*Discussiones Mathematicae*
*General Algebra and Applications xx (xxxx) 1–16*

# CRYPTO-AUTOMORPHISM GROUP OF SOME QUASIGROUPS

Yakub Tunde Oyebo

*Department of Mathematics*
*Lagos State University Ojo*
*Lagos State, 102101 Nigeria*

**e-mail:** oyeboyt@yahoo.com, yakub.oyebo@lasu.edu.ng

Benard Osoba[1]

*Bells University of Technology*
*Ota, Ogun State, Nigeria*

**e-mail:** benardomth@gmail.com

and

Tèmítọ́pẹ́ Gbọ́láhàn Jaíyéọlá

*Department of Mathematics*
*Obafemi Awolowo University*
*Ile Ife 220005, Nigeria*

**e-mail:** jaiyeolatemitope@yahoo.com, tjayeola@oauife.edu.ng

## Abstract

In quasigroup and loop theory, a pseudo-automorphism (with single companion) is known to generalize automorphism. In this work, the set of crypto-automorphisms (with twin companion) of a quasigroup with right and left identity elements were shown to form a group. For a quasigroup with right and left identity elements, some results on autotopic characterizations of crypto-automorphisms were established and used to deduce some subgroups of the crypto-automorphism group of a middle Bol loop. The crypto-automorphism group and Bryant-Schneider group (this has been used in the study of the isotopy-isomorphy of some varieties of loops e.g. Bol loops, Moufang loops, Osborn loops) of a loop were found to coincide.

**Keywords:** quasigroup, loop, crypto-automorphism, Bryant-Schneider group.

[1]All correspondence to be addressed to this author.

**2010 Mathematics Subject Classification:** Primary 20N05; Secondary 08A05.

# 1 Introduction

## 1.1 Quasigroup and Loop

Let '$Q$' be a non -empty set. Defining a binary operation " $\cdot$ " on $Q$. If $x \cdot y \in Q$ for all $x, y \in Q$, then the pair $(Q, \cdot)$ is called a groupoid or Magma. If the system of equations: $a \cdot x = b$ and $y \cdot a = b$ have a unique solutions in $Q$ $\forall x, y$ respectively, then $(Q, \cdot)$ is called a quasigroup. Let $(Q, \cdot)$ be a quasigroup and there exist a unique element $e \in Q$ called the identity element such that for all $x \in Q, x \cdot e = e \cdot x = x$, then $(Q, \cdot)$ is called a loop. We write $xy$ instead of $x \cdot y$ and stipulat that $\cdot$ has lower priority than juxtaposition among factors to be multiplied. Let $(Q, \cdot)$ be a groupoid and "a" be a fixed element in $Q$, then the left $L_a$ and right $R_a$ translations are respectively defined by $xL_a = a \cdot x$ and $xR_a = x \cdot a$. Also, the mapping $P_x : Q \to Q$ defined by $y \backslash x = yP_x$ and $x/y = yP_x^{-1}$ are called middle translations.

The symmetric group of $SYM(Q)$ of $Q$ is defined as

$SYM(Q) = \{U : Q \to Q \mid U \text{ is a permutation or bijection}\}$. For a loop $(Q, \cdot)$, the group generated by its left and right translations is called the multiplication group $Mult(Q, \cdot) \leq SYM(Q)$.

For any non-empty set $Q$, the set of all permutations on $Q$ forms a group $SYM(Q)$ called the symmetric group of $Q$. Let $(Q, \cdot)$ be a loop and let $A, B, C \in SYM(Q)$. If

$$xA \cdot yB = (x \cdot y)C \ \forall \ x, y \in Q$$

then the triple $(A, B, C)$ is called an autotopism and such triples form a group $AUT(Q, \cdot)$ called the autotopism group of $(Q, \cdot)$. If $A = B = C$, then $A$ is called an automorphism of $(Q, \cdot)$ which form a group $AUM(Q, \cdot)$ called the automorphism group of $(Q, \cdot)$.

**Definition 1.1.** Let $(Q, \cdot)$ be a loop.

1. A mapping $\theta \in SYM(Q, \cdot)$ is a right special map for $Q$ if there exist $f \in Q$ so that $(\theta, \theta L_f^{-1}, \theta) \in AUT(Q, \cdot)$.

2. A mapping $\theta \in SYM(Q, \cdot)$ is a left special map for $Q$ if there exist $g \in Q$ so that $(\theta R_g^{-1}, \theta, \theta) \in AUT(Q, \cdot)$.

3. A mapping $\theta \in SYM(Q)$ such that $(\theta R_g^{-1}, \theta L_f^{-1}, \theta) \in AUT(Q, \cdot)$ for some $f, g \in Q$, then $BS(Q, \cdot)$ is called the Bryant-Schneider group of the loop $(Q, \cdot)$.

From this Definition 1.1, it is clearly seen that

$$(\theta R_g^{-1}, \theta L_f^{-1}, \theta) = (\theta, \theta, \theta)(R_g^{-1}, L_f^{-1}, I),$$

which implies that $\theta$ is an isomorphism of $(Q, \cdot)$ onto some $f, g$-isotope of it.

**Theorem 1.1** [21]**.** Let the set $BS(Q, \cdot) = \{\theta \in SYM(Q, \cdot) : \exists f, g \in Q \ni (\theta R_g^{-1}, \theta L_f^{-1}, \theta) \in AUT(Q, \cdot)\}$, then $BS(Q, \cdot) \leq SYM(Q, \cdot)$

**Theorem 1.2** (Pflugfelder [37])**.** Let $(G, \cdot)$ and $(H, \circ)$ be two isotopic loops. For some $f, g \in G$, there exists an $f, g$-principal isotope $(G, *)$ of $(G, \cdot)$ such that $(H, \circ) \cong (G, *)$.

Jaiyéọlá [22] and Jaiyéọlá et al. [26, 27] used the Bryant-Schneider group to study Smarandache loop, Osborn loop and its universality. For more on quasigroups and loops, see Jaiyéọlá [23], Shcherbacov [38] and Pflugfelder [37].

