*$ to be modulo n, so we may write the additive inverses as $p - k$ where $k = \{a_3, a_8, b_2, b_7\}$. Using their inverses in (14) in place of the constants, the first coordinate of the equation takes the form,

$$\begin{aligned} &\frac{(p - a_3)((p - a_8)(p - b_2) - (p - b_7))}{(p - a_8)(p - b_7)} + (p - a_3)x_2 + \frac{(p - a_8)(p - b_2)}{(p - b_7)}y_1 + (p - a_8)x_2y_1 \\ &(p - a_3)[\frac{p^2 - pb_2 - pa_8b_2a_8 - p - b_7}{p^2 - pb_7 - ppa_8 + a_8b_7}] + px_2 - a_3x_2 + \\ &[\frac{p^2 - pb_2 - pa_8 + b_2a_8}{p - b_7}]y_1 + px_2y_1 - a_8x_2y_1 \end{aligned}$$

  Since all operations in the field are modulo n, so, further simplification will yield,

$$\begin{aligned}&\frac{(pb_2a_8 - p^2 - pb_7) - (a_3b_2a_8 + pa_3 + a_3b_7)}{a_8b_7} - a_3x_2 + \frac{b_2a_8}{(p-a_7)}y_1 - a_8x_2y_1\\ &= \frac{-a_3b_2a_8 + a_3b_7}{a_8b_7} - a_3x_2 + \frac{b_2a_8}{(p-b_7)}y_1 - a_8x_2y_1\\ &= \frac{-a_3(b_2a_8 - b_7)}{a_8b_7} - a_3x_2 - \frac{b_2a_8}{b_7}y_1 - a_8x_2y_1\end{aligned}$$

Similarly, for the second coordinate, we have the following expression,

$$\frac{-b_2(a_8 + a_3b_7)}{a_8b_7} - \frac{a_3b_7}{a_8}y_2 - b_2x_1 - b_7x_1y_2$$

So finally we have,

$$\begin{aligned}(x_1, x_2) * (y_1, y_2) = \Big(&\frac{-a_3(a_8b_2 - b_7)}{a_8b_7} - a_3x_2 - \frac{a_8b_2}{b_7}y_1 - a_8x_2y_1,\\ &\frac{-b_2(a_8 + a_3b_7)}{a_8b_7} - \frac{a_3b_7}{a_8}y_2 - b_2x_1 - b_7x_1y_2\Big)\end{aligned}$$

This expression is very similar to (14) and satisfies the design criteria (i)-(iv) just like it. Hence we can say that whenever (14) is a solution of the system (13), the expression obtained by replacing the constants with their respective additive inverses is also a solution of (13).

- Let us consider the element, $\left(\frac{-a_3}{a_8}, \frac{-b_2}{b_7}\right)$ and let $x = (x_1, x_2)$ be an arbitrary element of G. Using (14),

$$\begin{aligned}(x_1, x_2) * \Big(\frac{-a_3}{a_8}, \frac{-b_2}{b_7}\Big) &= \left(\frac{a_3(a_8b_2 - b_7)}{a_8b_7} + a_3x_2 + \frac{a_8b_2}{b_7}\Big(\frac{-a_3}{a_8}\Big) + a_8\Big(\frac{-a_3}{a_8}\Big)x_2,\right.\\ &\qquad \left.\frac{-b_2(a_8 - a_3b_7)}{a_8b_7} + \frac{a_3b_7}{a_8}\Big(\frac{-b_2}{b_7}\Big) + b_2x_1 + b_7\Big(\frac{-b_2}{b_7}\Big)x_1\right)\\ &= \left(\frac{a_3b_2}{b_7} - \frac{a_3}{a_8} + \Big(\frac{-a_3b_2}{b_7}\Big), \frac{-b_2}{b_7} + \frac{b_2a_3}{a_8} + \Big(\frac{-a_3b_2}{a_8}\Big)\right)\\ &= \Big(\frac{-a_3}{a_8}, \frac{-b_2}{b_7}\Big)\end{aligned}$$

Similarly, $\left(\frac{-a_3}{a_8}, \frac{-b_2}{b_7}\right) * (x_1, x_2) = \left(\frac{-a_3}{a_8}, \frac{-b_2}{b_7}\right)$.
Hence, the element, $\left(\frac{-a_3}{a_8}, \frac{-b_2}{b_7}\right)$ is the *multiplicative zero* of the groupoid, $(G, *)$ and we denote it by, $\mathbf{0}_* = \left(\frac{-a_3}{a_8}, \frac{-b_2}{b_7}\right)$.

$$x * \mathbf{0}_* = \mathbf{0}_* * x = \mathbf{0}_* \quad \forall x \in G. \tag{15}$$

- Next, consider the element, $\left(\frac{1}{b_7} - \frac{a_3}{a_8}, \frac{1}{a_8} - \frac{b_2}{b_7}\right)$ and an arbitrary element $x = (x_1, x_2)$ of G. Using (14),

$$\begin{aligned}\Big(\frac{1}{b_7} - \frac{a_3}{a_8}, \frac{1}{a_8} - \frac{b_2}{b_7}\Big) * (x_1, x_2) &= \left(\frac{a_3(a_8b_2 - b_7)}{a_8b_7} + a_3\Big(\frac{1}{a_8} - \frac{-b_2}{b_7}\Big) + \frac{a_8b_2}{b_7}x_1 + a_8\Big(\frac{1}{a_8} - \frac{b_2}{b_7}\Big)x_1,\right.\\ &\qquad \left.\frac{-b_2(a_8 - a_3b_7)}{a_8b_7} + \frac{a_3b_7}{a_8}x_2 + b_2\Big(\frac{1}{b_7} - \frac{-a_3}{a_8}\Big) + b_7\Big(\frac{1}{b_7} - \frac{-a_3}{a_8}\Big)x_2\right)\\ &= \left(\frac{a_8b_2}{b_7}x_1 + x_1 - \frac{a_8b_2}{b_7}x_1, \frac{a_3b_7}{a_8}x_2 + x_2 - \frac{a_3b_7}{a_8}x_2\right)\\ &= (x_1, x_2) = x\end{aligned}$$

Hence, $\mathbf{1}_* = \left(\frac{1}{b_7} - \frac{a_3}{a_8}, \frac{1}{a_8} - \frac{b_2}{b_7}\right)$ is called the *multiplicative left unit* of the groupoid $(G, *)$ and,

$$\mathbf{1}_* * x = x \quad \forall x \in G. \tag{16}$$

There are $(p-1)$ distinct square roots of the left unity $\mathbf{1}_*$,

$$\mathbb{S}(p) = \{x \mid x * x = \mathbf{1}_*\} \quad \text{and} \quad |\mathbb{S}(p)| = p - 1 \tag{17}$$

- For every $x = (x_1, x_2) \neq (0, 0)$ in G, its *inverse multiplicative element*, x_*^{-1} with repect to the left unit $\mathbf{1}_*$ is given by,

$$x_*^{-1} = \Big(\frac{1 - a_3b_2 - a_3b_7x_2}{a_8(b_2 + b_7x_2)}, \frac{1 - a_3b_2 - a_8b_2x_1}{b_7(a_3 + a_8x_1)}\Big) \tag{18}$$

for which,

$$x * x_*^{-1} = x_*^{-1} * x = \mathbf{1}_*. \tag{19}$$

3.4 *Operations in* $(\mathbb{F}_p)^L$ *when* $L = 2$*, that is, for* $G = \mathbb{F}_p \times \mathbb{F}_p$ *:*
Let $x = (x_1, x_2), y = (y_1, y_2)$ be two elements of the set $G = \mathbb{F}_p \times \mathbb{F}_p$. The *additive operation*, $\boxplus$, i.e., $x \boxplus y$ is defined as:

$$(x_1, x_2) \boxplus (y_1, y_2) = \Big(x_1 + y_1 + \frac{a_3}{a_8}, x_2 + y_2 + \frac{b_2}{b_7}\Big) \tag{20}$$

where $a_3, a_8, b_2, b_7 \in \mathbb{F}_p$, are defined as in (14).
Let $\boxminus$ denote the corresponding *inverse* of the additive operation $\boxplus$. Then it can be defined as,

$$(x_1, x_2) \boxminus (y_1, y_2) = \Big(x_1 - y_1 - \frac{a_3}{a_8}, x_2 - y_2 - \frac{b_2}{b_7}\Big). \tag{21}$$

We may use $\boxminus$ as a unary operation and the notation $\boxminus x$ would then mean,

$$\boxminus x = \mathbf{0}_* \boxminus x = \Big(-\frac{a_3}{a_8} - x_1, -\frac{b_2}{b_7} - x_2\Big). \tag{22}$$

3.5 The algebraic structure $(G, \boxplus, *)$ thus obtained as a result of 3.3 and (20) is a *ringoid* where $(G, \boxplus)$ is an Abelian group with a neutral element $\mathbf{0}_*$, $(G, *)$ is a non-commutative and non-associative groupoid with a zero element $\mathbf{0}_*$, a left unit element $\mathbf{1}_*$ and $*$ is distributive over $\boxplus$ i.e.,

$$x * (y \boxplus z) = (x * y) \boxplus (x * z) \quad \text{and} \quad (x \boxplus y) * z = (x * z) \boxplus (y * z). \tag{23}$$

3.6 The ringoid $(G, \boxplus, *)$ is denoted by $\mathbb{E}_{p^2}$ and is called the ***Finite Entropic ring*** or ***Finite Entropoid***. Clearly it has p^2 elements.
For given values of p, a_3, a_8, b_2 and b_7, $a_3 \neq 0$, $b_2 \neq 0$ it will be denoted as $\mathbb{E}_{p^2}(a_3, a_8, b_2, b_7)$ or just by $\mathbb{E}_{p^2}$ if the specification of the consants is not important.

4. **Maximal multiplicative subgroupoid, $\mathbb{E}^*_{(p-1)^2}$:**
The subset $\mathbb{E}^*_{(p-1)^2}$ of $\mathbb{E}^*_{p^2}$ is defined as,

$$\mathbb{E}^*_{(p-1)^2} = \left(\Big(\mathbb{F}_p \setminus \Big\{-\frac{a_3}{a_8}\Big\}\Big) \times \Big(\mathbb{F}_p \setminus \Big\{-\frac{b_2}{b_7}\Big\}\Big)\right) \tag{24}$$

The groupoid $\mathbb{E}^*_{(p-1)^2}$ is called the ***maximal multiplicative subgroupoid*** of $\mathbb{E}_{p^2}$.

4.1 $\mathbb{E}^*_{(p-1)^2}$ has $(p-1)^2$ elements of the form (x_1, x_2) where, clearly from the sets of definition of the subgroupoid, x_1 cannot be the first component and x_2 cannot be the second component of the multiplicative zero $\mathbf{0}_*$. Based on (14), we can say that $(\mathbb{E}^*_{(p-1)^2}, *)$ is non-commutative and non-associative and has a left unit element, $\mathbf{1}_*$.
Now, for every $c = (c_1, c_2)$ and every $d = (d_1, d_2)$, the equations, $x * c = d$ and $c * x = d$ my be written using (14) as,

$$\begin{aligned} c * x = (c_1, c_2) * (x_1, x_2) = \Big(&\frac{a_3(a_8b_2 - b_7)}{a_8b_7} + a_3c_2 + \frac{a_8b_2}{b_7}x_1 + a_8c_2x_1, \\ &\frac{-b_2(a_8 - a_3b_7)}{a_8b_7} + \frac{a_3b_7}{a_8}x_2 + b_2c_1 + b_7c_1x_2\Big) \\ &= (d_1, d_2) \end{aligned}$$

Comparing components,

$$\begin{aligned} \frac{a_3(a_8b_2 - b_7)}{a_8b_7} + a_3c_2 + \frac{a_8b_2}{b_7}x_1 + a_8c_2x_1 = d_1 \\ \frac{-b_2(a_8 - a_3b_7)}{a_8b_7} + \frac{a_3b_7}{a_8}x_2 + b_2c_1 + b_7c_1x_2 = d_2 \end{aligned}$$

and,

$$\begin{aligned} x * c = (x_1, x_2) * (c_1, c_2) = \Big(&\frac{a_3(a_8b_2 - b_7)}{a_8b_7} + a_3x_2 + \frac{a_8b_2}{b_7}c_1 + a_8x_2c_1, \\ &\frac{-b_2(a_8 - a_3b_7)}{a_8b_7} + \frac{a_3b_7}{a_8}x_2 + b_2c_1 + b_7c_1x_2\Big) \\ &= (d_1, d_2) \end{aligned}$$

Comparing components,

$$\begin{aligned} \frac{a_3(a_8b_2 - b_7)}{a_8b_7} + a_3x_2 + \frac{a_8b_2}{b_7}c_1 + a_8x_2c_1 = d_1 \\ \frac{-b_2(a_8 - a_3b_7)}{a_8b_7} + \frac{a_3b_7}{a_8}x_2 + b_2c_1 + b_7c_1x_2 = d_2 \end{aligned}$$

A bit further simplification will yield,

$$\begin{aligned} \Big(\frac{a_8b_2}{b_7} + a_8c_2\Big)x_1 - (a_3 + a_8c_1)x_2 = \Big(\frac{a_8b_2}{b_7}c_1 - a_3c_2\Big) \\ \Big(\frac{a_3b_7}{a_8} + b_7c_1\Big)x_2 - (b_2 + b_7c_2)x_1 = \Big(\frac{a_3b_7}{a_8}c_2 - b_2c_1\Big) \end{aligned}$$

So, we have two equations in order to solve two variables x_1 and x_2. This implies that we will get a unique solution $x = (x_1, x_2)$ and therefore, the equations,

$$x * c = d \quad \text{and} \quad c * x = d \tag{25}$$

will always have solutions.
This precisely proves that $(\mathbb{E}^*_{(p-1)^2}, *)$ is a ***quasigroup***. It is entropic.

