Math. Appl. **10** (2021), 37–53
DOI: 10.13164/ma.2021.04

LATIN QUANDLES AND APPLICATIONS TO CRYPTOGRAPHY

ABEDNEGO OROBOSA ISERE, JOHN OLÚSỌLÁ ADÉNÍRAN AND TÈMÍTỌ́PẸ́ GBỌ́LÁHÀN JAIYÉỌLÁ

Abstract. This work investigated some properties of Latin quandles that are applicable in cryptography. Four distinct cores of an Osborn loop (non-diassociative and non-power associative) were introduced and investigated. The necessary and sufficient conditions for these cores to be (i) (left) quandles (ii) involutory quandles (iii) quasi-Latin quandles and (iv) involutory quasi-Latin quandles were established. These conditions were judiciously used to build cipher algorithms for cryptography in some peculiar circumstances.

1. Introduction

Quandles are strictly non-associative binary algebras that are idempotent and distributive. The concept of quandle was introduced independently in 1982 by Joyce [34] and Matveev [42]. However, the notion of self-distributive binary algebra is not new in literature. It appears with many different names [10, 16]. One of the earliest examples is the work of Burstin and Mayer of 1929 [4, 49]. Since then, different authors at different times, have developed this notion either in part or as a whole. For example, Takasaki [52], in 1943, called this notion Kei. Today, Kei is understood as an involutory quandle. In 1955 and 1976, Orrin [45] and Smith [50] worked on self distributive systems and distributive quasigroups respectively. The latter has become known as Latin quandle in the present terminology.

In this paper, we will be focusing more on Latin quandles, particularly those of cyclic type (see Def. 2.18). The foregoing shows that there are many examples of quandles. For a detailed study of variuos examples of quandle structures, the reader can check the following references [1,2,8,10–13,15,34,35]. Quandles provide several invariants of knots, especially the class of connected quandles. It is less surprising, therefore, that researchers pay more attention to connected quandles. Kamada et al. [36] worked on the set of isomorphism classes of quandles of cyclic type. These classes of quandles are not only connected quandles but they also have symmetric and less complicated structures. All quandles of cyclic type are Latin quandles but all Latin quandles are not quandles of cyclic type. Therefore, Latin quandles are a generalization of quandles of cyclic type.

The word Latin quandle comes from Latin squares, which are very popular in combinatorics and Statistics. A Latin square is an $n \times n$ array on n symbols having

MSC (2010): primary 20N05; secondary 57M27.
Keywords: Latin quandles, cyclic type, quasigroups, core of Osborn loop, cryptography.

the property that each symbol appears exactly once in each row and column. A set with a binary operation whose multiplication table is a Latin square is called a quasigroup. Therefore, a quasigroup is a groupoid that gives unique solutions to the equations $a \star x = b$ and $y \star a = b$ whenever two of the elements are specified. A quasigroup that is self-distributive (Ogunrinade [43,44]) is a Latin quandle [49]. However, if there is a two sided identity, the quasigroup is a loop. Loops are also non-associative binary systems. For a comprehensive overview of loops see [7, 23, 47]. Latin quandles and loops are both non-associative quasigroups. While loops are equipped with a unique left and right identity element, Latin quandles are not. Consequently, the concept of a unique inverse element is generally not meaningful in quandles. However, for Latin quandles, the left and right divisions ($(a\backslash b)$ and (b/a)) are unique, which they inherit from their parent structure(quasigroup).

Applications of quasigroups in cryptography are well documented in literature (see [37, 38, 40, 48]). There are many broken designs based on quasigroups, but there are some with perfect crypto properties [40]. The most desirable quasigroups for building crypto primitives are the class of shapeless quasigroups. For details on shapelessness of quasigroup the reader can check [40, 48]. As reported in [49], Moskovich expressed an interesting statement on his blog that "while associativity caters to the classical world of space and time, distributivity is perhaps the setting for the emerging world of information". Latin quandles are distributive quasigroups. Application of these special quasigroups to cryptography has not been discussed. The foregoing is a strong motivation for this work.

There is no gainsaying the fact that ICT is the driving force in this world of information. Consequently, there is a need for cybersecurity. No wonder the African Agenda 2063 and the Global Agenda 2030 and its sustainable Development Goal (SDG) have cybersecurity as their major focus among the 7 aspirations, 20 goals and 39 priority areas, targets and indicators [41]. Cryptology has been highly applauded in literature for being capable of tackling cyberinsecurity [37, 38, 48]. Cryptology encompasses both cryptography (ciphering) and cryptanalysis (deciphering) and looks at the mathematical problems that underlie them. Much of cryptography is mathematics oriented and this is one of the major areas where algebra is finding application nowadays. It ranges from the use of patterns and algorithms to messages, texts, words, signals and other forms of communication [33].

In this paper, we shall recall some basic definitions and results that are relevant to establishing the main results, and also, introduce some new algebraic structures in Section 2 (preliminaries). In Section 3 (main results), we shall study: (i) quandles and involutory quandles formed by the cores of Osborn loops and their applications to cryptography; (ii) Latin quandles of cyclic type and their applications to cryptography since some of them can have long cycles and inverses as Latin quandles, which naturally makes them useful in cryptography.

2. Preliminaries

Definition 2.1. [11] A quandle is a set X with a binary operation $(a, b) \mapsto a \triangleright b$ such that

(1) for any $a \in X$, $a \triangleright a = a$;

(2) for any $a, b \in X$, there is a unique $x \in X$ such that $a = x \rhd b$;
(3) for any $a, b, c \in X$, $(a \rhd b) \rhd c = (a \rhd c) \rhd (b \rhd c)$.

Remark 2.2. Property (1) implies that every element in a quandle has self identity, and thus self inverse. Therefore, the notions of identity and inverse elements are generally not unique in quandles.

Definition 2.3. [11] A rack is a set with a binary operation that satisfies (2) and (3) in Definition 2.1.

Definition 2.4. [16] A quandle $(X, \rhd)$ is commutative if it satisfies the identity

$$x \rhd y = y \rhd x \ \forall \ x, y \in X.$$

Any set X with the operation $x \rhd y = x$ for any $x, y \in X$ is a quandle called the trivial quandle. The trivial quandle of n elements is denoted by T_n.

Definition 2.5. [34] An abelian quandle is a quandle satisfying the identity

$$(w \rhd x) \rhd (y \rhd z) = (w \rhd y) \rhd (x \rhd z).$$

Remark 2.6. Abelian quandles are referred to by some authors as medial quandles.

Definition 2.7. [16, 34] An involutory quandle is a quandle which satisfies

$$(x \rhd y) \rhd y = x.$$

Remark 2.8. An involutory quandle X is also called Kei, particularly if the right translations are involutions: $R_x^2 = id$ for all $x \in X$ [10].

Joyce reported a class of quandles in which the symmetries $S(y)$ are all involutions [49]. For this class of quandles the two operations in a quandle coincide.