### 1.2 Middle Bol Loop

Middle Bol loop (MBL) was first studied in the work of Belousov [6], where he gave the second identity in Definition 1.2(2) characterizing loops that satisfy the universal anti-automorphic inverse property. After this beautiful characterization by Belousov and the laying of foundations for a classical study of this structure, Gvaramiya in [17] proved that a loop $(Q, \circ)$ is middle Bol if there exist a right Bol loop $(Q, \cdot)$ such that $x \circ y = (y \cdot xy^{-1})y$ for all $x, y, \in Q$. If $(Q, \circ)$ is a middle Bol loop and $(Q, \cdot)$ is the corresponding right Bol loop, then

$$x \circ y = y^{-1} \backslash x \qquad \text{and} \qquad x \cdot y = y // x^{-1} \tag{1}$$

where for every $x, y \in Q$ '//' is the left division in $(Q, \circ)$.

Also, if $(Q, \circ)$ is a middle Bol loop and $(Q, \cdot)$ is the corresponding left Bol loop, then

$$x \circ y = x / y^{-1} \qquad \text{and} \qquad x \cdot y = x // y^{-1} \tag{2}$$

where '//' is the left division in $(Q, \circ)$.

Grecu [13] showed that right multiplication group of a middle Bol loop coincides with the left multiplication group of the corresponding right Bol loop. After then, middle Bol loops resurfaced in literature in 1994 and 1996 when Syrbu [39, 40] considered them in-relation to the universality of the elasticity law. In 2003, Kuznetsov [30], while studying gyrogroups (a special class of Bol loops) established some algebraic properties of middle Bol loop and designed a method of constructing a middle Bol loop from a gyrogroup.

In 2010, Syrbu [41] studied the connections between structure and properties of middle Bol loops and of the corresponding left Bol loops. It was noted that two middle Bol loops are isomorphic if and only if the corresponding left (right) Bol loops are isomorphic, and a general form of the autotopisms of middle Bol loops was deduced. Relations between different sets of elements, such as nucleus, left (right,middle) nuclei, the set of Moufang elements, the center, e.t.c. of a middle Bol loop and left Bol loops were established. In 2012, Grecu and Syrbu [14] proved that two middle Bol loops are isotopic if and only if the corresponding right (left) Bol loops are isotopic. In 2012, Drapal and Shcherbacov [11] rediscovered the middle Bol identities in a new way. In 2013, Syrbu and Grecu [42] established a necessary and sufficient condition for the quotient loop of a middle Bol loop and of its corresponding right Bol loop to be isomorphic. In 2014, Grecu and Syrbu [15] established that the commutant (centrum) of a middle Bol loop is an AIP-subloop and gave a necessary and sufficient condition when the commutant is an invariant under the existing isostrophy between middle Bol loop and the corresponding right Bol loop. Osoba and Oyebo [32] further investigated the multiplication group of middle Bol loop in relation to left Bol loop while Jaiyéọlá [24, 25] studied second Smarandache Bol loops. Smarandache nuclei of second Smarandache Bol loops was studied by Osoba [36] while more results on the algebraic properties of middle Bol loops was presented by Oyebo and Osoba [35].

Grecu [13] showed that right multiplication group of a middle Bol loop coincides with the left multiplication group of the corresponding right Bol loop.

In (Adeniran et al. [2], 2015) carried out a study of some isotopic characterisation of generalised Bol loops. In (Jaiyéọlá et al. [18], 2017) studied the holomorphic structure of middle Bol loops and showed that the holomorph of a commutative loop is commutative middle Bol loop if and only if the loop is a middle Bol loop and its automorphism group is abelian. Adeniran et al. [3, 4], Jaiyéọlá and Popoola [28] studied generalised Bol loops.

In (Jaiyéọlá et al. [20], 2018), in furtherance to their exploit obtained new algebraic identities of middle Bol loop, where necessary and sufficient conditions for a bi-variate mapping of a middle Bol loop to have RIP, LIP, RAP, LAP and flexible property were presented. Additional algebraic properties of middle Bol were announced in (Jaiyéọlá et al. [19], 2021)

Furtherance to earlier studies, authors in [34] unveiled some algebraic characterizations of right and middle Bol loops relatively from their cores.

### 1.3 Preliminaries

We now state some definitions and some needed results.

**Definition 1.2.** A loop $(Q, \cdot)$ is called a

1. right Bol loop if $(xy \cdot z)y = x(yz \cdot y)$ for all $x, y \in Q$.

2. middle Bol loop if $(x/y)(z\backslash x) = (x/(zy))x$ or $(x/y)(z\backslash x) = x((zy)\backslash x)$ for all $x, y \in Q$.

**Definition 1.3.** A groupoid (quasigroup) $(Q, \cdot)$ is said to have

1. left inverse property ($LIP$) if there exists a mapping $I_\lambda : x \mapsto x^\lambda$ such that $x^\lambda \cdot xy = y$ for all $x, y \in Q$.

2. right inverse property ($RIP$) if there exists a mapping $I_\rho : x \mapsto x^\rho$ such that $yx \cdot x^\rho = y$ for all $x, y \in Q$.

**Definition 1.4.** A loop $(Q, \cdot)$ is said to be

1. an automorphic inverse property loop (AIPL) if $(xy)^{-1} = x^{-1}y^{-1}$ for all $x, y \in Q$

2. an anti- automorphic inverse property loop (AAIPL) if $(xy)^{-1} = y^{-1}x^{-1}$ for all $x, y \in Q$.

**Definition 1.5.** A loop $(Q, \cdot)$ is called a

1. right Bol loop if $(xy \cdot z)y = x(yz \cdot y)$ for all $x, y, z \in Q$.

2. middle Bol loop if $(x/y)(z\backslash x) = (x/(zy))x$ or $(x/y)(z\backslash x) = x((zy)\backslash x)$ for all $x, y, z \in Q$.

**Definition 1.6.** Let $(Q, \cdot)$ be a loop.

1. $\phi \in SYM(Q)$ is called a left pseudo-automorphism with companion $a \in Q$ if $(\phi L_a, \phi, \phi L_a) \in AUT(Q, \cdot)$. The set of left pseudo-automorphisms $PS_\lambda(Q, \cdot)$ forms a group called the left pseudo-automorphism group of $(Q, \cdot)$. See [37].

2. $\phi \in SYM(Q)$ is called a right pseudo-automorphism with companion $a \in Q$ if $(\phi, \phi R_a, \phi R_a) \in AUT(Q, \cdot)$. The set of right pseudo-automorphisms $PS_\rho(Q, \cdot)$ forms a group called the left pseudo-automorphism group of $(Q, \cdot)$. See [37].

