Quasigroups and Related Systems **31** (2023), 53 – 64

https://doi.org/10.56415/qrs.v31.04

On the universality and isotopy-isomorphy of (r, s, t)-inverse quasigroups and loops with applications to cryptography

Richard Ilemobade, Olufemi George and Tèmítọ́pẹ́ Gbọ́láhàn Jaíyéọlá

Abstract. This paper introduced a condition called $\mathcal{R}$-condition under which (r, s, t)-inverse quasigroups are universal. Middle isotopic (r, s, t)-inverse loops, satisfying the $\mathcal{R}$-condition and possessing a trivial set of r-weak inverse permutations were shown to be isomorphic; isotopy-isomorphy for (r, s, t)-inverse loops. Isotopy-isomorphy for (r, s, t)-inverse loops was generally characterized. With the $\mathcal{R}$-condition, it was shown that for positive integers r, s and t, if there is a (r, s, t)-inverse quasigroup of order $3k$ with an inverse-cycle of length $gcd(k, r+s+t) > 1$, then there exists an (r, s, t)-inverse quasigroup of order $3k$ with an inverse-cycle of length $gcd\big(k(r+s+t), (r+s+t)^2\big)$. The procedure of application of such (r, s, t)-inverse quasigroups to cryptography was described and explained, while the feasibility of such (r, s, t)-inverse quasigroups was illustrated with sample values of k, r, s and t.

1. Introduction

Weak inverse property quasigroups (loops) and cross inverse property quasigroups (loops) are among the most studied loops with variation of inverse property. They have been studied in relation to Basarab loops by Jaiyéọlá and Effiong [16]. Weak and cross inverse property loops have been generalized by Karklin and Karklin to m-inverse loops. m-inverse quasigroups were introduced by Keedwell and Shcherbacov [19] and applications of this structure to cryptography was studied. They further generalized the concept of m-inverse quasigroup by defining (r, s, t)-inverse quasigroup and loop in [20], where r, s, and t are integers, and this include as special cases

2020 Mathematics Subject Classification: 20N02, 20N05.

Keywords: weak inverse, cross inverse, m-inverse, (r, s, t)-inverse quasigroups and loops, $\mathcal{R}$-condition, isotopy-isomorphy, long inverse cycle, cryptography.

all WIP-,CI- and m-inverse loops (and quasigroups). Thus some of the results on (r, s, t)-inverse loops and quasigroups generalizes some known ones on WIP-,CI- and m-inverse loops (and quasigroups).

Jaiyéọlá [7] investigated some isotopy-isomorphy conditions for m-inverse quasigroups and loops. There have been various studies of these two varieties of loops (with peculiar interest in their applications in cryptography) in the recent past and present. Among these are Jaiyéọlá [6, 7, 9, 10, 12], Jaiyéọlá and Adeniran [14], Jaiyéọlá and Smarandache [17], Oyebo et al. [25]. A universal WIPL is an Osborn loop. Application of Osborn loops to cryptography was reported by Jaiyéọlá and Adéníran [15] and Jaiyéọlá [11, 13]. Shcherbacov [27] has a chapter dedicated to the application of quasigroups in cryptology.

This present paper generalizes some results of Jaiyéọlá [7] on m-inverse loops and quasigroups to (r, s, t)-inverse loops and quasigroups. It also discusses their application to cryptography.

2. Definitions and notations

Let Q be a non-empty set. Let $(\cdot)$ be a binary operation on Q such that $x \cdot y \in Q \ \forall \ x, y \in Q$. Then $(Q, \cdot)$ is called a groupoid. If in addition, the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions $(x, y) \in Q \times Q$, then $(Q, \cdot)$ is called a quasigroup. A quasigroup with an element (identity element) e such that $x \cdot e = e \cdot x = x \ \forall \ x \in Q$ is called a loop. For brevity, sometimes, we shall write xy for $x \cdot y$. The permutations $J_\rho : Q \longrightarrow Q$ and $J_\lambda : Q \to Q$ defined by $J_\rho : x \mapsto x^\rho$ and $J_\lambda : x \mapsto x^\lambda$ are called the right and left inverse maps respectively and such that $x \cdot x^\rho = e$ and $x^\lambda \cdot x = e$.