Definition 2.9. [16] Given two quandles $(X, \rhd)$ and $(Y, \bullet)$, a map $f : (X, \rhd) \to (Y, \bullet)$ is a quandle homomorphism if

$$f(a \rhd b) = f(a) \bullet f(b) \ \forall \ a, b \in X.$$

If f is a bijection, then f is called an isomorphism, and $(X, \rhd)$ and $(Y, \bullet)$ are said to be isomorphic quandles.

The automorphism group of a quandle $(X, \rhd)$ denoted as Aut (X) is the group of all isomorphisms $\rho : X \to X$. The elements of Aut(X) act on those of X by right action. The inner automorphism group of a quandle $(X, \rhd)$ denoted as Inn(X) is the subgroup of Aut(X) generated by R_x, where $R_x : X \to X$ is the right multiplication by x.

Definition 2.10. An algebraic structure $(Q, \rhd)$ is called a Latin quandle if it obeys the following laws simultaneously:

(i) $x \rhd x = x$ for all $x \in Q$ (idempotent law);
(ii) $a \rhd x = b$ for all $x \in Q$ and a, b specified in Q (left division law);
(iii) $y \rhd a = b$ for all $y \in Q$ and a, b specified in Q (right division law);
(iv) $a \rhd (x \rhd y) = (a \rhd x) \rhd (a \rhd y)$ for all a, x and y in Q (left distributive law);
(v) $(x \rhd y) \rhd a = (x \rhd a) \rhd (y \rhd a)$ for all a, x and y in Q (right distributive law).

If, in addition, a Latin quandle $(Q, \triangleright)$ obeys

(vi) $x \triangleright (x \triangleright y) = y$ for all $x, y \in Q$ (left involutory law),

then, $(Q, \triangleright)$ is called a left involutory Latin quandle.

If, in addition, a Latin quandle $(Q, \triangleright)$ obeys

(vii) $(x \triangleright y) \triangleright y = x$ for all $x, y \in Q$ (right involutory law),

then, $(Q, \triangleright)$ is called an involutory Latin quandle.

Based on the above axioms in Definition 2.10, we introduce the following new structures.

Definition 2.11. Let Q be equipped with an operator $\triangleright$. Then,

(1) a groupoid $(Q, \triangleright)$ will be called a left-Latin quandle if (i), (ii), (iv) and (v) are satisfied;
(2) a groupoid $(Q, \triangleright)$ will be called a right-Latin quandle if (i), (iii), (iv) and (v) are satisfied;
(3) a groupoid $(Q, \triangleright)$ will be called an involutory left-Latin quandle if it is a left-Latin quandle that satisfies both (vi) and (vii);
(4) a groupoid $(Q, \triangleright)$ will be called an involutory right-Latin quandle if it is a right-Latin quandle that satisfies both (vi) and (vii).

Definition 2.12. A Latin quandle $(Q, \circ)$ that obeys the properties

(1) $x \circ (xy) = y$ Left Inverse Property (LIP) is called a LIPQ;
(2) $(yx) \circ x = y$ Right Inverse Property (RIP) is called a RIPQ;
(3) (1) and (2) Inverse Property (IP) is called an IPQ;
(4) $x \circ yx = y$ or $y = xy \circ x$ Cross Inverse Property (CIP) is called a CIPQ;

for all $x, y \in Q$.

Remark 2.13. (1) These properties are being introduced in this paper because of their usefulness in cryptography (see section 3). Recall that in Latin quandles, $x = x^{-1}$ precisely, for every $x \in Q$. The juxtaposition xy means $(x \circ y)$ and it takes precedence during multiplication over other operations when they appear together.

(2) These inverse properties define involutions on a quandle. For example, the left involutory quandle is a LIPQ and the right involutory (Kei) quandle is a RIPQ. Invariably, the CIPQ is a cross involutory quandle.

(3) The smallest Latin quandle is of order three. Behold, this Latin quandle obeys Definition 2.12. That is, it is both an IP and CIP Latin quandle. It is presented below in Table 1 for illustration purposes:

Table 1. The Smallest LIP, RIP and CIP Latin Quandle.

$\circ$	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

For universal algebra consideration [49], $(Q, \star, \backslash)$ is a quandle. But $(Q, \star, \backslash, /)$ is a Latin quandle. Therefore, while quandles are generally equipped with two binary operations, Latin quandles are equipped with three binary operations. This structure is completely devoid of a unique identity element e such that $ae = ea = a \ \forall \ a \in Q$, otherwise, $(Q, \star, e, \backslash, /)$ is a loop.

Definition 2.14. [49] A finite quandle Q is said to be connected if, for every $a, b \in Q$, there exist $x_1, ..., x_n \in Q$ such that $b = x_1 \star (x_2 \star (\ldots (\ldots (x_n \star a))))$.

The above definition therefore means that the inner mapping groups of Q act transitively on Q. Therefore, all Latin quandles are connected quandles, since $L_{x/y}(y) = x$ [3]. That is, if $(Q, \star)$ is a Latin quandle, for all $x, y \in Q$ one can write $(x/y) \star y = x$ or $x = y \star (y \backslash x)$.

Theorem 2.15. [10] *If $(X, \star)$ is a distributive quasigroup, then, for all $a \in X, (X, +, a)$ is a commutative Moufang loop.*

Proposition 2.16. [36] *Let X be a set and assume that there exists a map $S_x : X \to X$ for every $x \in X$. Then, the binary operator $\star$ defined by $y \star x = S_x(y)$ is a quandle structure on X if and only if*

(S1) $\forall \ x \in X, S_x(x) = x$;
(S2) $\forall \ x \in X, S_x$ *is bijective;*
(S3) $\forall \ x, y \in X, S_x \circ S_y = S_{S_{x(y)}} \circ S_x$.

Remark 2.17. This proposition holds for all Latin quandles. It is expanded in Definition 2.10(i–iv).

Definition 2.18. [36] A quandle of order n is said to be of cyclic type if the right translations are of order $n - 1$. In other words, a quandle (X, s) with $\sharp X = n \geq 3$ is said to be of cyclic type if, for every $x \in X, S_x$ acts on $X \backslash \{x\}$ as a cyclic permutation of order $n - 1$, where S_x is a right translation.

Remark 2.19. Definition 2.18 holds for all Latin quandles of cyclic type with $\sharp X = n \geq 3$ except when $n = 4k + 2, k \geq 1$.

Definition 2.20. Let $(Q, \rhd)$ be a Latin quandle such that $a \rhd b = b \rhd^{-1} a$ for all $a, b \in Q$. Then, the Latin quandle $(Q, \rhd^{-1})$ is called a symmetric inverse of $(Q, \rhd)$.

Definition 2.21. Let $(Q, \cdot)$ be a Latin quandle of cyclic type of order n. Then, a Latin quandle $(Q, \star)$ is said to be a symmetric inverse of cyclic type of $(Q, \cdot)$ if, for every $x \in Q$, S_x acts on $Q \backslash \{x\}$ as a cyclic permutation of order $n-1$ implying that the inverse of S_x (denoted here as $S_x^\star$) also acts on $Q \backslash \{x\}$ as a cyclic permutation of order $n - 1$ such that $a \cdot b = b \star a \ \forall \ a, b \in Q$.