3. $\phi \in SYM(Q)$ is called a middle pseudo-automorphism with companion $a \in Q$ if $(\phi R_a^{-1}, \phi L_{a^\lambda}^{-1}, \phi) \in AUT(Q, \cdot)$. The set of middle pseudo-automorphisms $PS_\mu(Q, \cdot)$ forms a group called the middle pseudo-automorphism group of $(Q, \cdot)$. See [42].

**Lemma 1** [37]. *1. Let $\theta$ be a right (left) pseudo automorphism of a loop, then $e\theta = e$.*

2. *Let $\theta$ be a right (left) pseudo automorphism of a LIP (RIP) loop Then $I\theta = \theta I$.*

**Lemma 2** ([37])**.** *Let $A = (U, V, W) \in AUT(Q, \cdot)$ of a loop $(Q, \cdot)$.*

1. *If $(Q, \cdot)$ is a left inverse property loop (LIPL), then $A_\lambda = (JUJ, W, V) \in AUT(Q, \cdot)$.*

2. *If $(Q, \cdot)$ is a right inverse property loop (RIPL), then $A_\rho = (W, JVJ, U) \in AUT(Q, \cdot)$.*

**Definition 1.7** (Capodaglio [9, 10])**.** In a loop $(G, \cdot)$, a permutation $U$ is called a crypto-automorphism if there exists $a, b \in L$ called the companions of $U$ such that for every $x, y \in L$,

$$(x \cdot a)U \cdot (b \cdot y)U = (x \cdot y)U.$$

Hence, $U$ is called a crypto-automorphism with companion $(a, b)$.

It will later be seen that the set $CAUM(G, \cdot)$ of crypto-automorphisms of a loop $(G, \cdot)$ forms a group.

Here are some existing results on some isostrophy invariants of Bol loops which involve autotopism, automorphism, pseudo-automorphism groups.

**Theorem 1.3** (Grecu and Syrbu [14])**.** Let $(Q, \circ)$ be a middle Bol loop and let $(Q, \cdot)$ and $(Q, *)$ be the corresponding right and left Bol loops respectively.

1. $AUM(Q, \circ) = AUM(Q, \cdot) = AUM(Q, *)$.

2. $AUT(Q, \circ) \cong AUT(Q, \cdot) \cong AUT(Q, *)$.

3. $PS_\lambda(Q, \circ) \cong PS_\rho(Q, \cdot) \cong PS_\lambda(Q, *)$.

**Theorem 1.4** (Syrbu and Grecu [42])**.** Let $(Q, \circ)$ be a middle Bol loop and let $(Q, \cdot)$ and $(Q, *)$ be the corresponding right and left Bol loops respectively.

1. $PS_\rho(Q, \circ) = PS_\mu(Q, \cdot)$.

2. $PS_\mu(Q, \circ) = PS_\lambda(Q, \cdot)$.

3. $PS_\rho(Q, \circ) = PS_\rho(Q, \cdot)$.

4. $\alpha \in PS_\lambda(Q, \circ) \Leftrightarrow I\alpha I \in PS_\rho(Q, \circ)$.

In Jaiyéọlá [34], the Bryant-Schneider group of a middle Bol was linked with some of the isostrophy-group invariance results in Theorem 1.3 and Theorem 1.4.

The objective of this paper is to investigate crypto-automorphisms of a quasigroup with right and left identity elements. For a quasigroup with right and left identity elements, some investigations on autotopic characterization of crypto-automorphisms were carried out and these were used to deduce some subgroups of the crypto-automorphism group of a middle Bol loop.

## 2 Main Results

**Lemma 3.** *Let $(G,\cdot)$ be a quasigroup. A mapping $U \in SYM(G)$ is a crypto-automorphism of $(G,\cdot)$ with companion $(a,b)$ iff $(R_aU, L_bU, U) \in AUT(G,\cdot)$.*

***Proof.*** Use Definition 1.7. ■

**Lemma 4.** *Let $(Q,\cdot)$ be a quasigroup with a right and left identity elements $e^\rho$ and $e^\lambda$ respectively. Then every automorphism $C$ of $(Q,\cdot)$ is a crypto-automorphism with companion $(e^\rho, e^\lambda)$.*

***Proof.*** $C \in AUM(Q,\cdot) \Leftrightarrow (x\cdot e^\rho)C\cdot(e^\lambda\cdot y)C = (xy)C \Leftrightarrow$ $C$ is a crypto-automorphism of $(Q,\cdot)$. ■

**Lemma 5.** *Let $C$ with companions $(a,b)$ and $D$ with companions $(p,q)$ be crypto-automorphisms of a quasigroup $(Q,\cdot)$ with right and left identity elements $e^\rho$ and $e^\lambda$. Then $CD^{-1}$ is a crypto-automorphism with companion $(c,d) = (e^\rho DC^{-1}F^{-1}, e^\lambda DC^{-1}E^{-1})$, where $E = R_aCD^{-1}R_p^{-1}DC^{-1}$ and $F = L_bCD^{-1}L_q^{-1}DC^{-1}$.*

***Proof.*** $C$ and $D$ being crypto-automorphisms of $(Q,\cdot)$ with respective companions $(a,b)$ and $(p,q)$ imply that $P = (R_aC, L_bC, C)$ and $Q = (R_pD, L_qD, D)$ are in the autotopism group of $(Q,\cdot)$. Also the product

$$PQ^{-1} = (R_aCD^{-1}R_p^{-1}, L_bCD^{-1}L_q^{-1}, CD^{-1}) \in AUT(Q,\cdot).$$

But

$$PQ^{-1} = (R_aCD^{-1}R_p^{-1}, L_bCD^{-1}L_q^{-1}, CD^{-1}) = (ECD^{-1}, FCD^{-1}, CD^{-1})$$

where $E = R_aCD^{-1}R_p^{-1}DC^{-1}$ and $F = L_bCD^{-1}L_q^{-1}DC^{-1}$. In fact, $QP^{-1} = (DC^{-1}E^{-1}, DC^{-1}F^{-1}, DC^{-1}) \in AUT(Q,\cdot)$. Now for any $x,y \in Q$,

$$xDC^{-1}E^{-1}\cdot yDC^{-1}F^{-1} = (xy)DC^{-1} \tag{3}$$

Set $x = xCD^{-1}$ and $y = e^\rho$, $y = yCD^{-1}$ and $y = e^\lambda$ in (3) to respectively get

$$E = R_{\left[e^\rho DC^{-1}F^{-1}\right]} \text{ and } F = L_{\left[e^\lambda DC^{-1}E^{-1}\right]}.$$

Therefore $CD^{-1}$ is a crypto-automorphism with companion

$$(c,d) = (e^\rho DC^{-1}F^{-1}, e^\lambda DC^{-1}E^{-1}).$$

■

**Theorem 2.1.** The set of crypto-automorphisms $CAUM(Q,\cdot)$ of a quasigroup $(Q,\cdot)$ with right and left identity elements forms a group.