4.2 *Subquasigroups of* $(\mathbb{E}^*_{(p-1)^2}, *)$:
Let $(\mathbb{E}^*_\nu, *)$ denote a *subquasigroup* of $(\mathbb{E}^*_{(p-1)^2}, *)$ such that $|\mathbb{E}^*_\nu| = \nu$. All subquasigroups of the quasigroup

$(\mathbb{E}^*_{(p-1)^2}, *)$ are entropic and, the order of the subquasigroups divides the order of the quasigroup, that is, $\nu | (p-1)^2$.
Let $\mathbb{F}_p$ be the finite field over which an entropoid $\mathbb{E}_{p^2}$ is defined. Let $\Gamma \subseteq \mathbb{F}^*_p$ be a cyclic subgroup of order $|\Gamma|$ of the multiplicative group $\mathbb{F}^*_p$ and let $\gamma \neq -\frac{a_3}{a_8}$ and $\gamma \neq -\frac{b_2}{b_7}$ is its generator, then $g = (\gamma, \gamma)$ is a generator of a subgroupoid $(\mathbb{E}^*_\nu, *)$ and ν divides $|\Gamma|^2$.

4.3 *Sylow q_i-subquasigroups* : Let $(\mathbb{E}^*_{(p-1)^2}, *)$ be an entropic quasigroup such that $(p-1)^2$ be represented as product of the powers of its prime factors i.e., $(p-1)^2 = 2^{e_1} q_2^{e_2} \cdots q_k^{e_k}$. Then, the subquasigroup $(\mathbb{E}^*_\nu, *)$ is called a *Sylow q_i-subquasigroup* if $\nu = q_i^{e_i}$ for $i \in \{2, \cdots, k\}$.

5. **The list of associative class representatives, $R_a(x)$:**
An ordered list $R_a(x)o$ of $a-1$, $2 \leq a$ bracketing shapes is called the list of associative class representatives. It is defined as,

$$R_a(x) = [R_a(x)[0], R_a(x)[1], \cdots, R_a(x)[a-3], R_a(x)[a-2]] \tag{26}$$

where,

$$\begin{aligned} R_a(x)[0] &= x_{(x,a-1)to-left}, \\ R_a(x)[1] &= (x_{(x,1)to-left} * x)_{(x,a-3)to-left}, \\ R_a(x)[2] &= (x_{(x,2)to-left} * x)_{(x,a-4)to-left}, \\ &\cdots, \\ R_a(x)[a-3] &= (x_{(x,a-3)to-left} * x)_{(x,0)to-left}, \\ R_a(x)[a-2] &= (x_{(x,a-2)to-left} * x) \end{aligned} \tag{27}$$

Hence, any given $a \geq 2$, the $a-1$ bracketing shapes would be a member of any one of these classes.

5.1 For $a = 2$ the only class representative would be, $R_2(x) = [R_2(x)[0]] = (x * x)$.
For $a = 3$, $R_3(x) = [R_3(x)[0], R_3(x)[1]]$, where, according to (27),

$$\begin{aligned} R_3(x)[0] &= x_{(x,3-1)to-left} = (x * (x * x)) \\ R_3(x)[1] &= (x_{(x,3-2)to-left} * x) = ((x * x) * x) \end{aligned}$$

Now, we observe that, $(x*(x*x)) = (x*(R_2(x)[0])) = (x*R_2(x))$ and, $((x*x)*x) = ((R_2(x)[0])*x)$. This means, for $a = 3$, we have, $R_3(x)[0] = (x * R_2(x)[0])$ and, $R_3(x)[1] = (R_2(x)[0] * x)$. This may intuitively point towards possible recurrent relations between the class representatives of a and $a+1$. Indeed, with the help of induction, we can prove that the following recurrent relations hold true:

$$\begin{aligned} R_{a+1}(x)[0] &= (x * R_a(x)[0]), \\ R_{a+1}(x)[1] &= (x * R_a(x)[1]), \\ R_{a+1}(x)[2] &= (x * R_a(x)[2]), \\ &\cdots, \\ R_{a+1}(x)[a-2] &= (x * R_a(x)[a-2]), \\ R_{a+1}(x)[a-1] &= (R_a(x)[0] * x) \end{aligned} \tag{28}$$

5.2 *Equivalent classes and their representatives*:
It was mentioned earlier in (4) that for a given a the set $S_a(x)$ of all bracketing shapes $\mathbb{A} = (a, a_s)$ has cardinality equal to the $(a-1)th$ Catalan number, C_{a1}. But for entropic groupoids $\mathbb{E}^*_{p^2}$ the size of the set $\{x^{\mathbb{A}}\}$ is actually limited to $a-1$. The corresponding sets of these $a-1$ types of bracketing shapes partition the set $S_a(g)$ into equivalent classes.
(Theorem 3, [1]) Let $\mathbb{E}_{p^2}$ be given, and let g be a generator of its maximal multiplicative subgroupoid $(\mathbb{E}^*_{(p-1)^2}, *)$, where $*$ is defined as in 3.1 and equation (14). For every $3 \leq a < b_{max}$, evaluating the bracketing shapes of the set $S_a(g)$ gives a partitioning in $a-1$ equivalent classes $S_{1,a(g)}, S_{2,a(g)}, \cdots, S_{a-2,a(g)}, S_{a-1,a(g)}$, whose corresponding representatives are given by the corresponding elements of $R_a(g)$ as defined in (27)

and the cardinality of the sets $S_{i,a(g)}$ for $i = 1, \cdots, a-1$ is given by the following expression:

$$\left|S_{i,a(g)}\right| = N(a-1, i) = \frac{1}{a-1}\binom{a-1}{i}\binom{a-1}{i-1} \tag{29}$$

where $N(a-1, i)$ are the Narayana numbers.
Definition of the integer b_{max}: Let $\mathbb{E}_{p^2}$ be a given finite entropoid. An integer b_{max} is defined as follows:

$$b_{max} = min\Big\{b \mid \frac{1}{b}\binom{2b-2}{b-1} > (p-1)^2\Big\} \tag{30}$$

The value b_max is the smallest integer for which the Catalan number $C_{b-1} = \frac{1}{b}\binom{2b-2}{b-1}$ exceeds the number of elements in the maximal multiplicative subgroupoid $(\mathbb{E}^*_{(p-1)^2}, *)$.

6. **Representing (exponentially) large bracketing shapes:**
In order to better distinguish between power indices in this context, we use $\mathfrak{b} \geq 2$ for smaller bracketing patterns. A power index $(\mathbf{A}, \mathfrak{b})$ may also be represented as, $(a, a_s, \mathfrak{b})$.

6.1 Let integer $b \geq 2$ be a base. The power index $(\mathbf{A}, \mathfrak{b}) = (a, a_s, \mathfrak{b})$ is defined as a triplet consisting of two lists and an integer $\mathfrak{b}$. Let $a \in \mathbb{Z}^+$ be represented in base $\mathfrak{b}$ as $a = A_0 + A_1\mathfrak{b} + \cdots + A_k\mathfrak{b}^k$, or in little-endian notation with the list of digits $0 \leq A_i \leq \mathfrak{b}-1$, as $a = [A_0, A_1, \cdots, A_k]_{\mathfrak{b}}$. Let the bracketing pattern a_s be represented with a list of digits $a_s = [P_0, P_1, \cdots, P_k]_{\mathfrak{b}-1}$ where $0 \leq P_i \leq \mathfrak{b}-2$ for $i = 0, \cdots, k$. For base $\mathfrak{b}$ and $a = [A_0, A_1, \cdots, A_k]_{\mathfrak{b}} \in \mathbb{Z}^+$ the set of all possible patterns is given by,

$$\mathbb{L}[a, \mathfrak{b}] = \{a_s \mid a_s = [P_0, \cdots, P_k]_{\mathfrak{b}-1}\}, \tag{31}$$

for all $P_j \in \mathbb{Z}_{\mathfrak{b}-1}, j = \{0, \cdots, k\}$.
Once we have a way to represent (possibly large) a, we would want to know how exactly to define the sequential multiplication of factors for any given bracketing shape.

6.2 *Defining* $x^{(\mathbf{A},\mathfrak{b})}$ *:* For any $x \in \mathbb{E}_{p^2}$, $(\mathbf{A}, \mathfrak{b})$ is defined as follows:

$$\begin{aligned} w_0 &= x, \\ w_i &= R_b(w_{i-1})[P_i], \ \ \text{for} i = 1, \cdots, k, \end{aligned} \tag{32}$$

If j =index of the first nonzero digit A_j,

$$x_j = \begin{cases} w_j, \ \text{if} A_j = 1, \\ R_{A_j}(w_j)[P_j \mod (A_j - 1)], \ \text{if} A_j > 1 \end{cases} \tag{33}$$

for $i = j+1, \cdots, k$,

$$x_i = \begin{cases} x_{i-1}, \ \text{if} A_i = 0, \\ w_i * x_{i-1}, \ \text{if } A_i = 1 \text{ and } P_{i-1} \text{ is even,} \\ x_{i-1} * w_i, \ \text{if } A_i = 1 \text{ and } P_{i-1} \text{ is odd,} \\ R_{A_i}(w_i)[P_i \mod (A_i - 1)] * x_{i-1}, \ \text{if } A_i > 1 \text{ and } P_{i-1} \text{ is even,} \\ x_{i-1} * R_{A_i}(w_i)[P_i \mod (A_i - 1)], \ \text{if } A_i > 1 \text{ and } P_{i-1} \text{ is odd,} \end{cases} \tag{34}$$

$$x^{(\mathbf{A},\mathfrak{b})} = x^k. \tag{35}$$

Note that the non-associativity and non-commutativity of the operation $*$ is reflected in the above equations.
Next, let us try to calculate the total number of multiplications required to achieve $x^{(\mathbf{A},\mathfrak{b})}$. In (32), according to the definition of $R_a(x)$ (here, a is replaced by the base $\mathfrak{b}$), the number of times x has been multiplied would be $k(\mathfrak{b}-1)$. From the cases in (33), if $A_j > 0$, then the number of multiplications will be $A_j - 1$ and, lastly, in (34) for $i = j+1, \cdots, k$ we will need one multiplication with x_{i-1} and $A_i - 1$ multiplications

as per the expression $R_{A_i}(w_i)[P_i \mod (A_i - 1)]$. An expression for the total multiplications of x required is summarised in the following:

6.3 For every base $\mathfrak{b} \leq 2$, every $x \in \mathbb{E}_{p^2}$, every $a \in \mathbb{Z}^+$ and every bracketing pattern $a_s = [P_0, P_1, \cdots, P_k]_{\mathfrak{b}-1}$, the value $x^{(\mathbf{A},\mathfrak{b})}$ is a product of $'a'$ multiplications of x,

$$x^{(\mathbf{A},\mathfrak{b})} = x^{(a,a_s,\mathfrak{b})} = \underbrace{(x * \cdots (x * x) \cdots)}_{\text{a copies of x}} \tag{36}$$

If O_b^* denotes the number of operations (multiplications) $*$ used to compute the result $x^{(\mathbf{A},\mathfrak{b})}$, then its value is given by the following expression,

$$O_b^* = k(\mathfrak{b} - 1) - 1 + \sum_{A_i \neq 0} A_i \tag{37}$$

.