Definition 2.22. (Osborn [46]) A loop $(G, \cdot)$ is called an Osborn loop if for all $x, y, z \in G$, it satisfies the identity

$$x(yz \cdot x) = (x \cdot yE_x) \cdot zx \ , where \ E_x = R_x R_{x^\rho} = (L_x L_{x^\lambda})^{-1} = R_x L_x R_x^{-1} L_x^{-1}.$$

Definition 2.23. (Belousov [6]) Let $(G, \cdot)$ be a group, or, more generally, a Bol loop. The binary algebra $(G, \star)$, with

$$x \star y = xy^{-1}x, \tag{2.1}$$

is an involutory quandle called the core of $(G, \cdot)$.

The core operation was first introduced by Bruck [7]. He had earlier shown that the core of a Moufang loop, originally defined as

$$x + y = yx^{-1}y, \tag{2.2}$$

is an involutory (Kei) quandle. Bruck actually proved that isotopic Moufang loops have isomorphic cores ([7, 49]). A beautiful result that links loops with quandles is stated by Stuhl and P. Vojtěchovský that there is a one-to-one correspondence between involutory Latin quandles and uniquely 2-divisible Bruck loops [51].

Equations (2.1) and (2.2) of Definition 2.23 have been used in the past to examine the relationship between a loop and a quandle. In Section 3, these concepts will be generalized and will be used to examine the relationship between an involutory quandle and Osborn loops.

Some other identities that equivalently define an Osborn loop (Definition 2.22) exist in literature and are presented in Theorem 2.24. In fact, Drápal and Kinyon [9] rediscovered some of these identities and some additional ones.

Theorem 2.24. *A loop $(G, \cdot)$ is an Osborn loop if and only if, for all $x, y, z \in G$, it satisfies any of the identities below:*

(1) $(x \cdot zy)x = xy \cdot (yE_x^{-1} \cdot x)$,
(2) $(x^\lambda \backslash y) \cdot zx = x(yz \cdot x)$ ([5, 39]),
(3) $xy \cdot (z/x^\rho) = (x \cdot yz)x$ ([27]),
(4) $x(yx^\lambda \cdot x) \cdot zx = x(yz \cdot x)$ ([9]),
(5) $[x \cdot y(zx^\rho)]x = xy \cdot z$ ([27]),
(6) $x[(x^\lambda y)z \cdot x] = y \cdot zx$ ([28]),
(7) $(x \cdot yz)x = xy \cdot [(x \cdot x^\rho z) \cdot x]$ ([27]),

$x^\rho, x^\lambda \in G$ represent the right and left inverse of $x \in G$, respectively.

The proof of condition (1) follows from Definition 2.22. The proof of the others are found in their corresponding references indicated above.

The smallest Osborn loop is of order 16 [39]. Osborn loops of order $4n$ were constructed in [17–20]. For more works on Osborn loops see [14, 21, 22, 24–26, 29–32, 46].

Although non-trivial Osborn loops (non-Moufang) are not LIP or RIP loops, they display a much weaker form of LIP than RIP.

Algorithm 2.25. ([48, Algorithm 3.1, p. 198]) Let A be a non-empty alphebet, k be a natural number, $u_i, v_i \in A, i \in \{1, \cdots, k\}$. Define a quasigroup $(A, \cdot)$. It is clear that the quasigroup $(A, \backslash)$ is defined in a unique way. Take a fixed element l ($l \in A$), which is called a leader.

Let $u_1u_2 \cdots u_k$ be a k-tuple of letters from A. The authors propose the following ciphering procedure $v_1 = l \cdot u_1, v_i = v_{i-1} \cdot u_i$, $i = 2, \ldots, k$. Therefore, we obtain the following cipher-text $v_1v_2 \cdots v_k$. The enciphering algorithm is constructed in the following way: $u_1 = l \backslash v_1, u_i = v_{i-1} \backslash v_i, i = 2, \ldots, k$.

It was reported that the authors of the above algorithm claim that this cipher is resistant to a brute force attack (exhaustive search) and to a statistical attack. It is also remarked that the cipher which is described in the above algorithm

and its generalizations are now probably the most known used quasigroup based stream-ciphers [48].

Interestingly, most Latin quandles that obey the following properties $x\cdot(x\star y) = y$ and $x\star(x\cdot y) = y$ are either CIPQ, LIPQ or RIPQ of cyclic type (with symmetric inverse, see Definition 2.21) or whose paratrophes can be suitable for cryptographic identities. Subsection 3.2 will be presenting three examples of stream ciphers as applications of these types of Latin quandles in cryptography.

3. Main results

3.1. Quandles formed by cores of Osborn loops and their applications to cryptography

In a generalized manner of (2.1) and (2.2), we now define the core of an Osborn loop (which is neither dissociative nor power associative) in four ways. Let $(G,\cdot)$ be an Osborn loop. If for all $x, y \in G$:

$$\begin{aligned} x +_1 y &= xy^{\rho}\cdot x, \quad (G,+_1) \text{ is called the first core of } (G,\cdot);\\ x +_2 y &= x\cdot y^{\lambda}x, \quad (G,+_2) \text{ is called the second core of } (G,\cdot);\\ x +_3 y &= yx^{\rho}\cdot y, \quad (G,+_3) \text{ is called the third core of } (G,\cdot);\\ x +_4 y &= y\cdot x^{\lambda}y, \quad (G,+_4) \text{ is called the fourth core of } (G,\cdot). \end{aligned}$$

Theorem 3.1. *Let $(G,\cdot)$ be an Osborn loop. Then,*

(1) $(G,+_1)$ *obeys the idempotent law;*
(2) $(G,+_1)$ *has the left division law;*
(3) $(G,+_1)$ *has the left distributive law if and only if*

$$\underbrace{a(bc^{\rho}\cdot b)^{\rho}\cdot a = (ab^{\rho}\cdot a)(ac^{\rho}\cdot a)^{\rho}\cdot(ab^{\rho}\cdot a)}_{LDL1}$$

for all $a,b,c \in G$;

(4) $(G,+_1)$ *has the right distributive law if and only if*

$$\underbrace{(ab^{\rho}\cdot a)c^{\rho}\cdot(ab^{\rho}\cdot a) = (ac^{\rho}\cdot a)(bc^{\rho}\cdot b)^{\rho}\cdot(ac^{\rho}\cdot a)}_{RDL1}$$

for all $a,b,c \in G$;

(5) $(G,+_1)$ *has the left involutory law if and only if*

$$\underbrace{a(ab^{\rho}\cdot a)^{\rho}\cdot a = b}_{LIL1}$$

for all $a,b \in G$;

(6) $(G,+_1)$ *has the cross inverse property law (cross involutory law) if and only if*

$$\underbrace{a(ba^{\rho}\cdot b)^{\rho}\cdot a = b}_{CIL1}$$

for all $a,b \in G$.

Proof. (1) $(G,+_1)$ is idempotent law if and only if $x +_1 x = x \Leftrightarrow xx^{\rho}\cdot x = x \Leftrightarrow e\cdot x = x$.