***Proof.*** By Lemma 5. ■

**Corollary 2.2.** Let $(Q,\cdot)$ be a loop. Then, $AUM(Q,\cdot) \leq CAUM(Q,\cdot)$.

***Proof.*** This follows from Lemma 4 and Theorem 2.1. ■

**Theorem 2.3.** Let $(Q,\cdot)$ be a quasigroup with right and left identity elements $e^\rho$ and $e^\lambda$. If $(A,B,C) \in AUT(Q,\cdot)$

1. then, $C^{-1}$ is a crypto-automorphism with companion $(a,b) = (e^\rho B, e^\lambda A)$.
2. then, $C$ is a crypto-automorphism with companion $\big(e^\lambda AC^{-1}, e^\rho BC^{-1}\big)$.
3. such that $e^\rho B = e^\rho$ and $e^\lambda A = e^\lambda$, then $C \in AUM(Q,\cdot)$.

***Proof.***
1. Suppose $(A,B,C) \in AUT(Q,\cdot)$ , then $xA \cdot yB = (x\cdot y)C$. Setting $x = e^\lambda$ and $y = e^\rho$, we respectively get $B = CL_b^{-1}$ and $A = CR_a^{-1}$ where $b = e^\lambda A$ and $a = e^\rho B$. So, $C^{-1}$ is a crypto-automorphism with companion $(a,b) = (e^\rho B, e^\lambda A)$.
2. By 1. and Lemma 5, $C$ is a crypto-automorphism with companion $\big(e^\lambda AC^{-1}, e^\rho BC^{-1}\big)$.
3. By 1.

■

**Theorem 2.4.** Let $(Q,\cdot)$ be a quasigroup with right and left identity elements $e^\rho$ and $e^\lambda$ such that $C$ is a crypto-automorphism with companion $(a,b)$.

1. Then the following statements are equivalent:
   - **(i)** $e^\lambda C = e^\lambda$.
   - **(ii)** $T = (R_aC, L_{a^\lambda}C, C) \in AUT(Q,\cdot)$.
   - **(iii)** $Y = (R_{(b\backslash e^\lambda)}C, L_bC, C) \in AUT(Q,\cdot)$.
2. Then the following statements are equivalent:
   - **(i)** $e^\rho C = e^\rho$.
   - **(ii)** $T = (R_{b^\rho}C, L_bC, C) \in AUT(Q,\cdot)$.
   - **(iii)** $Y = (R_aC, L_{(e^\rho/a)}C, C) \in AUT(Q,\cdot)$.

***Proof.***
1. Given that $C$ is a crypto-automorphism, it implies that $\alpha = (R_aC, L_bC, C) \in AUT(Q,\cdot)$, so for any $x,y \in Q$, $xR_aC \cdot yL_bC = (xy)C$.

**(i) $\Rightarrow$ (ii)** Let $e^\lambda C = e^\lambda$. Set $y = e^\rho$ to get $xR_aCR_{bC} = xC \Rightarrow CR_{bC} = R_a^{-1}C$. Thus for any $z \in Q$, $zCR_{bC} = zR_a^{-1}C \Rightarrow zC \cdot bC = (z/a)C$. If we set $z = e^\lambda$, then $bC = (e^\lambda/a)C \Leftrightarrow b = e^\lambda/a$, which gives the required autotopism $T$ obtained on substitution into $\alpha$.

**(ii) $\Rightarrow$ (iii)** Since $b = e^\lambda/a$ in (ii), then $a = b\backslash e^\lambda$. If this is put in autotopism $\alpha$, the required autotopism $Y$ is obtained.

**(iii) $\Rightarrow$ (i)** Since $Y = (R_{(b\backslash e^\lambda)}C, L_bC, C) \in AUT(Q,\cdot)$, for any $y,z \in Q$, we have $yR_{(b\backslash e^\lambda)}C \cdot zL_bC = (yz)C$. Set $y = b$, then $e^\lambda C \cdot (bz)C = (bz)C \Leftrightarrow e^\lambda C = e^\lambda$.

2. This is similar to 1.

■

**Corollary 2.5.** Let $(Q,\cdot)$ be a loop with identity $e$ such that $C$ is a crypto-automorphism with companion $(a,b)$. Then the following statements are equivalent:

**(i)** $eC = e$.

**(ii)** $C$ is a crypto-automorphism with companion $(a, a^\lambda)$.

**(iii)** $C$ is a crypto-automorphism with companion $(b^\rho, b)$.

***Proof.*** This follows by Theorem 2.4. ■

**Corollary 2.6.** Let $(Q,\cdot)$ be a quasigroup with right and left identity elements $e^\rho$ and $e^\lambda$ such that $(A,B,C) \in AUT(Q,\cdot)$.

1. Then the following statements are equivalent:

    **(i)** $e^\lambda C = e^\lambda$.

    **(ii)** $T = \left(R_{\left(e^\lambda AC^{-1}\right)}C, L_{\left(e^\lambda AC^{-1}\right)^\lambda}C, C\right) \in AUT(Q,\cdot)$.

    **(iii)** $Y = \left(R_{\left(\left(e^\rho BC^{-1}\right)\backslash e^\lambda\right)}C, L_{\left(e^\rho BC^{-1}\right)}C, C\right) \in AUT(Q,\cdot)$.

2. Then the following statements are equivalent:

    **(i)** $e^\rho C = e^\rho$.

    **(ii)** $T = \left(R_{\left(e^\rho BC^{-1}\right)^\rho}C, L_{\left(e^\rho BC^{-1}\right)}C, C\right) \in AUT(Q,\cdot)$.

    **(iii)** $Y = \left(R_{\left(e^\lambda AC^{-1}\right)}C, L_{\left(e^\rho/\left(e^\lambda AC^{-1}\right)\right)}C, C\right) \in AUT(Q,\cdot)$.