If there is a permutation J of elements of a quasigroup $(Q, \cdot)$ such that $\forall \ x, y \in Q$

$$(xy)J^r \cdot xJ^s = yJ^t,$$

where r, s and t are integers, then $(Q, \cdot)$ is called an (r, s, t)-inverse quasigroup. If $r = t = m$ and $s = m + 1$, we have

$$(xy)J^m \cdot xJ^{m+1} = yJ^m.$$

Hence, we have an m-inverse quasigroup. If in addition, $(Q, \cdot)$ is a loop and the permutation J is such that $x \cdot xJ = e$, where e is the identity element in Q, then $(Q, \cdot)$ is an m-inverse loop (or generally an (r, s, t)-inverse loop).

Let $(G, \cdot)$ and $(H, \circ)$ be groupoids (quasigroups, loops). Let A, B and C be three bijections, that maps G onto H. The triple $\alpha = (A, B, C) : G \to H$

is called an isotopism of $(G, \cdot)$ onto $(H, \circ)$ if

$$xA \circ yB = (xy)C \quad \forall\, x, y \in G.$$

If

- $\alpha = (A, B, B)$, then the triple is called a left isotopism and the groupoids (quasigroups, loops) are called left isotopes.
- $\alpha = (A, B, A)$, then the triple is called a right isotopism and the groupoids (quasigroups, loops) are called right isotopes.
- $\alpha = (A, A, B)$, then the triple is called a middle isotopism and the groupoids (quasigroups, loops) are called middle isotopes.

If $(G, \cdot) = (H, \circ)$, the triple $\alpha = (A, B, C)$ is called an autotopism. Such triples form a group $ATP(G, \cdot)$ called autotopism group of $(G, \cdot)$. If $A = B = C$, then $\alpha = (A, B, C) = (A, A, A) = A$ is called an automorphism. Such bijections form an automorphism group $AUT(G, \cdot)$ of $(G, \cdot)$.

Definition 2.1. (cf. [7]) A bijection β of a loop $(Q, \cdot)$, for which the identity $xJ^r = [(x\beta)J^r]\beta$ holds, where J is such that $x \cdot xJ = e$ is called an r-weak inverse permutation.

Definition 2.2. A property of a quasigroup is said to be isotopic invariant if the quasigroup possesses the property and all it isotopes also possess it. Hence, such quasigroup is said to be universal (or universal relative to a property).

Definition 2.3. (cf. [2]) In a loop $(L, \cdot)$ with unit element e, let J be the bijection defined by $x \mapsto xJ$, $x \cdot xJ = e$. If n is the least positive integer for which $xJ^n = x$, then $\{x,\ xJ,\ \ldots, xJ^{n-1}\}$ is called an inverse-cycle of length n

Definition 2.4. (cf. [19, 20]) Let Q be a m-inverse quasigroup or (r, s, t)-inverse quasigroup. Consider the permutation J of Q with finite sequence $x_1, x_2, \cdots, x_n$ such that $x_kJ \equiv x_{k+1} \pmod{n}$. This sequence is called cycles of inverses (or inverse cycles) of lenght n.

For the purpose of applying CIPQs to cryptography, Keedwell [18] constructed CIPQs with long inverse cycles. The author gave examples and detailed explanation and procedures of the use of these CIPQs for cryptography. Cross inverse property quasigroups have been found appropriate for cryptography because they give rise to what is called 'cycle of inverses' or 'inverse cycles' or simply 'cycles' i.e finite sequence. The origin of the idea of cycles can be traced back to Artzy [1, 2] where he also found their existence in WIPLs apart form CIPLs. Keedwell and Shcherbacov [19] investigated the existence of m-inverse quasigroups and loops with long inverse cycle such that $m \geqslant 1$. Likewise, Keedwell and Shcherbacov [21] proved the existence of (r, s, t)-inverse quasigroups for specified values of r, s and t. We present them below.