6.4 *(Theorem 4, [1])* Let $x, y \in \mathbb{E}^*_{(p-1)^2}$. For every $(\mathbf{A}, \mathfrak{b}_1)$ and $(\mathbf{B}, \mathfrak{b}_2)$ chosen at random from the set $\mathbb{L}$ of bracketing shapes,

$$(x * y)^{(\mathbf{A},\mathfrak{b}_1)} = x^{(\mathbf{A},\mathfrak{b}_1)} * y^{(\mathbf{A},\mathfrak{b}_1)} \tag{38}$$

and,

$$x^{(\mathbf{A},\mathfrak{b}_1)(\mathbf{B},\mathfrak{b}_2)} = \left(x^{(\mathbf{A},\mathfrak{b}_1)}\right)^{(\mathbf{B},\mathfrak{b}_2)} = \left(x^{(\mathbf{B},\mathfrak{b}_2)}\right)^{(\mathbf{A},\mathfrak{b}_1)} = x^{(\mathbf{B},\mathfrak{b}_2)(\mathbf{A},\mathfrak{b}_1)} \tag{39}$$

.

6.5 As a consequence of (10) and (11), the Logarithmetic of power indices $(\mathbf{A}, \mathfrak{b}_1) = (a, a_s, \mathfrak{b}_1)$ and $(\mathbf{B}, \mathfrak{b}_2) = (b, b_s, \mathfrak{b}_2)$, $a, b \in \mathbb{Z}^+$ can be defined as, $(\mathbf{C}, \mathfrak{b}_3) = (\mathbf{A}, \mathfrak{b}_1) + (\mathbf{B}, \mathfrak{b}_2)$ iff $x^{(\mathbf{C},\mathfrak{b}_3)} = x^{(\mathbf{A},\mathfrak{b}_1)} * x^{(\mathbf{B},\mathfrak{b}_2)}$ for all $x \in \mathbb{E}_{p^2}$ and, if $(\mathbf{C}, \mathfrak{b}_3) = (c, c_s, \mathfrak{b}_3)$ then, $c = a + b$. And, $(d, d_s, \mathfrak{b}_4) = (\mathbf{D}, \mathfrak{b}_4) = (\mathbf{A}, \mathfrak{b}_1)(\mathbf{B}, \mathfrak{b}_2)$ iff, $x^{(\mathbf{D},\mathfrak{b}_4)} = \left(x^{(\mathbf{A},\mathfrak{b}_1)}\right)^{(\mathbf{B},\mathfrak{b}_2)}$ for all $x \in \mathbb{E}_{p^2}$, $d = ab$.

6.6 For base $\mathfrak{b} = 2$, the bracketing pattern $a_s = [P_0, P_1, \cdots, P_k]_{\mathfrak{b}-1}$ where $0 \leq P_i \leq \mathfrak{b} - 2$ for $i = 0, \cdots, k$ becomes a constant pattern, $a_s = [0, 0, \cdots, 0]$. Thus a power index $(\mathbf{A}, 2)$ can be written as, $(a, [\mathbf{0}], 2)$. The elements of $\mathbb{E}_{p^2}$ raised to such power indices form subgroupoids given by,

$$\langle x \rangle_2 = \{x^{(\mathbf{A},2)} \mid (\mathbf{A}, 2) = (a, [\mathbf{0}], 2), a \in \mathbb{Z}^+\} \tag{40}$$

The subgroupoid $(\langle x \rangle_2, *)$ of $(\mathbb{E}^*_{|\langle x \rangle_2|}, *)$ is called a *cyclic subgroupoid* of $\mathbb{E}_{p^2}$ of order $|\langle x \rangle_2|$.
The set,

$$\langle x \rangle = \{x^{\mathbf{A}} \mid \mathbf{A} = (a, a_s), a \in \mathbb{Z}^+,\ a_s \text{ is a bracketing shape}\} \tag{41}$$

is called a *a multiplicative subgroupoid*, $(\langle x \rangle, *) = (\mathbb{E}_{|\langle x \rangle|}, *)$ of $\mathbb{E}_{p^2}$ of order $|\langle x \rangle|$.
Let us denote the order of $\langle x \rangle_2$ as, $s(x)_2 = |\langle x \rangle_2|$ and order of $\langle x \rangle$ as, $s(x) = |\langle x \rangle|$, then we have the following relations:

$$\begin{aligned} s(x)_2 &\mid 2(p-1) \\ \text{and} \quad s_{max}(x)_2 = \underset{x \in \mathbb{E}_{p^2}}{max} &(s(x)_2) = 2(p-1). \end{aligned} \tag{42}$$

and,

$$s(x)|(p-1)^2 \tag{43}$$

$$\text{and} \quad s_{max}(x) = \underset{x \in \mathbb{E}_{p2}}{max}\ s(x) = (p-1)^2. \tag{44}$$

6.7 *Generators of* $\mathbb{E}^*_{(p-1)^2}$:

(Conjecture 1, [1]) Let $\mathbb{E}_{p^2}$ be an entropoid defined with a safe prime p (a prime p is called a *safe prime* if it is of the form $p = 2q+1$ where q is a prime) of λ bits, and let $g \in \mathbb{E}^*_{(p-1)^2}$. If the following conditions are true,

$$\begin{aligned} g &\neq g^{(p,[\mathbf{0}],2)} && (45)\\ g * g &\neq g^{(p-1,[\mathbf{0}],2)} && (46)\\ (g*(g*g)) &\neq g^{(p-2,[\mathbf{0}],2)} && (47)\\ (g*(g*g)) &\neq ((g*g)*g) && (48)\\ (g*(g*(g*g))) &\neq ((g*(g*g))*g), && (49)\end{aligned}$$

then the probability that g is a generator of $\mathbb{E}^*_{(p-1)^2}$ is,

$$Pr[g \; is \; a \; generator \; of \; G^*] > 1 - \epsilon \tag{50}$$

where, $\epsilon < \frac{1}{2^\lambda}$.

The, the probablity that an element of the maximal multiplicative subgroupoid, $\mathbb{E}^*_{(p-1)^2}$ can be represented in terms of the powers of the generator g:

Let g be a generator of $\mathbb{E}^*_{(p-1)^2}$ (where p is a safe prime) obtained using the process described in the above mentioned conjecture. Let y be an arbitrary element of $\mathbb{E}^*_{(p-1)^2}$. Then the probability that there exists a power index $(\mathbf{A}, 2)$ such that $y = g^{(\mathbf{A},2)}$ is,

$$Pr[\{\exists(\mathbf{A}, 2) \; and \; y = g^{(\mathbf{A},2)}\}] = \frac{1}{q}. \tag{51}$$

Recall from 6.6 that the elements of $\mathbb{E}_{p^2}$ raised to the power of indices $(\mathbf{A}, \mathfrak{b})$ with base $\mathfrak{b} = 2$ form a cyclic subgroupoid of $\mathbb{E}_{p^2}$. For a generator g of $\mathbb{E}^*_{(p-1)^2}$, if $x = g^{(\mathbf{A},2)}$ then from (42), the order of x would be $2(p-1)$ and so, the order of an element $y = x^{(p-1,[\mathbf{0}],2)}$ would be 2 which means $y^2 = \mathbf{1}_*$ (implying that y is a square root of $\mathbf{1}_*$). So, y can be either $\mathbf{1}_*$ or $\boxminus\mathbf{1}_*$ beause otherwise the order of x will exceed the upper bound, $2(p-1)$. Thus, we have the following:

Let g be a generator of $\mathbb{E}^*_{(p-1)^2}$. Then for every bracketing shape $(\mathbf{A}, \mathfrak{b}) = (a, a_s, \mathfrak{b}) \in \mathbb{L}$,

$$\left(g^{(\mathbf{A},\mathfrak{b})}\right)^{(p-1,[\mathbf{0}],2)} = \begin{cases} \mathbf{1}_*, \text{ if } a \text{ is even,} \\ \boxminus\mathbf{1}_*, \text{ if } a \text{ is odd.} \end{cases} \tag{52}$$

(Conjecture 2, [1]) Let g be a generator of $\mathbb{E}^*_{(p-1)^2}$, where $p \leq 11$. Then,

$$g_q = (g*(g*(g*((g*g)*g)))), \tag{53}$$

is the generator of the Sylow q-subquasigroup $\mathbb{E}^*_{p^2}$.

Let g_q be a generator of the Sylow q-quasigroup $\mathbb{E}^*_{q^2}$. Then for every bracketing shape $(\mathbf{A}, \mathfrak{b}) = (a, a_s, \mathfrak{b}) \in \mathbb{L}$ the following relations hold:

$$\left(g_q^{(\mathbf{A},\mathfrak{b})}\right)^{(p-1,[\mathbf{0}],2)} = \mathbf{1}_* \tag{54}$$

$$\left(g_q^{(\mathbf{A},\mathfrak{b})}\right)^{(q,[\mathbf{0}],2)} = y, \tag{55}$$

where y belongs in a subset of the set of square roots of the left unit,i.e., $y \in \mathbb{S}_q(p) \subseteq \mathbb{S}(p)$, such that $\mid \mathbb{S}_q(p) \mid = q$.

II. Examples

1. **The entropoid, $\mathbb{E}_{7^2}$:**
Let, $\mathbb{E}_{7^2} = \mathbb{F}_7 \times \mathbb{F}_7$ where $\mathbb{F}_7$ is the field of integers modulo 7. We take, $a_3 = 6, a_8 = 3, b_2 = 3, b_7 = 4$. Then, according to equation (14), the operation $*$ is defined as,

$$\begin{aligned} x * y = (x_1, x_2) * (y_1, y_2) &= \Big(\frac{6((3)(3)-4)}{(3)(4)} + 6x_2 + \frac{(3)(3)}{4}y_1 + 3x_2y_1, \\ &- \frac{3(3-(6)(4))}{(3)(4)} + \frac{(6)(4)}{3}y_2 + 3x_1 + 4x_1y_2\Big) \\ &= \Big(\frac{30}{12} + 6x_2 + \frac{9}{4}y_1 + 3x_2y_2, \\ &- \frac{3(-21)}{12} + \frac{24}{3}y_2 + 3x_1 + 4x_1y_2\Big) \\ &\equiv (6 + 6x_2 + 4y_1 + 3x_2y_1, y_2 + 3x_1 + 4x_1y_2) \end{aligned} \tag{56}$$

as the operations are modulo 7 in the field.

1.1 The multiplicative zero is, $\mathbf{0}_* = \big(-\frac{6}{3}, -\frac{3}{4}\big) \equiv (5, 1)$ and the multiplicative left unit is, $\mathbf{1}_* = \big(\frac{1}{4} - \frac{6}{3}, \frac{1}{3} - \frac{3}{4}\big) \equiv (0, 6)$.

$\mathbb{E}_{7^2}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	(0,0)	$(\mathbf{0}, \mathbf{1})$	(0,2)	(0,3)	(0,4)	(0,5)	(0,6)
1	(1,0)	$(\mathbf{1}, \mathbf{1})$	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)
2	(2,0)	$(\mathbf{2}, \mathbf{1})$	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)
3	(3,0)	$(\mathbf{3}, \mathbf{1})$	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)
4	(4,0)	$(\mathbf{4}, \mathbf{1})$	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)
5	$(\mathbf{5}, \mathbf{0})$	$(\mathbf{5}, \mathbf{1})$	$(\mathbf{5}, \mathbf{2})$	$(\mathbf{5}, \mathbf{3})$	$(\mathbf{5}, \mathbf{4})$	$(\mathbf{5}, \mathbf{5})$	$(\mathbf{5}, \mathbf{6})$
6	(6,0)	$(\mathbf{6}, \mathbf{1})$	(6,2)	(6,3)	(6,4)	(6,5)	(6,6)

Table 1: Elements of $\mathbb{E}_{7^2}$

1.2 In Table 1, the row and column corresponding to the zero element, $\mathbf{0}_* = (5, 1)$ have been highlighted to indicate their exclusion from $\mathbb{F}_7 \setminus \{-\frac{6}{3}\} \times \mathbb{F}_7 \setminus \{-\frac{3}{4}\} \equiv \mathbb{F}_7 \setminus \{5\} \times \mathbb{F}_7 \setminus \{1\} = \mathbb{E}^*_{6^2}$.
Next, as an illustration of how different bracketing shapes may give different outputs when applied to the same element, we give the following table for $a = 2, 3$ and 4.

a	**bracketing shape $\mathbf{a_s}$**	$(\mathbf{0}, \mathbf{0})$	$(\mathbf{0}, \mathbf{6})$	$(\mathbf{5}, \mathbf{1})$	$(\mathbf{6}, \mathbf{6})$
2	$(x * x)$	(6, 0)	(0, 6)	(5, 1)	(6, 0)
3	$(x * (x * x))$	(2, 0)	(0, 6)	(5, 1)	(6, 4)
	$((x * x) * x)$	(6, 4)	(0, 6)	(5, 1)	(2, 0)
4	$(x * (x * (x * x)))$	(0, 0)	(0, 6)	(5, 1)	(6, 6)
	$(x * ((x * x) * x))$	(2, 4)	(0, 6)	(5, 1)	(2, 4)
	$((x * x) * (x * x))$	(2, 4)	(0, 6)	(5, 1)	(2, 4)
	$((x * (x * x)) * x)$	(6, 6)	(0, 6)	(5, 1)	(0, 0)
	$(((x * x) * x) * x)$	(2, 4)	(0, 6)	(5, 1)	(2, 4)

Table 2: Raising different elements $'x'$ of $\mathbb{E}_{7^2}$ to the powers $a = 2, 3, 4$ with different brackting shapes a_s

1.3 Notice the columns corresponding to the zero element, $\mathbf{0}_* = (5, 1)$ and the multiplicative left unit, $\mathbf{1}_* = (0, 6)$. We find that both retain their fixed value even when raised to different powers a, that is, $\mathbf{0}^a_* = \mathbf{0}_*$ and, $\mathbf{1}^a_* = \mathbf{1}_*$.