***Proof.*** We apply Theorem 2.3 and Theorem 2.4. ■

**Corollary 2.7.** Let $(Q,\cdot)$ be a loop such that $(A,B,C)\in AUT(Q,\cdot)$. Then the following statements are equivalent:

**(i)** $eC=e$.

**(ii)** $C$ is a crypto-automorphism with companion $\Big(\big(e^\lambda AC^{-1}\big),\big(e^\lambda AC^{-1}\big)^\lambda\Big)$.

**(iii)** $C$ is a crypto-automorphism with companion $\Big(\big(e^\rho BC^{-1}\big)^\rho,\big(e^\rho BC^{-1}\big)\Big)$.

***Proof.*** This follows by Corollary 2.5 and Theorem 2.3. ■

**Remark 2.1.** Greer and Kinyon [16] defined a middle pseudo-automorphism of a loop $(Q,\cdot)$ to be a mapping $U\in SYM(Q)$ such that $(xy)U=[(xU)/c^\rho][c\backslash(yU)]$ for some $c\in Q$. This definition is equivalent to that in Definition 1.6. Recall that $PS_\mu(Q,\cdot)\le SYM(Q)$. Hence, by Lemma 5 and Theorem 2.1, $PS_\mu(Q,\cdot)\le CAUM(Q,\cdot)$. It will later on be seen in Theorem 2.13 that a particular subgroup of $CAUM(Q,\circ)$ is equal to $PS_\mu(Q,\circ)$ whenever $(Q,\circ)$ is a middle Bol loop.

In Greer and Kinyon [16], it was shown that for a loop $(Q,\cdot)$ with identity element $e$, if $AUT_\mu(Q,\cdot)=\{(A,B,C)\in AUT(Q,\cdot)\mid eC=e\}$, then

$$\begin{aligned}AUT_\mu(Q,\cdot)&=AUT(Q,\cdot)\cap\{(UR_{c^\rho}^{-1},UL_c^{-1},U)\mid U\in SYM(Q),\ c\in Q\}\\&=AUT(Q,\cdot)\cap\{(R_{c^\rho}U,L_cU,U)\mid U\in SYM(Q),\ c\in Q\}.\quad(\textit{Remark } 2.1)\end{aligned}$$

The motivation for introducing the subgroup $AUT_\mu(Q,\cdot)$ of $AUT(Q,\cdot)$ by Greer and Kinyon [16] for a loop $(Q,\cdot)$ can be traced from the result in Corollary 2.7.

Let $(Q,\cdot)$ be a quasigroup with right and left identity elements $e^\rho$ and $e^\lambda$. If $C\in SYM(Q)$ such that $(R_aC,L_{a^\lambda}C,C)\in AUT(Q,\cdot)$ for some $a\in Q$, then $C$ will be called a left crypto-automorphism and their set will be represented by $LCAUM(Q,\cdot)$. If $C\in SYM(Q)$ such that $(R_{a^\rho}C,L_aC,C)\in AUT(Q,\cdot)$ for some $a\in Q$, then $C$ will be called a right crypto-automorphism and their set will be represented by $RCAUM(Q,\cdot)$

**Theorem 2.8.** Let $(Q,\cdot)$ be a quasigroup with right and left identity elements $e^\rho$ and $e^\lambda$. Then,

1. $LCAUM(Q,\cdot)=\{C\in CAUM(Q,\cdot)\mid e^\lambda C=e^\lambda\}\le CAUM(Q,\cdot)$.
2. $PS_\mu(Q,\cdot)=RCAUM(Q,\cdot)=\{C\in CAUM(Q,\cdot)\mid e^\rho C=e^\rho\}\le CAUM(Q,\cdot)$.

***Proof.*** This follows by Theorem 2.1 and Theorem 2.4. ■

**Corollary 2.9.** Let $(Q,\cdot)$ be a loop with identity $e$ such that $C$ is a crypto-automorphism with companion $(a,b)$. Then, $LCAUM(Q,\cdot) = PS_\mu(Q,\cdot) = RCAUM(Q,\cdot) = \{C \in CAUM(Q,\cdot) \mid eC = e\} \leq CAUM(Q,\cdot)$.

***Proof.*** This follows by Theorem 2.4. ∎

**Remark 2.2.** From Theorem 2.8 and Corollary 2.9, it can be concluded that left crypto-automorphism and right crypto-automorphism (or middle pseudo-automorphism) coincide for a loop but do not necessarily coincide in a quasigroup with right and left identity elements.

**Theorem 2.10.** Let $(Q,\cdot)$ be a loop with identity element $e$ and $C \in CAUM(Q,\cdot)$ with companion $(a,b)$.

1. If $(Q,\cdot)$ is an LIPL, then the following are equivalent:
   (a) $eC = e$.
   (b) $C \in LCAUM(Q,\cdot)$ with companion $(a,a^{-1})$.
   (c) $C \in PS_\lambda(Q,\cdot)$ with companion $(aC)^{-1}$.
2. If $(Q,\cdot)$ is an RIPL, then the following are equivalent:
   (a) $eC = e$.
   (b) $C \in RCAUM(Q,\cdot)$ with companion $(b^{-1},b)$.
   (c) $C \in PS_\rho(Q,\cdot)$ with companion $(bC)^{-1}$.

***Proof.*** 1. Let $(Q,\cdot)$ be a LIPL.

**(i)**$\Rightarrow$ **(ii)** If $eC = e$, then following Theorem 2.4, $(R_aC, L_{a^{-1}}C, C) \in AUT(Q,\cdot)$. Thus, $C \in LCAUM(Q,\cdot)$ with companion $(a,a^{-1})$.

**(ii)**$\Rightarrow$**(iii)** If $C \in LCAUM(Q,\cdot)$ with companion $(a,a^{-1})$, then $JL_a^{-1}C = R_aCJ$. So, $A = (R_aC, L_{a^{-1}}C, C) \in AUT(Q,\cdot)$ and by Lemma 2, $A_\lambda = (JR_aCJ, C, L_{a^{-1}}C) = (L_a^{-1}C, C, L_a^{-1}C)$, which implies that $C \in PS_\lambda(Q,\cdot)$ with companion $a$.