Theorem 2.5. (see [21])

1. *There exist (r, s, t)-inverse quasigroups of every order $3n$ such that n is not relatively prime to $r + s + t$ with inverse cycles of length equal to the GCD of n and $r + s + t$.*
2. *There exist (r, s, t)-inverse quasigroups of order $3(r+s+t)$ with inverse cycles of length $r + s + t$.*
3. *(r, s, t)-inverse quasigroups exist for every choice of positive integers r, s and t.*

Keedwell and Shcherbacov [20] were able to construct (r, s, t)-IQs using T-quasigroups. After the results of Keedwell and Shcherbacov [19, 20, 21] on existence (and non-existence) of finite m-inverse quasigroup of certain orders and the construction of (r, s, t)-inverse quasigroup with long inverse cycles, Looney [23] was able to further establish the existence (and non-existence) of finite m-inverse quasigroup of certain orders which earlier authors could not address.

The results on the holomorph of left and right key laws were shown by Ogunrinade et al. [24] to be applicable to symmetric cryptography (secret key cryptosystem) while Isere et al. [5] built cipher algorithms for cryptography in some peculiar circumstances using some quasi-Latin quandles.

In what follows, we shall employ the use of the bijections J, $L_x : y \mapsto xy$ and $R_x : y \mapsto yx$ for quasigroup $(G, \cdot)$, while J^*, $L^*_x : y \mapsto x \circ y$ and $R^*_x : y \mapsto y \circ x$ will be used for quasigroup isotope $(H, \circ)$ of it.

Definition 2.6 (**$\mathcal{R}$-condition**). Let $(G, \cdot)$ and $(H, \circ)$ be isotopic quasigroups under the isotopism (A, B, C). $(G, \cdot)$ is said to satify the $\mathcal{R}$-condition relative to $(H, \circ)$ if for integers r, s, and t, we have

$$J^{*r} = C^{-1}J^rA, \qquad J^{*s} = A^{-1}J^sB, \qquad J^{*t} = B^{-1}J^tC.$$

It is worth to note that whenever it is mentioned that $(G,\cdot)$ is an $\mathcal{R}$-conditioned quasigroup, then it is so relative to some isotope $(H,\circ)$ of $(G,\cdot)$. Note that if $(G,\cdot)$ is an $\mathcal{R}$-conditioned quasigroup (relative to $(H,\circ)$), then $(H,\circ)$ is also $\mathcal{R}$-conditioned (relative to $(G,\cdot)$).

See [3, 4, 8, 26, 27] for a general overview on quasigroups and loops.

Lemma 2.7. (cf. [20]) *Let $(G,\cdot)$ be a quasigroup. Then the following are equivalent to each other.*

1. *$(G,\cdot)$ is a (r,s,t)-inverse quasigroup.*
2. *$L_xJ^rR_{xJ^s}=J^t\ \ \forall\ x\in G$.*
3. *$R_xJ^{-t}L_{xJ^{-s}}=J^{-r}\ \ \forall\ x\in G$.*

Lemma 2.8. (cf. [19]) *An (r,s,t)-inverse loop $(G,\cdot)$ with identity element e in which $x\cdot xJ=e\ \forall\ x\in G$ is an r-inverse loop.*

Lemma 2.9. (cf. [20]) *J^{r+s+t} is an automorphism of an (r,s,t)-inverse quasigroup.*

3. Main results

Theorem 3.1. *Let $(G,\cdot)$ be a quasigroup that satisfies the $\mathcal{R}$-condition relative to an isotope $(H,\circ)$. $(G,\cdot)$ is an (r,s,t)-inverse quasigroup if and only if $(H,\circ)$ is an (r,s,t)-inverse quasigroup.*