#	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	9	2	36	4	9	36	1
1	12	2	6	18	12	6	36
2	3	2	12	36	3	12	9
3	36	2	18	2	36	18	4
4	12	2	6	18	12	6	36
5	2	1	2	2	2	2	2
6	3	2	12	36	3	12	9

Table 3: size of the sets $\langle x_1, x_2 \rangle$ denoted above by #

1.4 The elements of $\mathbb{E}_{7^2}$ can belong to different classes with cardinalities that are divisors of $(p-1)^2$ where $p = 7$. So, the cardinalities divide, $2^2 3^2$, i.e, they have possibilities, $\{1, 2, 3, 4, 6, 9, 18, 36\}$. All representatives of sets in Table 3 with 36 elements serve as generators for the maximal multiplicative groupoid, $(\mathbb{E}^*_{6^2}, *)$.

2. **The entropoid $\mathbb{E}_{11^2}$:**
Let the entropoid $\mathbb{E}_{11^2}$ be defined over the field of integers modulo 11 with $a_3 = 9, a_8 = 1, b_2 = 8, b_7 = 9$. Then, according to equation (14), the operation $*$ is defined as,

$$\begin{aligned} x * y = (x_1, x_2) * (y_1, y_2) &= \Big(\frac{9((1)(8) - 9)}{(1)(9)} + 9x_2 + \frac{(1)(8)}{9} y_1 + 1x_2 y_1, \\ &- \frac{8(1 - (9)(9))}{(1)(9)} + \frac{(9)(9)}{1} y_2 + 8x_1 + 9x_1 y_2\Big) \\ &\equiv (10 + 9x_2 + 7y_1 + x_2 y_1, 10 + 4y_2 + 8x_1 + 9x_1 y_2) \end{aligned} \tag{57}$$

as the operations are modulo 11 in the field.
The multiplicative zero is, $\mathbf{0}_* = \big(-\frac{9}{1}, -\frac{8}{9}\big) \equiv (2, 4)$ and the multiplicative left unit is, $\mathbf{1}_* = \big(\frac{1}{9} - \frac{9}{1}, \frac{1}{1} - \frac{8}{9}\big) \equiv (7, 5)$.

3. **We now demonstrate the computation of a power index in an entropoid:**
Let us consider the entropoid $\mathbb{E}_{7^2}$ with operation $*$ as defined in (56).
Here, $p = 7$ so, $(p-1)^2 = 36 = 2^2 \cdot 3^2$. Let, $\nu = q_1^{e_2}$. Then a Sylow 3-quasigroup of $(\mathbb{E}^*_{(p-1)^2}, *) = (\mathbb{E}^*_{36}, *)$ is $(\mathbb{E}^*_9, *)$.
A generator g_{q_i} of this 3-Sylow subquasigroup is $(6, 6)$ (figure 3). We choose two power indices, $(\mathbf{A}, \mathfrak{b}_1) = (a, a_s, \mathfrak{b}_1) = (5, 4, 3)$ and $(\mathbf{B}, \mathfrak{b}_2) = (b, b_s, \mathfrak{b}_2) = (6, 7, 4)$ and compute $g_{q_i}^{(\mathbf{A}, \mathfrak{b}_1)}$ and $g_{q_i}^{(\mathbf{B}, \mathfrak{b}_2)}$.
Using definitions in 6.1,
for base, $\mathfrak{b}_1 = 3$, $a = 5 = [A_0, A_1, \cdots, A_k]_{\mathfrak{b}_1} = [2, 1, 0]_3$ and, $a_s = 4 = [P_0, P_1, \cdots, P_k]_{\mathfrak{b}_1 - 1} = [0, 0, 1]_2$.
Using equations (32)-(35),

$$\begin{aligned} w_0 &= x = (6, 6) \\ i = 1 : w_1 &= R_3(w_0)[P_1] = R_3(x)[0] \\ &= x_{(x,2) to-left} = \big((6, 6) * \big((6, 6) * (6, 6)\big)\big) \\ &= (6, 4) \\ i = 2 : w_2 &= R_3(w_1)[P_2] = R_3(w_1)[1] \\ &= w_{1(w_1,1) to-left} * w_1 = \big((6, 4) * (6, 4)\big) * (6, 4) \\ &= (6, 4) \end{aligned}$$

Now, the first non-zero index of A_j, j is 0 ($A_0 \neq 0$).
Since $A_j = A_0 = 2 > 1$, hence,

$$x_0 = R_2(w_0)[0] = x * x = (6, 6) * (6, 6) = (6, 0)$$

For $i \in \{j + 1, \cdots, k\}$,

$$\begin{aligned} i = 1 : x_1 &= w_1 * x_0, \ \text{ as } A_i = A_1 = 1 \text{ and } P_{i-1} = P_0 = 0 \text{ is even} \\ &= (6,4) * (6,0) \\ &= (0,0) \\ i = 2 : x_2 &= x_1, \ \text{ as } A_i = A_2 = 0 \end{aligned}$$

Hence, $x^{(\mathbf{A},\mathfrak{b}_1)} = (6,6)^{(\mathbf{A},\mathfrak{b}_1)} = x_2 = (0,0)$.
Similarly, we proceed for the power index $(\mathbf{B}, \mathfrak{b}_2) = (b, b_s, \mathfrak{b}_2) = (6,7,4)$.
$b = 6 = [2,1]_4$ and, $b_s = [1,2]_3$.
Again, with the help of (32)-(35),

$$\begin{aligned} w_0 &= x = (6,6) \\ i = 1 : w_1 &= R_4(w_0)[P_1] = R_4(x)[0] \\ &= R_4(x)[0] * x = \big((6,6) * \big((6,6) * (6,6)\big)\big) * (6,6) \\ &= (0,0) \end{aligned}$$

Now, the first non-zero index of A_j, j is 0 $(A_0 \neq 0)$.
Since $A_j = A_0 = 2 > 1$, hence,

$$x_0 = R_2(w_0)[1 \mod 1] = x * x = (6,6) * (6,6) = (6,0)$$

For $i \in \{j+1, \cdots, k\}$,

$$\begin{aligned} i = 1 : x_1 &= x_0 * w_1, \ \text{ as } A_i = A_1 = 1 \text{ and } P_{i-1} = P_0 = 1 \text{ is odd} \\ &= (6,0) * (0,0) \\ &= (6,4) \end{aligned}$$

Hence, $x^{(\mathbf{B},\mathfrak{b}_2)} = (6,6)^{(\mathbf{B},\mathfrak{b}_2)} = x_1 = (6,4)$.

4. **Some observations:**
Suppose that the generator $g_{q_i)}$ and the value, $g_{q_i}^{(\mathbf{A},\mathfrak{b})}$ is publicly known. In our case, let the generator $(6,6)$ and the value, $(0,0)\Big(= (6,6)^{(a,a_s,\mathfrak{b}_1)}\Big)$ be known. Note that any attempt to retrieve the exact power index $(\mathbf{A}, \mathfrak{b}_1)$ would need a lot of computation power because, first, there may be multiple power indices that give the same value when raised to the power of $(6,6)$ and second, the exact pattern or an explicit bracketing shape cannot be determined just by analysing the known value.
This serves as a motivation to look for problems that may be perceived as 'hard' in an entropoid setting [1].

III. Entropoid based hard problems

In cryptography, an algorithm is said to be *polynomial time* if its running time has an upper bound in the form of a polynomial expression in the size of the input arguments, that is, running time $T(n) \approx O(n^k)$ for some positive constant k. If an algorithm or a computational problem *cannot* be solved efficiently, i.e., in polynomial time then that particular problem is termed as cryptographically *hard*.
One of the best known hard problems is the *Discrete Logarithmic Problem*, DLP. In a group setting, it can be stated as: *'Given $\alpha \in$ group G and $\beta \in \langle \alpha \rangle$, find the least positive integer x such that $\alpha^x = \beta$.'* The Diffie-Hellman Key Exchange protocol in a group setting is precisely based on the hardness of DLP.
Often, the hardness of a new or complicated problem is related to the computational hardness assumption of a better understood problem.
Here, we briefly state a few cryptographically hard problems in an entropoid setting [1].

1. **Discrete Entropoid Logarithmic Problem, DELP:** An entropoid $\mathbb{E}_{p^2}$ and a generator g_{q_i} of one of its Sylow subquasigroups $\mathbb{E}_{\nu}^*$ are publicly known. Given an element $y \in \mathbb{E}_{\nu}^*$ the problem is to find a power index $(\mathbf{A}, \mathfrak{b})$ such that $y = g_{q_i}^{(\mathbf{A},\mathfrak{b})}$.
The DLP is defined for groups whose operations are commutative and associative, unlike the DELP which is based on entropoid operations and hence donot have these additonal properties. Also, note here that a common approach to solve the DLP would make use of the cyclic group structure in group G say of order N with

generator g. Thus, G will have a unique index $i \in \{1, 2, \cdots, N\}$ such that for every element $y \in G$, $g^i = y$. However it is not the case in entropoids. $\mathbb{E}^*_{(p-1)^2}$ is not cyclic, for every $y \in \mathbb{E}^*_{(p-1)^2}$, there may exist multiple indices $(\mathbf{A}, \mathfrak{b})$ such that $y = g^{(\mathbf{A},\mathfrak{b})}$. Being able to find any one of these indices will solve the DELP.
Any quantum algorithm for solving will need quantum circuits that implement non-commutative operations of multiplication and also perform unknown patterns of bracketing shapes of non-commutative and non-associative operations. This poses a tough challenge especially because the number of such patterns can be exponentially high. The DLP is no harder to solve than the DELP, meaning, $DLP \leq DELP$.

2. **Computational Entropoid Diffie-Hellman Problem, CEDHP:** An entropoid $\mathbb{E}_{p^2}$ and a generator g_{q_i} of one of its Sylow subquasigroups $\mathbb{E}^*_{\nu}$ are publicly known. Given $g_{q_i}^{(\mathbf{A},\mathfrak{b}_1)}$ and $g_{q_i}^{(\mathbf{B},\mathfrak{b}_2)}$, where $(\mathbf{A}, \mathfrak{b}_1), (\mathbf{B}, \mathfrak{b}_2)$ are chosen at random from $\mathbb{L}$, the problem is to compute $g_{q_i}^{(\mathbf{A},\mathfrak{b}_1)(\mathbf{B},\mathfrak{b}_2)}$.
If an adversary can solve the DELP then it can also solve the CEDHP, i.e, if the power indices $(\mathbf{A}, \mathfrak{b}_1)$ and $(\mathbf{B}, \mathfrak{b}_2)$ can be extracted from the knowledge of the values of $g^{(\mathbf{A},\mathfrak{b}_1)}$ and $g^{(\mathbf{B},\mathfrak{b}_2)}$ then the value of $g^{(\mathbf{A},\mathfrak{b}_1)(\mathbf{B},\mathfrak{b}_2)}$ can be computed efficiently.
Thus, CEDHP is no harder to solve than DELP, that is, $CEDHP \leq DELP$.