**(iii)**$\Rightarrow$**(i)** Let $C \in PS_\lambda(Q,\cdot)$ with companion $(aC)^{-1}$, then $C^{-1} \in PS_\lambda(Q,\cdot)$ with companion $a$. So, for any $y,z \in Q$, $yC^{-1}L_a \cdot zC^{-1} = (yz)C^{-1}L_a$, set $z = e$ to get $eC = e$.

2. This is similar to the proof of 1.

∎

**Remark 2.3.** Theorem 2.10 suggests that for LIP or RIP loops, the concept of crypto-automorphism reduces to (left or right) pseudo-automorphism and (left or right) crypto-automorphism, whenever $C$ fixes the identity of the loop.

**Theorem 2.11.** A loop $(Q,\cdot)$ is a G-loop if and only if every pair of elements $(a,b)\in Q^2$ is a companion of some crypto-automorphism of $(Q,\cdot)$ if and only if every $x\in Q$ is the companion of some left pseudo-automorphism and some right pseudo-automorphism of $(Q,\cdot)$.

***Proof.*** Let $(Q,\circ)$ be an arbitrary $b,a$-isotope of $(Q,\cdot)$. Using Theorem 1.2, $C\in CUM(Q,\cdot)$ with companion $(a,b)$ if and only if $(Q,\cdot)\xrightarrow[\text{autotopism}]{(R_aC,L_bC,C)}(Q,\cdot)\Leftrightarrow$ $(Q,\cdot)\xrightarrow[\text{principal isotopism}]{(R_a,L_b,I)}(Q,\circ)\xrightarrow[\text{isomorphism}]{(C,C,C)}(Q,\cdot)$. ■

**Remark 2.4.** The first part of Theorem 2.11 is another characterization of the class of G-loops which has no equational characterization.

**Theorem 2.12.** Let $(Q,\cdot)$ be a loop. Then, $BS(Q,\cdot)=CAUM(Q,\cdot)$ .

***Proof.*** Let $\theta\in BS(Q,\cdot)$ for some $f,g\in Q$, then $(\theta R_g^{-1},\theta L_f^{-1},\theta)\in AUT(Q,\cdot)$. For all $x,y\in Q$, we have

$$x\theta R_g^{-1}\cdot y\theta L_f^{-1}=(xy)\theta \tag{4}$$

Let $x\theta R_g^{-1}=a\Leftrightarrow ag=x\theta\Leftrightarrow x=(ag)\theta^{-1}$. Also, set $y\theta L_f^{-1}=b\Leftrightarrow y\theta=fb\Leftrightarrow$ $y=(fb)\theta^{-1}$. Put $x$ and $y$ into (4), we have

$$(ag)R_g^{-1}\cdot(fb)L_f^{-1}=\big((ag)\theta^{-1}\cdot(fb)\theta^{-1}\big)\theta$$
$$\Leftrightarrow(a\cdot b)\theta^{-1}=(a\cdot g)\theta^{-1}\cdot(f\cdot b)\theta^{-1}\Leftrightarrow(R_g\theta^{-1},L_f\theta^{-1},\theta^{-1})\in AUT(Q,\cdot)$$

Thus, $\theta^{-1}\in CAUM(Q,\cdot)$. So, by Theorem 2.1, $\theta\in CAUM(Q,\cdot)$. Conversely, we reverse the procedures to obtain $\theta\in BS(Q,\cdot)$ ■

**Lemma 6.** *Let $(\alpha,\beta,\gamma)$ be an autotopism of a middle Bol loop $(Q,\circ)$. Then $(I\beta I,I\alpha I,I\gamma I)$ is also an autotopism of $(Q,\circ)$.*

***Proof.*** Let $(Q,\circ)$ be a middle Bol loop and $(\alpha,\beta,\gamma)$ be the autotopism of $(Q,\circ)$, then for all $x,y\in Q$, we have

$$x\alpha\circ y\beta=(x\circ y)\gamma\Longrightarrow[x\alpha\circ y\beta]I=(x\circ y)\gamma I\Longrightarrow[(y\beta)I\circ(x\alpha)I]=(x\circ y)\gamma I.$$

Doing $y\mapsto yI$ and $x\mapsto xI$ in the last equation, we get

$$yI\beta I\circ xI\alpha I=[(xI\circ yI)\gamma]I\implies yI\beta I\circ xI\alpha I=[(y\circ x)I\gamma]I.$$

Thus, $(I\beta I,I\alpha I,I\gamma I)\in AUT(Q,\circ)$. ■

**Theorem 2.13.** Let $(Q,\circ)$ be a middle Bol loop and $(Q,\cdot)$ be the corresponding right Bol loop. Then, $LCAUM(Q,\circ)=RCAUM(Q,\circ)=PS_\lambda(Q,\cdot)=PS_\mu(Q,\circ)$.

***Proof.*** We rest on Theorem 2.8. We shall show that $U \in LCAUM(Q, \circ)$ if and only if $U \in PS_\lambda(Q, \cdot)$. $U$ is a crypto-automorphism if and only if $(\mathbb{R}_a U, \mathbb{L}_b U, U) \in AUT(Q, \circ) \Leftrightarrow$ the identity $(x \circ a)U \circ (b \circ y)U = (x \circ y)U$ holds for all $x, y \in Q$. Then, we have

$$xL_{a^{-1}}^{-1}U \circ yIP_bU = (x \circ y)U$$
$$\Leftrightarrow (yIP_bU)I\backslash xL_{a^{-1}}^{-1}U = (yI\backslash x)U$$
$$\Leftrightarrow xL_{a^{-1}}^{-1}U = (yP_bU)I \cdot (y\backslash x)U$$

Set $z = y\backslash x \Leftrightarrow x = y \cdot z$, then $(y \cdot z)L_{a^{-1}}^{-1}U = zU \cdot (yP_bU)I$. Put $z = e$, then with the hypothesis $e = eU$, it follows that $L_{a^{-1}}^{-1}U = P_bUI$. This implies that $(y \cdot z)L_{a^{-1}}^{-1}U = zU \cdot yL_{a^{-1}}^{-1}U \Leftrightarrow (L_{a^{-1}}^{-1}U, U, L_{a^{-1}}^{-1}U) \in AUT(Q, \cdot)$. Thus, $U^{-1} \in PS_\lambda(Q, \cdot)$ which implies that $U \in PS_\lambda(Q, \cdot)$.