(2) $(G, +_1)$ has the left division law if and only if there exists $x \in G$ that is unique for any $a, b \in G$ such that $x +_1 a = b$. Note that $x +_1 a = b \Leftrightarrow ax^{\rho} \cdot a = b \Leftrightarrow x = \left[a\backslash(b/a)\right]^{\lambda} \in G$. Also, $x \in G$ is unique.

(3) $(G, +_1)$ has the left distributive law if and only if

$$a +_1 (b +_1 c) = (a +_1 b) +_1 (a +_1 c) \Leftrightarrow a +_1 (bc^{\rho} \cdot b) = (ab^{\rho} \cdot a) +_1 (ac^{\rho} \cdot a) \Leftrightarrow$$
$$a(bc^{\rho} \cdot b)^{\rho} \cdot a = (ab^{\rho} \cdot a)(ac^{\rho} \cdot a)^{\rho} \cdot (ab^{\rho} \cdot a).$$

(4) $(G, +_1)$ has the right distributive law if and only if

$$(a +_1 b) +_1 c = (a +_1 c) +_1 (b +_1 c) \Leftrightarrow (ab^{\rho} \cdot a) +_1 c = (ac^{\rho} \cdot a) +_1 (bc^{\rho} \cdot b) \Leftrightarrow$$
$$(ab^{\rho} \cdot a)c^{\rho} \cdot (ab^{\rho} \cdot a) = (ac^{\rho} \cdot a)(bc^{\rho} \cdot b)^{\rho} \cdot (ac^{\rho} \cdot a).$$

(5) $(G, +_1)$ has the left involutory law if and only if

$$a +_1 (a +_1 b) = b \Leftrightarrow a +_1 (ab^{\rho} \cdot a) = b \Leftrightarrow a(ab^{\rho} \cdot a)^{\rho} \cdot a = b.$$

(6) $(G, +_1)$ has the cross involutory law if and only if

$$a +_1 (b +_1 a) = b \Leftrightarrow a +_1 (ba^{\rho} \cdot b) = b \Leftrightarrow a(ba^{\rho} \cdot b)^{\rho} \cdot a = b.$$

□

Theorem 3.2. *Let $(G, \cdot)$ be an Osborn loop.*

(1) $(G, +_2)$ *obeys the idempotent law;*

(2) $(G, +_2)$ *has the left division law;*

(3) $(G, +_2)$ *has the left distributive law if and only if*

$$\underbrace{a \cdot (b \cdot c^{\lambda}b)^{\lambda}a = (a \cdot b^{\lambda}a) \cdot (a \cdot c^{\lambda}a)^{\lambda}(a \cdot b^{\lambda}a)}_{LDL2}$$

for all $a, b, c \in G$;

(4) $(G, +_2)$ *has the right distributive law if and only if*

$$\underbrace{(a \cdot b^{\lambda}a) \cdot c^{\lambda}(a \cdot b^{\lambda}a) = (a \cdot c^{\lambda}a) \cdot (b \cdot c^{\lambda}b)^{\lambda}(a \cdot c^{\lambda}a)}_{RDL2}$$

for all $a, b, c \in G$;

(5) $(G, +_2)$ *has the left involutory law if and only if*

$$\underbrace{a \cdot (a \cdot b^{\lambda}a)^{\lambda}a = b}_{LIL2}$$

for all $a, b \in G$;

(6) $(G, +_2)$ *has the cross involutory law if and only if*

$$\underbrace{a \cdot (b \cdot a^{\lambda}b)^{\lambda}a = b}_{CIL2}$$

for all $a, b \in G$.

Proof. This is similar to the proof of Theorem 3.1. □

Theorem 3.3. *Let $(G, \cdot)$ be an Osborn loop.*

(1) $(G, +_3)$ *obeys the idempotent law;*

(2) $(G, +_3)$ *has the right division law;*

(3) $(G,+_3)$ *has the right distributive law if and only if*

$$\underbrace{c(ba^\rho \cdot b)^\rho \cdot c = (cb^\rho \cdot c)(ca^\rho \cdot c)^\rho \cdot (cb^\rho \cdot c)}_{RDL3}$$

for all $a,b,c \in G$*;*

(4) $(G,+_3)$ *has the left distributive law if and only if*

$$\underbrace{(cb^\rho \cdot c)a^\rho \cdot (cb^\rho \cdot c) = (ca^\rho \cdot c)(ba^\rho \cdot b)^\rho \cdot (ca^\rho \cdot c)}_{LDL3}$$

for all $a,b,c \in G$*;*

(5) $(G,+_3)$ *has the right involutory law if and only if*

$$\underbrace{b(ba^\rho \cdot b)^\rho \cdot b = a}_{RIL3}$$

for all $a,b \in G$*;*

(6) $(G,+_3)$ *has the cross involutory law if and only if*

$$\underbrace{a(ba^\rho \cdot b)^\rho \cdot a = b}_{CIL3}$$

for all $a,b \in G$*.*

Proof. Note that $x +_1 y = y +_3 x$ for all $x,y \in G$ and so $(G,+_1)$ and $(G,+_3)$ are anti-isotopic groupoids. So, the argument of proof follows from the symmetry of the proof of Theorem 3.1. □

Theorem 3.4. *Let* $(G,\cdot)$ *be an Osborn loop.*

(1) $(G,+_4)$ *obeys the idempotent law;*

(2) $(G,+_4)$ *has the right division law;*

(3) $(G,+_4)$ *has the right distributive law if and only if*

$$\underbrace{c \cdot (b \cdot a^\lambda b)^\lambda c = (c \cdot b^\lambda c) \cdot (c \cdot a^\lambda c)^\lambda (c \cdot b^\lambda c)}_{RDL4}$$

for all $a,b,c \in G$*;*

(4) $(G,+_4)$ *has the left distributive law if and only if*

$$\underbrace{(c \cdot b^\lambda c) \cdot a^\lambda (c \cdot b^\lambda c) = (c \cdot a^\lambda c) \cdot (b \cdot a^\lambda b)^\lambda (c \cdot a^\lambda c)}_{LDL4}$$

for all $a,b,c \in G$*;*

(5) $(G,+_4)$ *has the right involutory law if and only if*

$$\underbrace{b \cdot (b \cdot a^\lambda b)^\lambda b = a}_{RIL4}$$

for all $a,b \in G$*;*

(6) $(G,+_4)$ *has the cross involutory law if and only if*

$$\underbrace{a \cdot (b \cdot a^\lambda b)^\lambda a = b}_{CIL4}$$

for all $a,b \in G$*.*

Proof. Note that $x +_2 y = y +_4 x$ for all $x, y \in G$ and so $(G, +_2)$ and $(G, +_4)$ are anti-isotopic groupoids. So, the argument of proof follows from the symmetry of the proof of Theorem 3.2. □

Remark 3.5. Whether a core of a loop is a quandle or an involutory quandle depends on the properties of the underlying loop. This can be observed by comparing our results in Theorem 3.1, Theorem 3.2, Theorem 3.3 and Theorem 3.4 with the results in Definition 2.23.