3. **Decisional Entropoid Diffie-Hellman Problem, DEDHP:** An entropoid $\mathbb{E}_{p^2}$ and a generator g_{q_i} of one of its Sylow subquasigroups $\mathbb{E}^*_{\nu}$ are publicly known. Given $g_{q_i}^{(\mathbf{A},\mathfrak{b}_1)}$, $g_{q_i}^{(\mathbf{B},\mathfrak{b}_2)}$ and $g_{q_i}^{(\mathbf{C},\mathfrak{b}_3)}$, where $(\mathbf{A}, \mathfrak{b}_1), (\mathbf{B}, \mathfrak{b}_2), (\mathbf{C}, \mathfrak{b}_3)$ are chosen at random from $\mathbb{L}$, the problem is to decide if $(\mathbf{C}, \mathfrak{b}_3) = (\mathbf{A}, \mathfrak{b}_1)(\mathbf{B}, \mathfrak{b}_2)$ or if $(\mathbf{C}, \mathfrak{b}_3)$ is just chosen at random from $\mathbb{L}$.
The classical Decisional Diffie-Hellman, DDH is an easy problem for the multiplicative group $\mathbb{F}^*_p$ (for example, in $\mathbb{Z}^*_p$ where p is prime, the Legendre symbol of g^a helps to identify if a is even or odd and thus one can compare and compute significant bits of g^a, g^b and g^{ab} where g is a generator) but not for quadratic residue groups $QR(p)$ of $\mathbb{Z}^*_p$.
On similar lines, for an entropoid $\mathbb{E}_{p^2}$ and a generator g of its maximal quasigroup $\mathbb{E}^*_{(p-1)^2}$, then there is an efficient algorithm that solves DEDHP in $\mathbb{E}^*_{(p-1)^2}$.
However, we also have the following:
Let $\mathbb{E}_{p^2}$ be an entropoid, where $p = 2q + 1$ is a safe prime and g_q is the generator of its Sylow q-subquasigroup $\mathbb{E}^*_{q^2}$. Then there is no algorithm $\mathfrak{A}$ that solves DEDHP in $\mathbb{E}^*_{q^2}$ with significantly higher advantage over the strategy of uniformly random guesses for making the decisions.
If the CEDHP can be solved efficiently then one can compute the value of $g_{q_i}^{(\mathbf{A},\mathfrak{b}_1)(\mathbf{B},\mathfrak{b}_2)}$ and hence verify the nature of $(\mathbf{C}, \mathfrak{b}_3)$ thereby also solving the DEDHP. Hence, the DEDHP is no harder to solve than CEDHP, that is, $DEDHP \leq CEDHP$.

4. **Computational Discrete Entropoid Root Problem, CDERP:** An entropoid $\mathbb{E}_{p^2}$ and a generator g of its multiplicative quasigroups $\mathbb{E}^*_{(p-1)^2}$ are publicly known. Given $y = x^{(\mathbf{B},\mathfrak{b})}$ and $(\mathbf{B}, \mathfrak{b})$, where $x, y \in \mathbb{E}^*_{(p-1)^2}$ and $(\mathbf{B}, \mathfrak{b})$ chosen at random from $\mathbb{L}$, the problem is to compute $x = \sqrt[(\mathbf{B},\mathfrak{b})]{y}$.
The CDERP is no harder than DELP, i.e., $CDERP \leq DELP$.

IV. Cryptographic schemes

Post quantum cryptography is constantly looking for variations in DLP so as to regain its security. A natural implementation of DELP therefore is the following key exchange:

1. **Key Exchange Algorithm:** Let the underlying entropoid be $\mathbb{E}_{p^2}$ with suitable $(a_3, a_8, b_2, b_7) \in \mathbb{F}_p$. The prime p is a safe prime, $p = 2q + 1$ for some integer q.
   Parameters agreed upon by both parties: The prime q and hence the safe prime p of $\lambda = 128$ or 256 bits, a generator $g_q = GenQ(\lambda, p, a_3, a_8, b_2, b_7)$ and an odd base $\mathfrak{b}$ for the exponentiation operation.
   The key exchange algorithm is as follows:

   (i) Alice chooses a (random) power index $(\mathbf{A}, \mathfrak{b}) = (a, a_s, \mathfrak{b})$, $a \in \mathbb{Z}_p^*$ so as to compute $K_a = g_q^{(\mathbb{A},\mathfrak{b})}$ and send it to Bob.

   (ii) Bob chooses a (random) power index $(\mathbf{B}, \mathfrak{b}) = (b, b_s, \mathfrak{b})$, $b \in \mathbb{Z}_p^*$ so as to compute $K_b = g_q^{(\mathbb{B},\mathfrak{b})}$ and send it to Alice.

   (iii) Alice then computes $K_{ab} = K_b^{(\mathbb{A},\mathfrak{b})}$ whereas Bob calculates $K_{ba} = K_a^{(\mathbb{B},\mathfrak{b})}$.

   (iv) The public key is $K_{ab} = K_{ba}$.

2. **An ElGamal-like en(de)cryption algorithm:** An ElGamal scheme also uses the hardness of a DLP. We propose here an algorithm for encoding and decoding along this line but in an entropoid setting.
   Consider the following public parameters:

   (i) A safe prime $p = 2q + 1$ for some integer p and the quasigroup $\mathbb{E}^*_{(p-1)^2}$ which is also the maximal multiplicative subgroupoid of the entropoid $\mathbb{E}_{p^2}$ with suitable $(a_3, a_8, b_2, b_7) \in \mathbb{F}_p$.

   (ii) A generator g_q of $\mathbb{E}^*_{(p-1)^2}$.

   The algorithm is as follows:

   (i) Alice chooses a random power index $(\mathbf{A}, \mathfrak{b}_1) = (a, a_s, \mathfrak{b}_1)$, $a \in \mathbb{Z}_p^*$ so as to compute $K_a = g_q^{(\mathbb{A},\mathfrak{b}_1)}$. The private key is the power index $(\mathbf{A}, \mathfrak{b}_1) = (a, a_s, \mathfrak{b}_1)$

   (ii) Alice sends the pair (g_q, K_a) to Bob.

   (iii) Bob chooses a random power index $(\mathbf{B}, \mathfrak{b}_2) = (b, b_s, \mathfrak{b}_2)$, $b \in \mathbb{Z}_p^*$ and computes:

   - $K_b = g_q^{(\mathbb{B},\mathfrak{b}_2)}$, and,
   - $l = K_a^{(\mathbb{B},\mathfrak{b}_2)}$.
     The power index $(\mathbf{B}, \mathfrak{b}_2) = (b, b_s, \mathfrak{b}_2)$ serves as Bob's private key.

   (iv) Bob then carries out the encryption as follows:

   - First notice the fact that each element of the quasigroup $\mathbb{E}^*_{(p-1)^2}$ is a two-tuple which means K_a, K_b and l are all two tuple. For ease of implementation, we may take the help of a bijection that assigns to each ordered pair (x_1, x_2) of elements of $\mathbb{E}^*_{(p-1)^2}$ (in the sequence in which they appear in the Cartesian product of $\mathbb{F}_p^* \times \mathbb{F}_p^*$) an integer d in the range $\{0, 1, \cdots, p-2\}$. So, for example if we are dealing with the maximal multiplicative subgroupoid $\mathbb{E}^*_{6^2}$ in section II, Table 1, we may number the elements,

(0,0)	(0,2)	(0,3)	(0,4)	(0,5)	(0,6)
(1,0)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)
(2,0)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)
(3,0)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)
(4,0)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)
(6,0)	(6,2)	(6,3)	(6,4)	(6,5)	(6,6)

as,

$$\begin{array}{ccccc} 0 & 1 & 2 & \cdots & 5 \\ 6 & 7 & \cdots & \cdots & 11 \\ 12 & \cdots & \cdots & \cdots & 17 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 30 & \cdots & \cdots & \cdots & 35 \end{array}$$

Hence $\mathbb{E}^*_{(p-1)^2}$ may be represented as a quasigroup $Q = \{0, 1, \cdots, p-2\}$ with the entropic operation $*$.

- Consider the message, $M = \{m_1, m_2, \cdots, m_k\}$ to be encrypted. Recall the definition of $e-$ transformation from section I, equation (1f). The ciphertext $C = \{c_1, c_2, \cdots, c_k\}$ is given by,

$$\begin{aligned} c_1 &= l * m_1 \\ c_n &= c_{n-1} * m_n, \quad n \in \{2, 3, \cdots, k\} \end{aligned}$$

(v) Bob then sends the pair (K_b, C) to Alice.
Now the quasigroup operation $*$ will have a corresponding parastrophe operation $\setminus$ (equation 1e, section I). Then, using the theorem in section I, equation (1k) the decryption of the ciphertext can be carried out as follows:

(vi) Alice recovers the leader, $l = K_b^{(\mathbb{A}, \mathfrak{b}_1)}$.

(vii) The message M is retrieved by,

$$\begin{aligned} m_1 &= l \setminus c_1 \\ m_n &= c_{n-1} \setminus c_n, \quad n \in \{2, 3, \cdots, k\} \end{aligned}$$

For reasons we gave in example 3 and 4 of section II, the private keys (the exact power indices) of both Alice and Bob cannot be recovered from knowledge of the public parameters alone. Next, an important advantage of the quasigroup string transformation is that all substrings of the transformed string are uniformly distributed [18]. Also, as a post-quantum cryptographic scheme, the computational load of the scheme seems to be within acceptable limits.
Note that this is just an intial design. The quasigroup $e-$ and $d-$ transformations and the operations have ample scope for improvement in order to adapt the scheme for specific applications.

Next, consider the Computational Discrete Entropoid Root Problem, CDERP. The hardness of the CDERP can be used in an identification scheme as follows:

3. **A Digital Signature Scheme:** Let the underlying entropoid be $\mathbb{E}_{p^2}$ with suitable $(a_3, a_8, b_2, b_7) \in \mathbb{F}_p$. The prime p is a safe prime, $p = 2q + 1$ for some integer q and the size of p is $\lambda \in \{128, 192, 256\}$. The base for exponentiation may be taken to be $\mathfrak{b} = 257$ such that the power index $(\mathbb{B}, 257) = (b, b_s, 257)$ be denoted by $\mathbb{B}$. The NIST standardized cryptographic hash function, **SHAXXX** where, **XXX** $\in \{256, 384, 512\}$ has been used. Let **SHAXXX**(M) $= h_1 || h_2$ where $|h_1| = |h_2| = \frac{\mathbf{XXX}}{2}$ bits and M denote any message. Define $truncate_{\mathbb{L}}(\mathbf{SHAXXX}(M)) = (h, h_s)$ where $h = h_1$ and the sequence of bits of h_1 are interpreted as a little-endian encoding for a number $h \in \mathbb{Z}_{2^{\frac{\mathbf{XXX}}{2}}}$. The bits of h_2 are partitioned as $h_2 = [P_0, \cdots, P_{k_{max}-1}]_{256}$ where k_{max} belongs to the list of $\{16, 24, 32\}$ bytes. Compute $k = log_{257} h - 1$. h_s is taken to be a list of the first $k + 1$ bytes, $h_s = [P_0, \cdots, P_k]_{256}$. If $k < k_{max} - 1$ we truncate the remaining bytes.
Let the set of all such power indices $\mathbb{L}[h, 257]$ be denoted here by $\mathbb{L}_{257}$. Define a map,

$Hash_{XXX} : \{0,1\}^* \to \mathbb{L}_{257}$ as,
$Hash_{XXX}(M) = truncate_{\mathbb{L}}(\mathbf{SHAXXX}(M)) = (h, h_s, 257)$.

2.1 Key Generation:

```
1: Set random $x \leftarrow \mathbb{E}^*_{(p-1)^2}$
2: Set $\mathbf{PrivateKey} = x$.
3: Set $y = x^{\mathbf{B}}$.
4: Set $\mathbf{PublicKey} = y$.
5: Return ($\mathbf{PrivateKey}$, $\mathbf{PublicKey}$)
```

2.2 Signing a message, M:

```
1: Set random $r \leftarrow \mathbb{E}^*_{(p-1)^2}$.
2: Set $I = r^{\mathbf{B}}$.
3: Set $\mathbf{H} = Hash_{XXX}(I||M)$.
4: Set $s = (x * r)^{\mathbf{H}}$.
5: Set $\sigma = (I, s)$.
6: Return $(M, \sigma)$.
```

2.3 Verification of digital signature:

```
1: Set $\mathbf{H} = Hash_{XXX}(I||M)$.
2: if
$s^{\mathbf{B}} = (y * I)^{\mathbf{H}}$ then
Return 'True'
4: else
Return 'False'
end if
```

Note that, $s^{\mathbf{B}} = ((x * r)^{\mathbf{H}})^{\mathbf{B}} = (x^{\mathbf{H}})^{\mathbf{B}} * (r^{\mathbf{H}})^{\mathbf{B}} = (x^{\mathbf{B}})^{\mathbf{H}} * (r^{\mathbf{B}})^{\mathbf{H}} = y^{\mathbf{H}} * I^{\mathbf{H}} = (y * I)^{\mathbf{H}}$, which verifies the correctness signature scheme.