Conversely, suppose that $U \in PS_\lambda(Q, \cdot) \Rightarrow U^{-1} \in PS_\lambda(Q, \cdot)$ and then $(L_{a^{-1}}^{-1}U, U, L_{a^{-1}}^{-1}U) \in AUT(Q, \cdot)$. For all $x, y, \in Q$, we have

$$xL_{a^{-1}}^{-1}U \cdot yU = (xy)L_{a^{-1}}^{-1}U$$
$$\Leftrightarrow x\mathbb{R}_aU \cdot yU = (xy)\mathbb{R}_aU$$
$$yU//(x\mathbb{R}_aU)I = (y//x^{-1})\mathbb{R}_aU$$

Set $z = y//x^{-1} \Leftrightarrow y = z \circ x^{-1}$, then $(z \circ x)U = z\mathbb{R}_aU \circ (xI\mathbb{R}_aU)I$. Set $z = e$ to get

$$xU = e\mathbb{R}_aU \circ (xI\mathbb{R}_aU)I \Leftrightarrow xU = xI\mathbb{R}_aUI\mathbb{L}_{aU}$$
$$\Leftrightarrow xU\mathbb{L}_{aU}^{-1} = xI\mathbb{R}_aIIUI$$
$$\Leftrightarrow xU\mathbb{L}_{aU}^{-1} = x\mathbb{L}_{a^\lambda}IUI \Leftrightarrow xU\mathbb{L}_{aU}^{-1} = x\mathbb{L}_{a^\lambda}UII$$
$$\Leftrightarrow xU\mathbb{L}_{aU}^{-1} = x\mathbb{L}_{a^\lambda}U.$$

For all $x, z \in Q$, we have $x\mathbb{R}_aU \circ z\mathbb{L}_{a^\lambda}U = (x \circ z)U \Leftrightarrow (\mathbb{R}_aU, \mathbb{L}_{a^\lambda}U, U) \in AUT(Q, \circ) \Leftrightarrow U \in CAUM(Q, \circ)$. Thus, $LCAUM(Q, \circ) = RCAUM(Q, \circ) = PS_\lambda(Q, \cdot) = PS_\mu(Q, \circ)$ by Corollary 2.9 and Theorem 1.4. ∎

**Theorem 2.14.** Let $(Q, \cdot)$ be a middle Bol loop. Let

$\phi_1(x) = IP_xL_x, \phi_2(x) = IP_x^{-1}R_x, \phi_3(x) = P_xL_xI, \phi_4(x) = P_x^{-1}R_xI$ for any $x \in Q$.

1. $\phi_i(x) \in CAUM(Q, \cdot)$ for any $x \in Q$ with companion $(x^{-1}, x^{-1})$ for $i = 1, 2$ and companion $(x, x)$ for $i = 3, 4$.

2. $\langle \phi_i(x) | x \in Q \rangle = \langle \phi_j(x) | x \in Q \rangle \leq CAUM(Q, \cdot)$ for any $i, j \in \{1, 2, 3, 4\}$.

***Proof.*** Going by the middle Bol loop identities in Definition 1.2, we have the autotopisms $MB1 = (IP_x^{-1}, IP_x, IP_xL_x)$ and $MB2 = (IP_x^{-1}, IP_x, IP_xL_x)$ for any $x \in Q$. Applying Lemma 6 to $MB1$ and $MB2$, we get the autotopisms $MB3 = (P_xI, P_x^{-1}I, P_xL_xI)$ and $MB4 = (P_xI, P_x^{-1}I, P_x^{-1}R_xI)$ for any $x \in Q$. for all $x, y \in Q$.

By using the facts that $MB1, MB2, MB3, MB4$ are autotopisms of a middle Bol loop in Theorem 2.3, we deduce that $\phi_i(x) \in CAUM(Q, \cdot)$ for any $x \in Q$ with companion $(x^{-1}, x^{-1})$ for $i = 1, 2$ and companion $(x, x)$ for $i = 3, 4$. From this and the fact in Theorem 2.1, $\langle \phi_i(x) | x \in Q\rangle = \langle \phi_j(x) | x \in Q\rangle \leq CAUM(Q, \cdot)$ for any $i, j \in \{1, 2, 3, 4\}$. ■

## REFERENCES


[1] Adeniran, J. O. (2003). Some properties of the Bryant-Schneider groups of certain Bol loops. Proc. Jangjeon Math. Soc. 6, no. 1, 71–80.

[2] Adeniran, J. O; Akinleye, S. A and Alakoya, T. O. (2015). On the core and some isotopic characterisations of generalised Bol loops, J. of the Nigerian Asso. Mathematical Phy. 1, 99–104 https://doi.org/10.22199/issn.0717-6279-4581

[3] Adeniran, J. O., Jaiyéọlá T. G. and Idowu, K. A. (2014). Holomorph of generalized Bol loops, Novi Sad Journal of Mathematics, 44, no. 1, 37–51.

[4] Adeniran, J. O., Jaiyéọlá T. G. and Idowu, K. A. (2022), On some characterizations of generalized Bol loops. Proyecciones Journal of Mathematics, 41, no. 4, 805–823. https://doi.org/10.22199/issn.0717-6279-4581

[5] Belousov V.D. (1971) Algebraic nets and quasigroups. (Russian), Kishinev, "Shtiintsa", 166 pp.

[6] Belousov, V. D. (1967). Foundations of the theory of quasigroups and loops, (Russian) Izdat. "Nauka", Moscow 223pp.

[7] Belousov, V. D.; Sokolov, E. I. (1988). $N$-ary inverse quasigroups (I-quasigroups), (Russian) Mat. Issled. No. 102, Issled. Oper. i Kvazigrupp, 26–36, 118.

[8] Burris S. and Sankappanavar, H. P. (1981). A course in universal algebra. Graduate Texts in Mathematics, 78. Springer-Verlag, New York-Berlin. xvi+276 .

[9] Capodaglio Di Cocco R. (1993), *On Isotopism and Pseudo-Automorphism of the loops*, Bollettino U. M. I. 7, 199–205.

[10] Capodaglio Di Cocco R. (2003), *Regular Permutation Sets and Loops*, Bollettino U. M. I. 8, 617–628.

[11] Drapal, A. and Shcherbacov, V. (2012), *Identities and the group of isostrophisms*, Comment. Math. Univ. Carolin. 53(3), 347–374.