Example 3.6. Let $(G, \cdot)$ be a uniquely 2-divisible group or generally, a CIP Osborn loop of order n such that

$$x + y = xy^{-1} \cdot x \quad \forall\ x, y \in G.$$

Then, $(G, +)$ is an involutory Latin quandle of order n.

Proof. By Definition 2.23, $(G, +)$ is a involutory quandle. It is a Latin quandle since it is uniquely 2-divisible. □

Remark 3.7. $(G, +)$ is a LIP Latin quandle and it is of cyclic type of order n whenever $n = 3, 5, 11, 13, 19$, etc. The latter property is rare with the core quandle defined as in equation (2.2).

Corollary 3.8. *Let $(G, \cdot)$ be an Osborn loop. For $i = 1, 2$*

(1) *the following are equivalent:*
   (a) *$(G, +_i)$ is a (left) quandle,*
   (b) *$(G, +_i)$ is a (left) rack,*
   (c) *LDLi is satisfied;*
(2) *$(G, +_i)$ is a (left) involutory quandle if and only if LDLi and LILi are satisfied;*
(3) *$(G, +_i)$ is a left-Latin quandle if and only if LDLi and RDLi are satisfied;*
(4) *$(G, +_i)$ is an involutory left-Latin quandle if and only if LDLi, RDLi, LILi and RILi are satisfied.*

Proof. This follows by Theorem 3.1 and Theorem 3.2. □

Corollary 3.9. *Let $(G, \cdot)$ be an Osborn loop. For $i = 3, 4$*

(1) *the following are equivalent:*
   (a) *$(G, +_i)$ is a quandle,*
   (b) *$(G, +_i)$ is a rack,*
   (c) *RDLi is satisfied;*
(2) *$(G, +_i)$ is an involutory quandle if and only if RDLi and RILi are satisfied;*
(3) *$(G, +_i)$ is a right-Latin quandle if and only if RDLi and RDLi are satisfied;*
(4) *$(G, +_i)$ is an involutory right-Latin quandle if and only if LDLi, RDLi, LILi and RILi are satisfied.*

Proof. This follows from Theorem 3.3 and Theorem 3.4. □

We shall highlight symmetric-key algorithms of how the identities in Theorem 3.1, Theorem 3.2, Theorem 3.3 and Theorem 3.4 can be used for cryptography in some peculiar circumstances.

Algorithm 3.10. (A–B Cryptographic Algorithm with Single Key) A cipher algorithm based on the assumption that $(G, +_1)$ obeys the left involutory law or the cross involutory law. Let $b = \textit{plaintext}$ and $a = \textit{key}$.

Isere–A (Encryption): Do b^ρ and compute the cipher text $ab^\rho \cdot a$. Then, send the key a and $ab^\rho \cdot a$ to the receiver (Jaiyeola).

Jaiyeola–B (Decryption): On receiving a and $ab^\rho \cdot a$, compute $a(ab^\rho \cdot a)^\rho \cdot a$, which gives the plaintext b.

A cipher algorithm based on the cross involutory law or a combination of both is similar.

Algorithm 3.11. (A–A1–A2–A3–A4–B Cryptographic Algorithm with Single Key) A cipher algorithm based on the assumption that $(G, +_1)$ obeys the left involutory law. LIL1 is a cryptographic identity (see [24, 25, Def. 2.2]) of order 6. In [24, 25], 'many receivers' cipher algorithm was discussed in detail and it applies here. That is, information from A (Isere) to B (Jaiyeola) through some other trusted parties (4) who the information is not meant for, but mindful of possible intruders. Based on LIL1, take $b = \textit{plaintext}$ and $a = \textit{key}$.

Algorithm 3.12. (A–B Cryptographic Algorithm with Twin Key) A cipher algorithm based on the assumption that $(G, +_1)$ obeys the right distributive law. Let $c = \textit{plaintext}$ and $(a, b) = \textit{key}$.

Isere–A (Encryption): Do $ac^\rho \cdot a, bc^\rho \cdot b, ab^\rho \cdot a$ and compute the cipher text $D = (ac^\rho \cdot a)(bc^\rho \cdot b)^\rho \cdot (ac^\rho \cdot a)$. Then, send D and $ab^\rho \cdot a$ to the receiver (Jaiyeola).

Jaiyeola–B (Decryption): On receiving D and $ab^\rho \cdot a$, it should be noted that $D = (ab^\rho \cdot a)c^\rho \cdot (ab^\rho \cdot a)$ based on RDL1. Thus, with the knowledge of $ab^\rho \cdot a$, compute

$$c = \Big[(ab^\rho \cdot a) \backslash \big(D/(ab^\rho \cdot a)\big)\Big]^\lambda$$

to get the plaintext.

Algorithm 3.13. (A–B Cryptographic Algorithm with Twin Key) A cipher algorithm based on the assumption that $(G, +_1)$ obeys the left distributive law. Let $c = \textit{plaintext}$ and $(a, b) = \textit{key}$.

Isere–A (Encryption): Do $ac^\rho \cdot a, ab^\rho \cdot a$ and compute the cipher text $E = (ab^\rho \cdot a)(ac^\rho \cdot a)^\rho \cdot (ab^\rho \cdot a)$. Then, send E and (a, b) to the receiver (Jaiyeola).

Jaiyeola–B (Decryption): On receiving E and (a, b), it should be noted that $E = a(bc^\rho \cdot b)^\rho \cdot a$ based on LDL1. Thus, with the knowledge of (a, b), compute

$$c = \left[b \backslash \left(\Big[a \backslash (E/a)\Big]^\lambda / b\right)\right]^\lambda$$

to get the plaintext.

Similarly, cipher algorithms based on the assumption that $(G, +_i)$ obeys the cross involutory law (CILi); the right and left involutory laws (RILi and LILi); the right distributive law (RDLi); the left distributive law (LDLi) can be highlighted when $i = 2, 3, 4$.

3.2. Latin quandles of cyclic type and their applications to cryptography using symmetric inverse algorithms

Lemma 3.14. *Let $(Q, \triangleright)$ be a Latin quandle of cyclic type such that $a \triangleright (a \backslash b) = b$ and $a \backslash (a \triangleright b) = b$. Then, $(Q, \backslash)$ is a Latin quandle of cyclic type if $(Q, \triangleright)$ is a CIPQ.*

Proof. We need to show that $(Q, \backslash)$ is a symmetric inverse of cyclic type of $(Q, \triangleright)$ since $(Q, \triangleright) \neq (Q, \backslash)$ (see Definition 2.20 and Definition 2.21). Recall that in $(Q, \triangleright)$ it holds that

$$a \triangleright (a \backslash b) = b$$

and since $(Q, \triangleright)$ is a CIPQ

$$a \triangleright (b \triangleright a) = b.$$

Then,

$$a \backslash b = b \triangleright a.$$

Therefore, $(Q, \backslash)$ is a symmetric inverse of cyclic type of $(Q, \triangleright)$. □

Remark 3.15. A symmetric inverse of a CIPQ is again a CIPQ.