V. A proposed attack

So far the structure of the entropoids and the operations defined on them have seem advantageous over the more traditional and now vulnerable algebraic structures like groups and fields. While entropic operations allow us to perform feasible exponentiations of large indices, the absence of non-associativity makes it difficult to reverse the process. But what if there was a hidden group structure in them? We give here a brief overview of how [2] explores this question.

1. **The hidden group structure:**
   We state here the first theorem from [3] that [2] uses to retrieve a group structure from entropoids.

1.1 *Theorem:* Let $G = \{a, b, c, \cdots\}$ satisfy the following axioms:
(i) There exists an operation in G which associates with each pair a, b of G an element c of G, i.e., $a * b = c$.
(ii) The operation $*$ satisfies, $(a * b) * (c * d) = (a * c) * (b * d)$.
(iii) If for a, b, c in G, there exists unique solution x for each of the equations, $a * x = c$ and $x * b = c$.
Then, G forms an abelian group with respect to the new operation, $x \cdot y = z$ which is defined by the equation,

$$a * s \cdot r * b = a * b, \tag{58}$$

where r and s denote two fixed elements in G.
Looking closely, we find that the conditions (i)-(iii) resemble those of the entropoids, $\mathbb{E}_{p^2}$ and more specifically of the maximal multiplicative quasigroup $(\mathbb{E}^*_{(p-1)^2}, *)$. Then, according to the theorem, it will form an abelian group with respect to a new operation, $'\cdot'$. If s is replaced by the left multipicative unit $\mathbf{1}_*$ in (58), then the new abelian group operation $\cdot$ can be characterised by the property,

$$(x * \mathbf{1}_*) \cdot y = x * y \tag{59}$$

$x, y \in \mathbb{E}^*_{(p-1)^2}$.

1.2 The abelian group structure, $(\mathbb{E}^*_{(p-1)^2}, \cdot)$ will have the identity element $\mathbf{1}_*$ and let us denote it as $\mathbf{1}$ and $\mathbb{E}^*_{(p-1)^2} := \mathbb{E}$ in the group setting.
The map, $\sigma : \mathbb{E} \to \mathbb{E}$ given by, $\sigma(x) = x * \mathbf{1}$ is an automorphism on $(\mathbb{E}, *)$ as well as $(\mathbb{E}, \cdot)$.
Then from the definition of $*$ in (14),

$$\begin{aligned} \sigma(x) = x * \mathbf{1} = (x_1, x_2) * \Big(\frac{1}{b_7} - \frac{a_3}{a_8}, \frac{1}{a_8} - \frac{b_2}{b_7}\Big) \\ = \Bigg(\frac{a_3(a_8b_2 - b_7)}{a_8b_7} + a_3x_2 + \frac{a_8b_2}{b_7}\Big(\frac{1}{b_7} - \frac{a_3}{a_8}\Big) + a_8x_2\Big(\frac{1}{b_7} - \frac{a_3}{a_8}\Big), \\ - \frac{b_2(b_7a_3 - a_8)}{a_8b_7} + \frac{a_3b_7}{a_8}\Big(\frac{1}{a_8} - \frac{b_2}{b_7}\Big) + b_2x_1 + b_7x_1\Big(\frac{1}{a_8} - \frac{b_2}{b_7}\Big)\Bigg) \\ = \Big(\frac{a_8^2b_2 - a_3b_7^2}{a_8b_7^2} + a_8b_7x^2, \frac{a_3b_7^2 - a_8^2b_2}{a_8^2b_7} + b_7a_8x_1\Big) \end{aligned} \tag{60}$$

The order of the automorphism σ is 2.

1.3 (59) can now be written as,

$$(x * \mathbf{1}_*) \cdot y = (x * \mathbf{1}) \cdot y = \sigma(x) \cdot y = x * y \tag{61}$$

The abelian group operation $\cdot$ can be defined as,

$$\begin{aligned} (x_1, x_2) \cdot (y_1, y_2) = \Big(b_7x_1y_1 + \frac{a_3b_7}{a_8}x_1 + \frac{a_3b_7}{a_8}y_1 + \frac{a_3^2b_7 - a_3a_8}{a_8^2}, \\ a_8x_2y_2 + \frac{a_8b_2}{b_7}x_2 + \frac{a_8b_2}{b_7}y_2 + \frac{a_8b_2^2 - b_2b_7}{b_7^2}\Big). \end{aligned} \tag{62}$$

Each component of $(\mathbb{E}, \cdot)$ is isomorphic to a direct product of $(\mathbb{F}_p^\times, \cdot)$ with itself, given by

$$\iota : \mathbb{E} \to (\mathbb{F}_p^\times)^2, \;\; (x_1, x_2) \to \Big(b_7x_1 + \frac{a_3b_7}{a_8}, a_8x_2 + \frac{a_8b_2}{b_7}\Big). \tag{63}$$

1.4 Equation (61) has the potential to reduce the non-associative exponentiations in $(\mathbb{E}^*_{(p-1)^2}, *)$ into exponentiations in the abelian group $(\mathbb{E}, \cdot)$. Thus the choice of non-associative bracketing shapes while operating an element x with itself with respect to $*$ would no longer matter.
We observe that, for an element x in $\mathbb{E}$, $x * x = \sigma(x) \cdot x$ and, $\sigma^2 = id$ on $\mathbb{E}$. Then x raised to any non-associative power index $\mathbf{A}$, that is, $x^{\mathbf{A}}$ can have the form,

$$(\sigma(x))^i \cdot x^j, \quad i, j \in \mathbb{Z}_{\geq 0}$$

or, using the notation x^σ for $\sigma(x)$ as in [2],

$$(x^\sigma)^i \cdot x^j, \quad i, j \in \mathbb{Z}_{\geq 0} \;\; \text{and} \;\; \sigma^2 = id \tag{64}$$

1.5 *Reducing DELP into a specific case of DLP:*
The problem of finding a power index $\mathbf{A}$ in DELP now reduces to recovering the constants i, j corresponding to the private key, $x \to x^{\mathbf{A}}$. Following are the steps involved:

- Using the isomorphism in (63), the generator g of $\mathbb{E}$, g^σ and $g^{\mathbf{A}}$ are mapped as given below:

$$\iota(g) = (\alpha_1, \alpha_2), \qquad \iota(g^\sigma) = (\beta_1, \beta_2), \qquad \iota(g^{\mathbf{A}}) = (\gamma_1, \gamma_2)$$

  where $\alpha_i, \beta_i, \gamma_i$ are in $\mathbb{F}_p$, $i = 1, 2$.

- Next, a generator κ of the group $\mathbb{F}_p^\times$ is chosen and the following are calculated:

$$r_i = \log_\kappa(\alpha_i) \qquad s_i = \log_\kappa(\beta_i) \qquad t_i = \log_\kappa(\gamma_i) \qquad i = 1, 2 \qquad in\ \ \mathbb{F}_p$$

- The linear system, $\begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} r_i & r_2 \\ s_i & s_2 \end{pmatrix} = \begin{pmatrix} t_i & t_2 \end{pmatrix} \mod (p-1)$, $(i, j) \in \mathbb{Z}^2$.

- The private key $x \to x^{\mathbf{A}}$ is evaluated as, $x \to \iota^{-1}((x^\sigma)^i \cdot x^j)$.

Thus, a total of six discrete logarithm problems in $\mathbb{F}_p$ and a 2×2 linear system in $\mathbb{Z}^2$ is solved and the final outcome used to construct an equivalent private key to x^A. We say *equivalent* because it is not strictly necessary to recover the exact power index of the private key as the map from a public to a private key is not injective.

2. **The general case:** A general attack on entropoid relies on a theorem composed from the works of Murdock[5], Toyoda[3] and Bruck[6].
(Theorem 1, [2]) 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,

$$x * y = x^\sigma \cdot y^\tau \cdot c \tag{65}$$

Note that (61) was a particular case with $\tau = id$ and $c = 1$.
This theorem reveals that the composition law in any entropic quasigroup actually comes from a multiplication in an abelian group where the elements have been mapped under automorphisms and translated by constants.

2.1 The proposed attack attempts to find ways to write the public key $g^{\mathbf{A}}$ in the form, $g^\xi \cdot g^\gamma$ $(\xi, \gamma \in \mathbb{Z}[\sigma, \tau])$ for a generator g such that $x^{\mathbf{A}}$ may be computed for any arbitrary $x \in G$. But, there are multiple solutions (ξ, γ) and not all result in equivalent private keys.

2.2 *Redundancy in* (ξ, γ) :
(Lemma 2, [2]) For a binary operation, $x * y = x^\sigma \cdot y^\tau \cdot c$ and any non-associative constant $\mathbf{A}$, there exists $\gamma \in \mathbb{Z}[\gamma, \tau]$ such that, for all $x \in G$,

$$x^{\mathbf{A}} = x^{1 + (\sigma + \tau - 1)\gamma} \cdot c^\gamma \tag{66}$$

If this equation holds for some $x = g \in G$ then it holds for every $x \in \langle g \rangle_*$.

VI. Modifications proposed in the initial structure of entropoids

Theorem 1 of [2] and hence the 'attack' is based on the assumption that the underlying entropic structures are always quasigroups. [7] constructs a multi-dimensional entropic operation that is not always a quasigroup operation.

1. Let the quasigroup operation $*$ defined in (14) be considered as a one-dimensional operation in the sense that, $\mathbb{E} = (\mathbb{F}_p^\times)^2$ is taken to be one-dimensional entropoid (thus an m-dimensional entropoid would be

$\mathbb{E}^m = ((\mathbb{F}_p^\times)^2)^m)$. So,

$$(x_1, x_2) *_1 (y_1, y_2) = \Big(\frac{a_3(a_8 b_2 - b_7)}{a_8 b_7} + a_3 x_2 + \frac{a_8 b_2}{b_7} y_1 + a_8 x_2 y_1, \\ \frac{-b_2(a_8 - a_3 b_7)}{a_8 b_7} + \frac{a_3 b_7}{a_8} y_2 + b_2 x_1 + b_7 x_1 y_2\Big) \tag{67}$$

1.1 *Product of m-dimensional elements of* $\mathbb{E})^m$*:*
For $x, y \in \mathbb{E}^m$, i.e., $x = (x_0, \cdots, x_{m-1})$ and $y = (y_0, \cdots, y_{m-1})$, the component-wise product $\prod$ of x and y is defined as:

$$z = \prod(x, y) = (z_0, \cdots, z_{m-1}) \tag{68}$$

where $z_i = x_i *_1 y_i$ for $i \in \mathbb{Z}_m$.
Note that, $x_i *_1 y_1 = (x_{i1}, x_{i2}) *_1 (y_{i1}, y_{i2})$, where each $x_{ij}, y_{ij} \in \mathbb{F}_p^\times,\ \ 0 \le i \le m-1,\ \ j = 1, 2.$

1.2 *D-transformation of an element in* $\mathbb{E}^m$*:*
For an element $x = (x_0, \cdots, x_{m-1}) \in \mathbb{E}^m$, and a non-zero element l of $\mathbb{E}$, i.e., $l \in \mathbb{E}^*$, a D-transformation of x with respect to the leader element l is defined as:

$$z = D_l(x) = (z_0, \cdots, z_{m-1}) \tag{69}$$

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

1.3 *Derangement permutation:* A derangement permutation is one in which there is no fixed element. A derangement permutation Δ_m of an element $x = (x_0, \cdots, x_{m-1}) \in \mathbb{E}^m$ is defined as,

$$\Delta_m(x) = (x_0, \cdots, x_{m-1}) = (x_{\delta(0)}, \cdots, x_{\delta(m-1)}) \tag{70}$$

such that, $\delta(i) \ne i$ for all $i \in \mathbb{Z}_m$.

1.4 *Generalised Feistel transformation:*
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 respect to a leader l is defined as follows:

$$\mathcal{F}_{m,l}(x) := \Delta_m(D_l(x)), \tag{71}$$

and, on similar lines, a multiple rounds, $'Rounds'$ generalized Feistel transformation, $\mathcal{F}_{m,L}^{(Rounds)} : \mathbb{E}^m \to \mathbb{E}^m$ with respect to the list of leaders, $L = \{l_1, l_2, \cdots, l_{Rounds}\}$ is defined as:

$$\mathcal{F}_{m,L}^{(Rounds)}(x) := \mathcal{F}_{m,l_{Rounds}}(x) \circ \cdots \circ \mathcal{F}_{m,l_1}(x) \tag{72}$$

Thus, a *Rounds* generalised Feistel transformation can be viewed as a composition of *Rounds* number of one round general Feistel transformations with leaders $l_{Rounds}, \cdots, l_1$.