[12] Foguel, T; Kinyon, M .K and Phillips, J. D. (2006). On twisted subgroups and Bol loops of odd order. Rocky Mountain J. Math. 36, no. 1, 183–212. https://www.jstor.org/stable/44239103

[13] Grecu, I. (2014). On multiplication groups of isostrophic quasigroups, Proceedings of the Third Conference of Mathematical Society of Moldova IMCS-50, August 19-23, 2014, Chisinau, Republic of Moldova, 78-81. http://dspace.usm.md:8080/xmlui/handle/123456789/1292

[14] Grecu, I. and Syrbu, P. (2012), *On Some Isostrophy Invariants of Bol Loops*, Bulletin of the Transilvania University of Brasov, Series III: Mathematics, Informatics, Physics, 5(54), 145–154.

[15] Grecu, I. and Syrbu, P. (2014), *Commutants of middle Bol loops*, Quasigroups and Related Systems, 22, 81–88.

[16] Greer, M. and Kinyon, M. (2012), *Pseudoautomorphisms of Bruck loops and their generalizations*, Comment. Math. Univ. Carolin. 53(3), 383-–389.

[17] Gvaramiya A. (1971). On a class of loops (Russian), Uch. Zapiski MAPL. 375, 25-34.

[18] Jaiyéọlá, T. G; David, S. P and Oyebo, Y. T. (2015). New algebraic properties of middle Bol loops. ROMAI J. 11, no. 2, 161–183

[19] Jaiyéọlá, T. G.; David, S. P and Oyebola, O. O. (2021). New algebraic properties of middle Bol loops II. Proyecciones Journal of Mathematics 40, no. 1, 85–106. http://dx.doi.org/10.22199/issn.0717-6279-2021-01-0006

[20] Jaiyéọlá, T. G; David, S. P; Ilojide. E; Oyebo, Y. T. (2017). Holomorphic structure of middle Bol loops. Khayyam J. Math. 3, no. 2, 172–184. https://doi.org/10.22034/kjm.2017.51111

[21] Robinson, D. A. (1980). The Bryant-Schneider group of a loop. Ann. Soc. Sci. Bruxelles Sér. I 94 , no. 2-3, 69–81 (1981).

[22] Jaiyéọlá, T. G. (2008). On Smarandache Bryant Schneider group of A Smarandache loop, International Journal of Mathematical Combinatorics, 2, 51–63. http://doi.org/10.5281/zenodo.820935

[23] Jaiyéọlá, T. G. (2009). A study of new concepts in smarandache quasigroups and loop, ProQuest Information and Learning(ILQ), Ann Arbor, 127pp. https://doi.org/10.5281/zenodo.8913

[24] Jaiyéọlá, T. G. (2009); Basic Properties of Second Smarandache Bol Loops, International Journal of Mathematical Combinatorics, 2, 11–20. http://doi.org/10.5281/zenodo.32303

[25] Jaiyéọlá, T. G. (2011); Smarandache Isotopy Of Second Smarandache Bol Loops, Scientia Magna Journal, 7, no. 1., 82–93. http://doi.org/10.5281/zenodo.234114

[26] Jaiyéọlá, T. G., Adéníran, J. O. and Sòlárìn, A. R. T. (2011), Some necessary conditions for the existence of a finite Osborn loop with trivial nucleus, Algebras, Groups and Geometries, 28, no. 4, 363–380.

[27] Jaiyéọlá, T. G., Adéníran, J. O. and Agboola, A. A. A. (2013); On the Second Bryant Schneider Group of Universal Osborn loops, Societatea Română de Matematică Aplicată si Industrială Journal (ROMAI J.), 9, no. 1, 37–50.

[28] Jaiyéọlá, T. G. and Popoola, B. A. (2015). Holomorph of generalized Bol loops II, Discussiones Mathematicae-General Algebra and Applications, 35, no. 1, 59-–78. doi:10.7151/dmgaa.1234.

[29] Jaiyéọlá T. G., Osoba, B. and Oyem, A., Isostrophy Bryant-Schneider Group-Invariant of Bol loops, pre-print.

[30] Kuznetsov, E. (2003), *Gyrogroups and left gyrogroups as transversals of a special kind*, Algebraic and discrete Mathematics 3, 54–81.

[31] Shcherbacov, V. A. (2011). *A-nuclei and A-centers of quasigroup*, Institute of mathematics and computer Science Academiy of Science of Moldova Academiei str. 5, Chisinau, MD -2028, Moldova

[32] Osoba, B and Oyebo, Y. T. (2018). *On Multiplication Groups of Middle Bol Loop Related to Left Bol Loop*, Int. J. Math. and Appl., 6, no. 4, 149–155.

[33] Osoba. B and Oyebo. Y. T (2018). *On Relationship of Multiplication Groups and Isostrophic quasigroups*, International Journal of Mathematics Trends and Technology (IJMTT), 58, no. 2, 80–84. DOI:10.14445/22315373/IJMTT-V58P511

[34] Osoba, B. and Jaiyéọlá T. G. *Algebraic Connections between Right and Middle Bol loops and their Cores*, Quasigroups and Related Systems, 30, 149-160, 2022.

[35] Oyebo, Y. T. and Osoba, B. *More results on the algebraic properties of middle Bol loops.* Journal of the Nigerian mathematical society, accepted for publication.

[36] Osoba, B. *Smarandache Nuclei of Second Smarandache Bol Loops*, Scientia Magna Journal, accepted for publication.

[37] Pflugfelder, Hala O. (1990). *Quasigroups and loops: introduction* . Sigma Series in Pure Mathematics, 7. Heldermann Verlag, Berlin. viii+147

[38] Shcherbacov, V. A. (2017), *Elements of quasigroup theory and applications.* Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL.

[39] Syrbu, P. (1994), *Loops with universal elasticity*, Quasigroups Related Systems 1, 57–65.

[40] Syrbu, P. (1996), *On loops with universal elasticity*, Quasigroups Related Systems 3, 41–54.

[41] Syrbu, P. (2010), *On middle Bol loops*, ROMAI J. 6,2, 229–236.

[42] Syrbu, P. and Grecu, I. (2013). On some groups related to middle Bol loops, Revistă Ştiinţifică a Universităţii de Stat din Moldova, 7(67), 10–18.

[43] Vanliurova, A. (2005). Cores of Bol loops and symmetric groupoids. Bul. Acad. Lztiinle Repub. Mold. Mat, 49, no. 3, 153–164.

Received
Revised
Accepted