Theorem 3.16. *Let $(Q, \triangleright)$ be a Latin quandle of cyclic type such that $a \triangleright b = b \triangleright^{-1} a$ holds for all $a, b \in Q$. Then, $(Q, \triangleright^{-1})$ is a Latin quandle of cyclic type if $(Q, \triangleright^{-1}) = (Q, \backslash)$.*

Proof. The expression $a \triangleright b = b \triangleright^{-1} a$, where $a \in Q$ is acting from the left in $a \triangleright b$ and acting from the right in $b \triangleright^{-1} a$, means that $(Q, \triangleright^{-1})$ is a symmetric inverse of cyclic type of $(Q, \triangleright)$. The remaining part of the proof follows from Lemma 3.14. □

Theorem 3.17. *Let $(Q, \cdot)$ be a Latin quandle of cyclic type that is not a CIPQ such that $a \backslash (a \cdot b) = b$ and $a \cdot (a \backslash b) = b$ for all $a, b \in Q$, then $(Q, \backslash)$ is a Latin quandle that is not of cyclic type.*

Proof. Suppose $(Q, \backslash)$ is a Latin quandle of cyclic type. Then, by Theorem 3.16 we need to show that $(Q, \backslash)$ is a symmetric inverse (of cyclic type) of $(Q, \cdot)$. That is,

$$a \cdot b = b \backslash a.$$

Then,

$$b \cdot (a \cdot b) = b \cdot (b \backslash a) = a.$$

Thus, $(Q, \cdot)$ is a CIPQ (a contradition). Therefore, $(Q, \backslash)$ is a Latin quandle that is not of cyclic type. □

Remark 3.18. Theorem 3.17 is a counter. $(Q, \cdot)$ is a Latin quandle of cyclic type and yet $(Q, \backslash)$ is not a symmetric inverse of $(Q, \cdot)$ nor a Latin quandle of cyclic type.

The following three examples describe symmetric inverse algorithms applied to various Latin quandles.

Example 3.19. Let $(Q, \triangleright)$ be a Latin quandle of cyclic type containing alphabets as elements, and let n be a natural number, $u_i, v_i \in Q, i \in \{1, \ldots, n\}$. The Latin quandle $(Q, \triangleright^{-1})$ is the symmetric inverse of $(Q, \triangleright)$ based on Theorem 3.16. Take a fixed element k ($k \in Q$), which is called a leader. Let $u = u_1 u_2 \ldots u_n$ be the plaintext containing elements in Q.

Let the Latin quandle $(Q, \triangleright)$ be defined by the Cayley Table 2 with the ciphering procedure as $v_1 = k \triangleright u_1, v_i = v_{i-1} \triangleright u_i$ and deciphering procedure as $u_1 = k \triangleright^{-1} v_1$ and $u_i = v_{i-1} \triangleright^{-1} v_i \; \forall \; i = 2, ..., n$. Then, $(Q, \triangleright^{-1})$ has the following Cayley Table 3.

Table 2. Latin Quandle (CIPQ) of Cyclic Type.

$\triangleright$	a	b	c	d
a	a	d	b	c
b	c	b	d	a
c	d	a	c	b
d	b	c	a	d

Table 3. Latin Quandle (CIPQ) of Cyclic Type.

$\triangleright^{-1}$	a	b	c	d
a	a	c	d	b
b	d	b	a	c
c	b	d	c	a
d	c	a	b	d

Let $k = a$ and the plaintext is $u = adabaccada$. Then the cipher text is $v = acdcdabcbc$. Applying the decoding function as provided in the example on v, we have $u = adabaccada$.

Example 3.20. Let $(Q, \triangleright)$ be a Latin quandle of cyclic type containing alphabets as elements, and let n be a natural number, $u_i, v_i \in Q, i \in \{1, \ldots, n\}$. The Latin quandle $(Q, \triangleright^{-1})$ is the symmetric inverse of $(Q, \triangleright)$ based on Theorem 3.17. Take a fixed element k ($k \in Q$), which is called a leader. Let $u = u_1 u_2 \ldots u_n$ be the plaintext containing elements in Q.

Let the Latin quandle $(Q, \triangleright)$ be defined by the Cayley Table 4 with the ciphering procedure as $v_1 = k \triangleright u_1, v_i = v_{i-1} \triangleright u_i$ and deciphering procedure as $u_1 = v_1 \triangleright^{-1} k$ and $u_i = v_i \triangleright^{-1} v_{i-1} \; \forall \; i = 2, \ldots, n$. Then, $(Q, \triangleright^{-1})$ has the following Cayley Table 5. Let $k = a$ and the plaintext is $u = adabaccada$. Then the cipher text is

Table 4. Latin Quandle (LIPQ) of Cyclic Type.

$\triangleright$	a	b	c	d	e
a	a	e	d	c	b
b	c	b	a	e	d
c	e	d	c	b	a
d	b	a	e	d	c
e	d	c	b	a	e

Table 5. Latin Quandle (RIPQ).

$\triangleright^{-1}$	a	b	c	d	e
a	a	c	e	b	d
b	e	b	d	a	c
c	d	a	c	e	b
d	c	e	b	d	a
e	b	d	a	c	e

$v = acecebaace$. Applying the decoding function as provided in the example on v, we have $u = adabaccada$

.

Example 3.21. Let $(Q, \triangleright)$ be a Latin quandle containing alphabets as elements, and let n be a natural number, $u_i, v_i \in Q, i \in \{1, \ldots, n\}$. The Latin quandle $(Q, \triangleright^{-1})$ is the symmetric inverse of $(Q, \triangleright)$ based on Theorem 3.16. Take a fixed element k ($k \in Q$), which is called a leader. Let $u = u_1 u_2 \ldots u_n$ be the plaintext containing elements in Q.

Let the Latin quandle $(Q, \triangleright)$ be defined by the Cayley Table 6 with the ciphering procedure as $v_1 = k \triangleright u_1, v_i = v_{i-1} \triangleright u_i$ and deciphering procedure as $u_1 = k \triangleright^{-1} v_1$ and $u_i = v_{i-1} \triangleright^{-1} v_i \ \forall \ i = 2, \ldots, n$. Then, $(Q, \triangleright^{-1})$ has the following Cayley Table 7. Then, $(Q, \triangleright^{-1})$ has the following Cayley multiplication table:

Table 6. A CIPQ that is not of Cyclic Type.

$\triangleright$	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
a	a	c	d	b	i	k	l	j	m	o	p	n	e	g	h	f
b	d	b	a	a	l	j	i	k	p	n	m	o	h	f	e	g
c	b	d	c	a	j	l	k	i	n	p	o	m	f	h	g	e
d	c	a	b	d	k	i	j	l	o	m	n	p	g	e	f	h
e	m	o	p	n	e	g	h	f	a	c	d	b	i	k	l	j
f	p	n	m	o	h	f	e	g	d	b	a	c	l	j	i	k
g	n	p	o	m	f	h	g	e	b	d	c	a	j	l	k	i
h	o	m	n	p	g	e	f	h	c	a	b	d	k	i	j	l
i	e	g	h	f	m	o	p	n	i	k	l	j	a	c	d	b
j	h	f	e	g	p	n	m	o	l	j	i	k	d	b	a	c
k	f	h	g	e	n	p	o	m	j	l	k	i	b	d	c	a
l	g	e	f	h	o	m	n	p	k	i	j	l	c	a	b	d
m	i	k	l	j	a	c	d	b	e	g	h	f	m	o	p	n
n	l	j	i	k	d	b	a	c	h	f	e	g	p	n	m	o
o	j	l	k	i	b	d	c	a	f	h	g	e	n	p	o	m
p	k	i	j	l	c	a	b	d	g	e	f	h	o	m	n	p

Table 7. A CIPQ that is not of Cyclic Type.