1.5 *Defining* $* := *_m$ *with the help of (68)-(72):*
Let $m \ge 2$, $Rounds \ge 1$, and let $x, y \in \mathbb{E}^m$. The operation $* := *_{m,Rounds}$ is defined as:

$$x * y = \prod\Big(y, \mathcal{F}_{m,L}^{(Rounds)}\big(\prod(x, y)\big)\Big) \tag{73}$$

So, if $\prod(x, y) = (z_0, \cdots, z_{m-1}) = z$, then, $x * y = \prod\Big(y, \mathcal{F}_{m,L}^{(Rounds)}(z)\Big) = \prod\Big(y, \Delta_m\big(D_L(z)\big)\Big)$.

2. **Observations:**

2.1 The multi-dimensional operation $*$ is entropic as defined in equation (1).
If,

$$\begin{aligned}\prod(p,q) &= k \\ &= (k_0, \cdots, k_{m-1}) \\ &= \prod(r,s) = (t_0, \cdots, t_{m-1}) \\ &= t,\end{aligned}$$

then it means,

$$\begin{aligned} k_i &= t_i \forall i \in \mathbb{Z}^m \\ \Rightarrow p_i *_1 q_i &= r_i *_1 s_i \forall i \in \mathbb{Z}^m. \end{aligned}$$

Since $*_1$ is entropic so, $p_i *_1 r_i = q_i *_1 s_i \forall i \in \mathbb{Z}^m$, hence, the operation $*_{m,Rounds} := *$ is also entropic.

2.2 The operation $*$ is not always a quasigroup operation. 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, that is, there exists no $e \in \mathbb{E}^2$ such that, $e * x = x$ holds or $x * e = x$ holds.

2.3 As the dimension m increases, the degree of the multivariate polynomials describing the operation $*$ grows even faster. Thus, the approach of constructing commuting automorphisms, σ, τ and infact the abelian operation $\cdot$ of $(G, \cdot)$ becomes tough.
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,
$a(n) = 2Fibonacci(n) + 1$, where, $Fibonacci(n)$ is the n-th Fibonacci number.
Without a feasible algorithm to determine the automorphisms σ, τ or even the isomorphism ι, describing the structure of the hidden abelian group is not efficient.

3. **Examples:**

3.1 Let the following Cayley table represent a 4×4 medial quasigroup operation $*_1$:

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

We experimented with a few sets of leaders, $L_1 = \{0, 0\}$, $L_2 = \{0, 1\}$, $L_3 = \{1, 0\}$, $L_4 = \{0, 0, 1, 1\}$.

$L_1 = \{0, 0\}$:

$*_1$	0	1	2	$\cdots$	5	$\cdots$	15
0	$\cdot$	$\cdot$	$\cdot$	$\cdots$	$\cdot$	$\cdots$	$\cdot$
1	$\cdot$	0	$\cdot$	$\cdots$	0	$\cdots$	$\cdot$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
15	$\cdot$	$\cdot$	$\cdot$	$\cdots$	$\cdot$	$\cdots$	$\cdot$

$L_2 = \{0, 1\}$:

$*_1$	0	$\cdots$	8	$\cdots$	12	$\cdots$	15
0	$\cdot$	$\cdots$	12	$\cdots$	12	$\cdots$	$\cdot$
1	$\cdot$	$\cdots$	$\cdot$	$\cdots$	$\cdot$	$\cdots$	$\cdot$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
15	$\cdot$	$\cdots$	$\cdot$	$\cdots$	$\cdot$	$\cdots$	$\cdot$

None of the above structures are Latin squares and hence donot correspond to quasigroups. Even those generated using L_3 and L_4 were not quasigroups. In such a case, the threat that the presence of the hidden abelian group structure posed could be averted.

3.2 Next, let us discuss the example of the entropic quasigroup that [7] gives:

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

The set of leaders $L = \{2, 3, 1, 1, 0, 1, 0, 0, 1\}$ again didnot produce a quasigroup.
However, when the operation $*$ was applied to the set $L = \{2, 3, 1, 1, 0, 1, 0, 0\}$ it produced the following entropic quasigroup:

$*$	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

The examples given above make use of a 4 × 4 starting entropoid. In terms of complexity, these structures may still be susceptible to brute-force attacks. It should therefore be noted that implementing larger order quasigroups may be beneficial to resist these attacks. The order of the quasigroups will infact be dictated by the current capabilities of the equation solvers and high performance computing systems.

4. **Investigation of properties:**
Next, as and when the multi-dimensional entropic operation (73) produces a quasigroup, a natural progression is to look for some definitive properties that ensure that the quasigroup formed is suitable for cryptographic use. [8], [9], [10], [11], [12], [13] state some such properties that have been found useful.

4.1 Polynomial completeness: The problem of verifying solutions of equations is NP-complete over polynomially complete quasigroups. A finite quasigroup is polynomially complete iff it is simple and non-affine. While there is no dearth of ways to check simplicity or non-affiness, it is the nature and size of the quasigroup that determines which way to go.

(i) Simplicity: One of the ways is to take into account the equivalence relations of the quasigroup (Q, f). A quasigroup is simple if f preserves no non-trivial equivalence relations on Q. In other words, a quasigroup is simple if it has only trivial congruences. This motivates us for an algorithm [14] to check for simplicity given in the next page.
Consider the quasigroup (Q, f) with $Q = \{0, 1, \cdots, k-1\}$, $k \in \mathbb{N}$. For implementation purposes and complexity analysis, let the quasigroup be represenated by its Cayley table and its operations be represenated by the arithmetic operations in $\mathbb{Z}_k$.

The complexity of the algorithm is $O(|Q|^3)$.

```
Input: Pairs $(0, i)$
Output: Classification: simple/non-simple
----------------------------------------
1. for $i = 1$ to $k - 1$
(i) cycle through all pairs $(0, i)$
(ii) build the transitive closures of the relation $0 \sim i$ under the action of $f$
2. if (relation is non-trivial)
return "non-simple"
endif
endcycle
return "simple"
```

Algorithm: Checking simplicity

(ii) Non-affineness: A universal algebra A is called *affine* iff A is equipped with a structure of an additive abelian group such that each basic n-ary operation f of A has the form $f(x_1, \cdots, x_n) = \alpha_1(x_1) + \cdots + \alpha_n(x_n) +$, where $c \in A$ and $\alpha_1, \cdots, \alpha_n$ are group endomorphisms of $(A, +)$. In case of quasigroups, it is called a T-quasigroup or 'affine' if the abelian group $(Q, +, 0, -)$ is such that α and β in $x \cdot y = \alpha(x) + \beta(y) + c$ are both automorphisms of $(Q, +, 0, -)$ for some $c \in Q$.
Suppose that the T-quasigroup Q is defined on a cyclic group $(Q, +)$ of order n. Then each automorphisms has the form $x \to ax$, where a is an invertible element of the ring $\mathbb{Z}_n$. Thus, $xy = ax + by + c$, a, b are invertible elements in $\mathbb{Z}_n$. In such a T-quasigroup with $n = pq$, the relation $x \sim y \Leftrightarrow x \cong y($ mod $q)$ is a congruence. If n is not a prime then this congruence will be non-trivial and hence Q non-simple.
An algorithm to check non-affineness [12] is given below:
The complexity of the algorithm is $O(|Q|^3)$.

```
Input: $n \times n$ Cayley table corresponding to the quasigroup
Output: Classification: affine/non-affine
----------------------------------------
1. Reorder the rows and columns of the Cayley table so that:
the first row and the first column specify the identical permutation.
2. check: whether the resulting table specifies an Abelian group
3. if no,
return "non-affine"
4. $A \leftarrow$ column of the original Cayley table starting with 0
$B \leftarrow$ row of the original Cayley table starting with 0
5. if
$A$ or $B$ are not automorphisms with respect to $+$,
return "non-affine"
6. $C \leftarrow$ upper left element of the original Cayley table
check: the identity $f(x, y) = A(x) + B(y) + C$ holds
if yes,
return "affine"
else
return "non-affine"
```

Algorithm: Verifying affineness

Notice that the 'attack' described in the previous section was possible precisely because of the hidden abelian group structure in the initial entropoids.
As a different approach, we can also check for the polynomial completeness of a quasigroup of order $n > 5$ with the help of the algorithm given below.
Consider a quasigroup Q of order n represented by its $n \times n$ Latin square. Let the row permutations be defined by σ_i and the column permutations by τ_i.

While it may seem like checking for polynomial completeness is more efficient than checking for simplicity and non-affiness separately, it should be noted that there are instances when the above algorithm will not

```
Input: $n \times n$ Latin square corresponding to the quasigroup Q of order $n$
Output: Classification: quasigroup is polynomially complete/unidentified

1. flag=0
2. for $i = 1$ to $n$
      Decompose row permutation $\sigma_i$ of $Q$ into disjoint cycles;
      Check: existence of a sub-cycle of $\sigma_i$ of prime length
    $p \in (\lfloor \frac{n}{2} \rfloor + 1, n - 2)$;
    • if yes, then check whether $(n - p \geq 3)$ or $(n - p = 2$ and $n \neq 2^t$ for
    $t \in \mathbb{N})$;
       if yes then flag=1; break; endif
      endif
      endfor
3. if flag=0 then repeat step 2 for column permutation $\tau_j$ , $1 \leq j \leq n$ of $Q$
endif 4. if flag=1 print : Polynomially Complete
else print : unidentified
endif
```

Algorithm: Verifying polynomial completeness

be able to identify the nature of the quasigroup.

As an example, consider the first row permutation of the 16×16 Cayley table in section 3.2 give by, $\sigma_1 = (1\,5\,7\,13\,8\,10)(2\,3\,14)(4\,12\,11\,16\,9\,6)(15)$. Here $n = 16$ so according to the algorithm given above, to classify the quasigroup as polynomially complete, σ_1 would need to have a sub-cycle of length p which must be prime and hence belong to one of the following, $\{11, 13\}$. Since none of the sub-cycles of σ_1 has this length, the decision cannot be made. So we need to move on to the next row permutation, $\sigma_2 = (1)(2\,11\,8\,14\,10\,9)(3\,6\,12\,15\,7\,5)(4\,16\,13)$. Again, we fail to make a decision. So we continue with the next row permutation.

It can be seen that all row permutations have sub-cycles of the same lengths, that is, of lengths $1, 3, 6$. So we will not be able to reach a decision even after we go through all the 16 row permutations. We therefore have to move on to the column permutations:

$\tau_1 = (1\,2\,11\,13\,15\,10)(3\,7\,4\,14\,6\,16)(5\,9\,8)(12)$. We are once again faced with unclear markers. Since all the other column permutations also have a similar sub-cycle structure, the algorithm given above will not be helpful in deciding the polynomial completeness of the said quaisgroup.

4.2 Non-associativity and associative triples: Let the row and column permutations of the corresponding Cayley table of a quasigroup Q of order n be denoted by σ_i and τ_i respectively. Then,the subgroup of permutations in Q generated by,

$\sigma_1, \cdots, \sigma_n, \tau_1, \cdots, \tau_n$ is known as the *Multiplication group*, *MultQ*.

The subgroup of *MultQ* generated by the permutations,

$$\sigma_j \sigma_1^{-1}, \;\; \tau_j \tau_1^{-1}, \;\; i, j = 2, \cdots, n$$

is denoted by $G(Q)$.

A quasigroup is called highly non-associative if $MultQ = Sym(Q)$, the symmetric group of permutations [10]. A highly non-associative quasigroup of any order is simple.

In an algebra $\mathfrak{A}$, the *associator* [15],

$$(x, y, z) = (xy)z - x(yz)$$

of any three elements is a measure of associativity or for that matter a lack of it, in $\mathfrak{A}$. The associator (x, y, z) is linear in each argument.

For a quasigroup Q, a triple (a, b, c), $a, b, c \in Q$, is called associative if

$$(ab)c = a(bc)$$

that is, in terms of the associator,

$$(a, b, c) = 0$$

The total number of associative triples in Q is denoted by $a(Q)$.
$a(Q)$ is called the associativity index of Q. Infact, for an associative triple (x, a, y) of the quasigroup Q, the expression, $x(ay) = (xa)y$ can be written in terms of the left multiplication (by x) map L_x and right multiplication (by y) map R_y as, $L_x R_y a = R_y L_x a$.
Now, let $x = x_i$, $y = x_j$. So, in terms of the row and column permutations $\sigma_1, \cdots, \sigma_n$ and $\tau_1, \cdots, \tau_n$ repectively,
$L_x = \sigma_i$, $R_y = \tau_j$. Thus, $L_x R_y a = \sigma_i \tau_j a, R_y L_x a = \tau_j \sigma_i a$.This implies that a triple (x_i, a, x_j) is associative if and only if $\sigma_i \tau_j a = \tau_j \sigma_i a$. Or, equivalently, $\sigma_i^{-1} \tau_j^{-1} \sigma_i \tau_j a = a$.
An algorithm to check for associative triples:
Let $[\sigma_i^{-1}, \tau_j^{-1}] = \sigma_i^{-1} \tau_j^{-1} \sigma_i \tau_j$ denote a group commutator.
For example, again consider the quasigroup in 3.2:

```
**Input:** $n \times n$ Cayley table corresponding to the quasigroup
**Output:** Associative triples and their total numbers in $Q$
1. List all the row and column permutations as well as their inverses, that is,
$\sigma_1, \cdots, \sigma_n$ and $\tau_1, \cdots, \tau_n$ and correspondingly, $\sigma_1^{-1}, \cdots, \sigma_n^{-1}$ and $\tau_1^{-1}, \cdots, \tau_n^{-1}$.
2. for $i = 1$ to $n$
for $j = 1$ to $n$
(i) Calculate the commutator, $[\sigma_i^{-1}, \tau_j^{-1}] = \sigma_i^{-1} \tau_j^{-1} \sigma_i \tau_j$
(ii) Represent the calculated permutation above in cycle form
3. List all elements $x_k$ in $Q$ that donot belong to any non-trivial cycle of $[\sigma_i^{-1}, \tau_j^{-1}]$ and let it be denoted by $\bar{x_k}$.
4. for each $[\sigma_i^{-1}, \tau_j^{-1}]$,
assoiative triples are $(x_i, \bar{x_k}, x_j)$ $\forall \bar{x_k}$.
5. Total number of associative triples $= \sum \# \bar{x_k}$ for each $i, j$.
```

Algorithm: Associative triples

We had determined the first row and first column permutation as, $\sigma_1 = (1\,5\,7\,13\,8\,10)(2\,3\,14)(4\,12\,11\,16\,9\,6)(15)$ and
$\tau_1 = (1\,2\,11\,13\,15\,10)(3\,7\,4\,14\,6\,16)(5\,9\,8)(12)$ respectively.
Their inverses are: $\sigma_1^{-1} = (1\,2\,11\,13\,15\,10)(3\,7\,4\,14\,6\,16)(5\,9\,8)(12)$ and $\tau_1^{-1} = (1\,10\,15\,13\,11\,2)(3\,16\,6\,14\,4\,7)(5\,8\,9)(12)$.
Then, $[\sigma_1^{-1}, \tau_1^{-1}] = \sigma_1^{-1} \tau_1^{-1} \sigma_1 \tau_1 = (1\,3\,13\,15)(2\,16\,14\,4)(5\,6\,9\,10)(7\,12\,11\,8)$. Since this permutation has no fixed elements so no $x_k \in Q$ is a part of any non-trivial cycle. Thus there are no associative triples with respect to σ_1 and τ_1.
Next, let us calculate $[\sigma_2^{-1}, \tau_1^{-1}]$. We have,
$\sigma_2 = (1)(2\,11\,8\,14\,10\,9)(3\,6\,12\,15\,7\,5)(4\,16\,13)$ and hence,
$\sigma_2^{-1} = (1)(2\,9\,101\,4\,8\,11)(3\,5\,7\,15\,12\,6)(4\,13\,16)$.
Then, $[\sigma_2^{-1}, \tau_1^{-1}] = (1\,9\,13\,5)(2\,10\,14\,6)(3\,11\,15\,7)(4\,12\,16\,8)$. Again, no associative triples with respect to σ_2 and τ_1.
In this way we can check for associative triples taking into account the rest of the row and column permutations. Note that quasigroups with a small associativity index are preferred as they prevent second pre-image based attacks in certain types of cryptographic schemes.

4.3 Existence of subquasigroups [12, 13]: Being able to identify subquasigroups (clearly of lesser orders) within the chosen quasigroup could make it susceptible to less complex brute-force attacks or even lead to the attacker being able to exploit hidden patterns in these structures.
A method to check for existence of subquasigroups:
Consider any subset Q' of the quasigroup (Q, f) and let, $[Q']$ denote the set of all constants generated by the quasigroup operation f from Q'. Then Q' is a subset of a proper subquasigroup of Q iff $[Q'] \neq Q$.
To verify if there exists proper subquasigroups of size say, atleast k one can list all k-element subsets Q' of Q and compute $[Q']$ for all of them. The complexity of this procedure is $O(|Q|^{k+2})$ and to improve this bound, one could additionally do the following:
1. compute the 'partial closures' of all Q' upto a specified size.
2. if
a subquasigroup is found, stop

3. else
build a system of representatives that generate minimum elements in the set of 'partial closures' and then compute the 'full closures' of all representatives.
(Note that a set of represenatatives can be found because the operation $[Q']$ is monotonous).
(Theorem 3, [12]) The algorithm proposed decides whether there exists a non-trivial subquasigroup with temporal complexity $O(|Q|^3 \log |Q|)$ and spatial complexity $O(|Q|^{5/2})$. Existence of arbitrary proper subquasigroups is decided with temporal complexity $O(|Q|^{7/3} \cdot (\log |Q|)^{2/3})$ and spatial complexity $O(|Q|^2)$.

Some advancements: A recent updated version of [2] in the ePrint server suggests that the attack can be generalised to break the muti-dimensional structures (even those that are not quasigroups). It discusses two ways to do so:

(i) Since the multi-dimensional entropic operations are essentially defined over copies of $\mathbb{E}_{p^2}$, the initial attack strategy can still be used to linearise these starting entropoids and hence break the mutli-dimensional structures.

(ii) There exist some generalisations of Toyoda's theorem (Theorem 1.1, section V) that can be applied to entropic magmas (which are not necessarily quasigroups) to again obtain abelian structures.

As for the first strategy, as has already been mentioned in the text, starting out with suitably higher order entropoids will greatly increase the attack complexity and may well help resist it. We analyse the second method:
Out of three papers [2] consults for the generalisations, we take a look at [19]. First some definitions from [19]:
Consider a groupoid $(G.\cdot)$ and an element $a \in G$.

(i) Mappings λ_a and $\mathfrak{e}_a$ from $G \to G$ are defined as,

$$\lambda_a(x) = ax, \quad \mathfrak{e}_a(x) = xa, x \in G.$$

(ii) Left (right) cancellative and left (right) regular elements: An element $a \in G$ is said to be left (right) cancellative element of the groupoid $(G, \cdot)$ iff λ_a $(\mathfrak{e}_a)$ is an injection and left (right) regular element iff , λ_a $(\mathfrak{e}_a)$ is a bijection.

Lemma 4 of [19] states that: *Let $(G, \cdot)$ be and entropic groupoid and $f \in G$ a left and $g \in G$ a right regular element of $(G, \cdot)$ such that ff is a left and gg is a right cancellative element of $(G, \cdot)$. Then, $(G, +)$ is an abelian semigroup with a neutral element, where $+$ is defined as,*

$$a + b = \mathfrak{e}_g^{-1}(a) \cdot \lambda_f^{-1}(b)$$

Further, the main theorem of the text states: *A groupoid $(G, \cdot)$ is entropic and there are a left regular element f and a right regular element g of $(G, \cdot)$ such that ff is left cancellative element and gg is right cancellative element of $(G, \cdot)$ iff there is a commutative semigroup $(G, +)$ with the neutral element such that the identity,*

$$ab = \phi(a) + \psi(b) + h$$

holds, where h is a regular element of $(G, +)$ and ϕ, ψ are two automorphisms of $(G, +)$ such that $\phi \circ \psi = \psi \circ \phi$.
Hence, in order to design an algorithm for an attack based on the abovementioned lemma or the theorem, an attacker would first need to search over all the elements of the magma to look for those which are left/right regular. Again, if the entropic groupoid is huge, this method will require substantial time and effort. Additionally, there is not always a gurantee that the entropic magmas will possess such elements. [2] admits that their efficiency has not yet been determined.
Finally, as an addition to our list of cryptographically suitable properties, we can include the condition that the presence of regular elements in these entropic magmas must preferably be rare.

Conclusion

While the absence of commutativity and associativity in entropoids prevent group-theoretic attacks, the scope for fast exponentiation of non-associative power indices make them suitable for use in various cryptographic primitives. The knowledge of a hidden abelian group within the structure of entropoids does pose threats and demands some alteration in its operations. The construction of multi-dimensional entropic operations (which are not always quasigroup operations) serves as a better shield. One way to make use of these algebraic structures or higher-order quasigroups generated as a result of these modifications is to use our proposed list of cryptographically important properties as a cheat-sheet to check for their compatibility in real-life applications. Additionally, it would be an interesting research problem to develop new cryptanalytic attacks that can be applied with the aim of improving the security of these schemes. In light of the recent updates, deriving stronger conditions (like minimizing the number of regular elements) in the entropic magmas could further aid attack resistance. We propose to take these as a part of our future work. We expect this paper and its elaborate discussions to be a useful tool for advancing the area of quasigroup-based cryptography.

Acknowledgements: We would like to thank Lorenz Panny for notifying and discussing the recent updates in his paper with us.

Bibliography

1. D. Gligoroski, *Entropoid Based Cryptography*, IACR Cryptology ePrint Archive 2021/469, 2021, https://ia.cr/2021/469.

2. L. Panny, *Entropoid-based cryptography is group exponentiation in disguise*, 2021, https://eprint.iacr.org/2021/583.

3. K. Toyoda, *On axioms of linear functions*, In: Proceedings of the Imperial Academy 17.7(1941), pp. 221–227.

4. K. Toyoda, *On Axioms of Mean Transformations and Automorphic Transformations of Abelian Groups*, Tôhoku Math. Journal, 47 (1940), pp. 239-251.

5. D. C. Murdoch, *Quasi-Groups Which Satisfy Certain Generalized Associative Laws*, In: American Journal of Mathematics 61.2 (1939), pp. 509–522.

6. R. H. Bruck, *Some Results in the Theory of Quasigroups*, In: Transactions of the American Mathematical Society 55.1 (1944), pp. 19-52.

7. D. Gligoroski, *Rebuttal to claims in Section 2.1 of the ePrint report 2021/583 "Entropoid-based cryptography is group exponentiation in disguise"*, https://ia.cr/2021/896, 2021.

8. V. A. Artamonov, *Applications of Quasigroups to Cryptography*, Sarajevo Journal of Mathematics, Vol.14 (27), No.2, (2018), pp. 191-205, https://www.anubih.ba/Journals/vol.14,no-2,y18/08_1303_V.A.%20Artamonov.pdf.

9. V. A. Artamonov, *Quasigroups and their applications*, Chebyshevskii Sb., 2018, Volume 19 (2), pp.111-122.

10. V. A. Artamonov, *On n-ary Polynomially Complete Quasigroups*, New Trends in Algebras and Combinatorics, (2020), pp. 34-40.

11. A. V. Galatentko, A. E. Pankratiev, S. B. Rodin, *Polynomially Complete Quasigroups of Prime Order*, Algebra and Logic, Vol. 57, (2018), pp. 327-335, https://link.springer.com/article/10.1007/s10469-018-9505-6.

12. A.V. Galatenko, A.E. Pankratiev, V.M. Staroverov, *Deciding Cryptographically Important Properties of Finite Quasigroups*, Computer Algebra, 4th International Conference, Moscow 2021, pp. 53-56.

13. V. A. Artamonov, A. Viacheslav, *Automorphisms of Finite Quasigroups with No Subquasigroups*, Vestnik of St Petersburg University. Mathematics. Mechanics. Astronomy, Vol. 7 (65), Issue 2, (2020), pp. 197-209, http://hdl.handle.net/11701/17927.

14. A.V. Galatenko, A.E. Pankratiev, V.M. Staroverov, *Efficient verification of polynomial completeness of quasigroups*, Lobachevskii Journal of Mathematics. 2020. Vol. 41, No. 8., pp. 1444-1453.

15. R. D. Schafer, *An Introduction to Nonassociative Algebras*, The Project Gutenberg EBook (2008), EBook #25156.

16. D. Nager, "Danny" N. Jianfang, *Xifrat - Compact Public-Key Cryptosystems based on Quasigroups*, Cryptology Eprint Archive, 2021/444, ia.cr/2021/444.

17. S. Markovski, *Design of crypto primitives based on quasigroups*, Quasigroups and Related Systems, 23(2015), pp. 41 - 90.

18. S. Markovski, D. Gligoroski, V. Bakeva, *Quasigroup String Processing*, AMS Mathematics Subject Classification, (1991), 20N05, 60J10, 60J20.

19. V. Volenec, *Extension of Toyoda's theorem on entropic groupoids*, Mathematische Nachrichten 102 (1981), pp. 183-188.