$\triangleright^{-1}$	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
a	a	d	b	c	m	p	n	o	e	h	f	g	i	l	j	k
b	c	b	d	a	o	n	p	m	g	f	h	e	k	j	l	i
c	d	a	c	b	p	m	o	n	h	e	g	f	l	i	k	j
d	b	c	a	d	n	o	m	p	f	g	e	h	j	k	i	l
e	i	l	j	k	e	h	f	g	m	p	n	o	a	d	b	c
f	k	j	l	i	g	f	h	e	o	n	p	m	c	b	d	a
g	l	i	k	j	h	e	g	f	p	m	o	n	d	a	c	b
h	j	k	i	l	f	g	e	h	n	o	m	p	b	c	a	d
i	m	p	n	o	a	d	b	c	i	e	j	k	e	h	f	g
j	o	n	p	m	c	b	d	a	k	j	e	i	g	f	h	e
k	p	m	o	n	d	a	c	b	e	i	k	j	h	e	g	f
l	n	o	m	p	b	c	a	d	j	k	i	l	f	g	e	h
m	e	h	f	g	i	l	j	k	a	d	b	c	m	p	n	o
n	g	f	h	e	k	j	e	i	c	b	d	a	o	n	p	m
o	h	e	g	f	l	i	k	j	d	a	c	b	p	m	o	n
p	f	g	e	h	j	k	i	l	b	c	a	d	n	o	m	p

Let $k = a$ and the plaintext is $u = adabaccada$. Then the cipher text is $v = abdaadbddc$. Applying the decoding function as provided in the example on v, we have $u = adabaccada$

Remark 3.22. The algorithms of symmetric inverse highlighted in the three examples above are based on Theorem 3.16 and Theorem 3.17. Notably, the

deciphering procedure in Example 3.20 is slightly different from the other two examples. This type of deciphering procedure is suitable for Latin quandles that are not CIPQs. Observe also that, in Example 3.20, $(Q, \triangleright)$ is a LIPQ of cyclic type while $(Q, \triangleright^{-1})$, a paratrophe of $(Q, \triangleright)$ is a RIPQ but not a Latin quandle of cyclic type. Thus, Example 3.20 is a counter to Example 3.19.

4. Conclusion

This work examined the properties of Latin quandles that are applicable in cryptography. Moreover, the relationship between the cores of Osborn loops and involutory quandles were established. The necessary and sufficient conditions for these cores of Osborn loops to be various quandle structures were also established. These conditions were judiciously used to build cipher algorithms for cryptography. The results in Theorem 3.1, Theorem 3.2, Theorem 3.3 and Theorem 3.4 are remarkable contributions in quandle theory and in the application of Osborn loops. The properties of Latin quandles that are applicable to cryptography were stated in Definition 2.12 and generalized in Theorem 3.16 and Theorem 3.17. Three practical examples of how these properties can be applied in cryptography were illustrated in Example 3.19, Example 3.20 and Example 3.21. The results show that the cipher text built from Example 3.20 is stronger than the cipher text from Example 3.21. What makes the difference is the length of the cycles, not necessarily the order of the quandle. Latin quandles of cyclic type of order n have cycles of length $n-1$. For example, the Latin quandle of order 5 used in Example 3.20 is of cyclic type of length four while a Latin quandle of order 16 (that is not of cyclic type) used in Example 3.21 has cycles of length three. Hence, the cipher text from the latter is just a mere shuffling of the alphabets a, b, c, d of the plaintext, whereas the Latin quandle in example 3.20 has a much stronger cipher text with a letter replaced entirely by another. Thus, the longer the cycle the stronger the cipher text. Therefore, cipher texts built from Latin quandles of cyclic type are much stronger than those from Latin quandles that are not of cyclic type.

Acknowledgment. The authors wish to thank the anonymous referee whose comments and recommendations improved the original version of this manuscript.

References

[1] W. Alexander and G. B. Briggs, *On types of knotted curves*, Annals of Math. **28** (1926), 562–586.

[2] V. G. Bardakov, P. Dey and M. Singh, *Automorphism Groups of Quandles Arising from Groups*, Monatsh. Math. **184** (2017), 519–530.

[3] M. Bonatto and P. Vojtěchovský, *Simply connected Latin quandles*, J. Knot Theory Ramifications **27** (2018), Article ID 1843006, 32 pp.

[4] C. Burstin and W. Mayer, *Distributive Gruppen von endlicher Ordnung*, J. Reine Angew. Math. **160** (1929), 111–130.

[5] A. S. Basarab and A. I. Belioglo, *Osborn UAI-loops*, Mat. Issled. **51** (1979), 8–13.

[6] V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Russian, Izdat. "Nauka", Moscow, 1967.

[7] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, Berlin–Göttingen–Heidelberg, 1966.

[8] N. N. Didurik and V. A. Shcherbacov, *On definition of CI-quasigroup*, ROMAI J. **13** (2017), 55–58.
[9] A. Drápal and M. Kinyon, *Normality, nuclear squares and Osborn identities*, Comment. Math. Univ. Carolin. **61** (2020), 481–500.
[10] M. Elhamdadi, *Distributivity in quandles and quasigroups*, in: A. Makhlouf, E. Paal, S. D. Silvestrov and A. Stolin (eds.), Algebra, Geometry and Mathematical Physics, Springer Proceedings in Mathematics and Statistics **85**, Springer-Verlag, Heidelberg, 2014, pp. 325–340.
[11] M. Elhamdadi, J. Macquarrie and R. Restrepo, *Automorphism groups of quandles*, J. Algebra Appl. **11** (2012), Article ID 1250008, 9 pp.
[12] M. Elhamdadi and S. Nelson, *Quandles: An Introduction to the Algebra of Knots*, Student Mathematical Library **74**, AMS, Providence, RI, 2015.
[13] B. Ho and S. Nelson, *Matrices and finite quandles* , Homology Homotopy Appl. **7** (2005), 197–208.
[14] E. D. Huthnance, *A Theory of Generalised Moufang Loops*, Ph.D. thesis, Georgia Institute of Technology, 1968.
[15] Indu R. U. Churchill, M. Elhamdadi, M. Hajij and S. Nelson, *Singular knots and involutive quandles*, J. Knot Theory Ramifications **26** (2017), Article ID 1750099, 14 pp.
[16] A. O. Isere, *A quandle of order 2n and the concept of quandles isomorphism*, J. Niger. Math. Soc. **39** (2020), 155–166.
[17] A. O. Isere, J. O. Adéníran and A. R. T. Solarin, *Somes examples of finite Osborn loops*, J. Niger. Math. Soc. **31** (2012), 91–106.
[18] A. O. Isere, S. A. Akinleye and J. O. Adéníran, *On Osborn loops of order* $4n$, Acta Univ. Apulensis, Math. Inform. **37** (2014), 31–44.
[19] A. O. Isere, J. O. Adéníran and T. G. Jaiyéọlá, *Generalized Osborn loops of order* $4n$, Acta Univ. Apulensis, Math. Inform. **43** (2015), 19–31.
[20] A. O. Isere, J. O. Adéníran and T. G. Jaíyéọlá, *Classification of Osborn loops of order 4n*, Proyecciones **38** (2019), 31–47.
[21] A. O. Isere, J. O. Adéníran and T. G. Jaíyéọlá, *Holomorphy of Osborn loops*, An. Univ. Vest Timiş. Ser. Mat.–Inform. **53** (2015), 81–98.
[22] A. O. Isere, J. O. Adéníran and A. A. A. Agboola, *Representations of finite Osborn loops*, J. Niger. Math. Soc. **35** (2016), 381–389.
[23] T. G. Jaíyéọlá, *A Study of New Concepts in Smarandache Quasigroups and Loops*, ProQuest Information and Learning (ILQ), Ann Arbor, USA, 2009.
[24] T. G. Jaiyéọlá, *On three cryptographic identities in left universal Osborn loops*, J. Discret. Math. Sci. Cryptogr. **14** (2011), 33–50.
[25] T. G. Jaiyéọlá, *On two cryptographic identities in universal Osborn loops*, J. Discret. Math. Sci. Cryptogr. **16** (2013), 95–116.
[26] T. G. Jaiyéọlá and E. Effiong, *Basarab loop and its variance with inverse properties*, Quasigroups Relat. Syst. **26** (2018), 229–238.
[27] T. G. Jaiyéọlá and J. O. Adéníran, *Not every Osborn loop is universal*, Acta Math. Acad. Paedagog. Nyiregyhaziensis **25** (2009), 189–190.
[28] T. G. Jaiyéọlá and J. O. Adéníran, *New identities in universal Osborn loops*, Quasigroups Relat. Syst. **17** (2009), 55–76.
[29] T. G. Jaiyéọlá and J. O. Adéníran, *Loops that are isomorphic to their Osborn loop isotopes (G-Osborn loops)*, Octogon **19** (2011), 328–348.
[30] T. G. Jaiyéọlá and J. O. Adéníran, *On another two cryptographic identities in universal Osborn loops*, Surv. Math. Appl. **5** (2010), 17–34.
[31] T. G. Jaiyéọlá and J. O. Adéníran, *A new characterization of Osborn–Buchsteiner loops*, Quasigroups Relat. Syst. **20** (2012), 233–238.
[32] T. G. Jaiyéọlá , J. O. Adéníran and A. R. T. Sòlárìn, *Some necessary conditions for the existence of a finite Osborn loop with trivial nucleus*, Algebras Groups Geom. **28** (2011), 363–380.
[33] A. Joseph Raphael and V. Sundaram, *Secured communication through Fibonacci numbers and unicode symbols*, International Journal of Scientific and Engineering Research **3** (2012), 490–494.

[34] D. Joyce, *A classifying invariant of knots, the knot quandle* , J. Pure Appl. Alg. **23** (1982), 37–66.
[35] D. Joyce, *Simple quandles*, J. Alg. **79** (1982), 307–318.
[36] S. Kamada, H. Tamaru and K. Wada, *On classification of quandles of cycle type*, Tokyo J. Math. **39** (2016), 157–171.
[37] A. D. Keedwell, *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Comb. **20** (1999), 241–250.
[38] A. D. Keedwell and V. A. Shcherbacov, *On m-inverse loops and quasigroups with a long inverse cycles*, Australas. J. Comb. **26** (2002), 99–119.
[39] M. K. Kinyon, *A survey of Osborn loops*, Mile High Conference on Quasigroups, Loops, and Nonassociative Systems (plenary talk), University of Denver, Denver, Colorado, 2005.
[40] S. Markovski, *Design of crypto primitives based on quasigroups* , Quasigroups Relat. Syst. **23** (2015), 41–90.
[41] M. Passalacqua, *Cybersecurity & sustainable development*, https://www.linkedin.com/pulse/cybersecurity-sustainable-development-massimiliano-passalacqua, June 7, 2018.
[42] S. Matveev, *Distributive groupoids in knot theory*, Math. USSR, Sb. **47** (1984), 73–83.
[43] S. O. Ogunrinade, S. O. Ajala, J. O. Olaleru and T. G. Jaiyéọlá, *Holomorph of self-distributive quasigroup with key laws*, International Journal of Mathematical Analysis and Optimization: Theory and Applications **2019** (2019), 426-–432.
[44] S. O. Ogunrinade, S. O Ajala, Y. T. Oyebo and T. G. Jaiyéọlá, *A Class of Distributive Quasigroup and Its Parastrophes*, J. Niger. Assoc. Math. Phys. **39** (2017), 1–8.
[45] F. Orrin, *Symmetric and self-distributive systems*, Amer. Math. Monthly **62** (1955), 699–707.
[46] J. M. Osborn, *Loops with the weak inverse property*, Pac. J. Math. **10** (1961), 295–304.
[47] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990.
[48] V. A. Shcherbacov, *Quasigroups in cryptology*, Comput. Sci. J. Mold. **17** (2009), 193–228.
[49] D. A. Stanovský, *A guide to self-distributive quasigroups or Latin quandles*, Quasigroups Relat. Syst. **23** (2015), 91–128.
[50] J. D. H. Smith, *Finite distributive quasigroups*, Math. Proc. Cambridge Philos. Soc. **80** (1976), 37–41.
[51] I. Stuhl and P. Vojtěchovský, *Enumeration of involutory Latin quandles, Bruck loops and commutative automorphic loops of odd prime power order*, in: P. Vojtěchovský *et al.* (eds.), Nonassociative Mathematics and its Applications, Fourth Mile High Conference on Nonassociative Mathematics, Denver, CO, USA, July 29–August 5, 2017, Contemp. Math. **721**, AMS, Providence, RI, 2019, pp. 261–276.
[52] M. Takasaki, *Abstractions of symmetric transformations*, Tôhoku Math. J. **49** (1943), 145–207.

Abednego Orobosa Isere, Department of Mathematics, Ambrose Alli University, Ekpoma 310001, Nigeria
e-mail: abednis@yahoo.co.uk, isereao@aauekpoma.edu.ng

John Olúsọlá Adéníran, Department of Mathematics, Federal University of Agriculture, Abeokuta 110101, Nigeria
e-mail: ekenedilichineke@yahoo.com, adeniranoj@funaab.edu.ng

Tèmítọ́pẹ́ Gbọ́láhàn Jaiyéọlá, Department of Mathematics, Obafemi Awolowo University, Ile Ife 220005, Nigeria
e-mail: jaiyeolatemitope@yahoo.com, tjayeola@oauife.edu.ng