Proof. Necessary condition: Let $(A,B,C):G\longrightarrow H$ be an isotopism from $(G,\cdot)$ onto $(H,\circ)$. Then, we have that $xA\circ yB=(xy)C\ \forall\ x,y\in G$. Now, $xA\circ yB=(xy)C\Rightarrow yBL^*_{xA}=yL_xC\Rightarrow L_x=BL^*_{xA}C^{-1}$. Also, $xA\circ yB=(xy)C\Rightarrow xAR^*_{yB}=xR_yC\Rightarrow R_y=AR^*_{yB}C^{-1}$. Since $(G,\cdot)$ is an (r,s,t)-inverse quasigroup, from Lemma 2.7, we have that $L_xJ^rR_{xJ^s}=J^t$. Applying the isotopism to $L_xJ^rR_{xJ^s}=J^t$, we obtain $BL^*_{xA}C^{-1}J^rAR^*_{xJ^sB}C^{-1}=J^t$. Hence, $L^*_{xA}C^{-1}J^rAR^*_{xJ^sB}=B^{-1}J^tC$. By the assumption that $(G,\cdot)$ is $\mathcal{R}$-conditioned, we have $L^*_{xA}J^{*r}R^*_{xAJ^{*s}}=J^{*t}$. Therefore, by Lemma 2.7, $(H,\circ)$ is an (r,s,t)-inverse quasigroup.

Sufficient condition: Recall that if $(G,\cdot)$ is a $\mathcal{R}$-conditioned quasigroup (relative to $(H,\circ)$), then $(H,\circ)$ is also $\mathcal{R}$-conditioned (relative to $(G,\cdot)$). Hence, assume that $(H,\circ)$ is an (r,s,t)-inverse quasigroup and the proof follows by a similar argument like the necessity part. □

Remark 3.2. Theorem 3.1 shows that under the $\mathcal{R}$-condition, the (r,s,t)-inverse property is isotopic invariant. Hence, under the $\mathcal{R}$-condition, (r,s,t)-inverse quasigroups are universal.

Theorem 3.3. *Let $(G,\cdot)$ and $(H,\circ)$ be loops satisfying the $\mathcal{R}$-condition, under a middle isotopism, such that $x\cdot xJ = e_G$ and $u\circ uJ^* = e_H$, where e_G and e_H are the identity elements in G and H respectively, for all $x\in G$ and $u\in H$. $(G,\cdot)$ is an (r,s,t)-inverse loop if and only if $(H,\circ)$ is an (r,s,t)-inverse loop. Furthermore, either of the loops has an r-weak inverse permutation.*

Proof. The first part follows from Theorem 3.1. Now, from Lemma 2.8, we can put $s=r+1$ and $t=r$ so that the $\mathcal{R}$-condition becomes

$$J^{*r} = C^{-1}J^rA = B^{-1}J^rC,$$
$$J^{*r+1} = A^{-1}J^{r+1}B.$$

From (1), $C^{-1}J^rA = B^{-1}J^rC$ so that $BC^{-1}J^rAC^{-1} = J^r$. Since $A=B$ (consequence of the middle isotopism), we have that $BC^{-1}J^rBC^{-1} = J^r$. It follows from Definiton 2.1 that $\beta = BC^{-1}$ is an r-weak inverse permutation of $(G,\cdot)$. Similar reasoning can be used to show the existence of an r-weak inverse permutation for $(H,\circ)$. The proof is complete. □

Remark 3.4. It is interesting to note that if $(G,\cdot)$ in Theorem 3.3 has a trivial set of r-weak inverse permutations, then $\beta = BC^{-1} = I$, where I is the identity map on G. Hence, $B=C$. Consequently, $(G,\cdot)$ is isomorphic to $(H,\circ)$. Therefore, we have the following theorem.

Theorem 3.5. *If two loops are $\mathcal{R}$-conditioned under a middle isotopism and any of them is an (r,s,t)-inverse loop and has a trivial set of r-weak inverse permutations, then the two loops are both (r,s,t)-inverse loops that are isomorphic.*

Remark 3.6. Theorem 3.5 gives some conditions for isotopy-isomorphy for (r,s,t)-inverse loops.

Lemma 3.7. *If $(G,\cdot)$ and $(H,\circ)$ are isotopic (r,s,t)-inverse quasigroup under the triple $\alpha=(A,B,C)$, then $J^rR_{xJ^s}J^{-t}B = CJ^{*r}R^*_{xAJ^{*s}}J^{*-t}$ and $J^{-t}L_{xJ^{-s}}J^rA = CJ^{*-t}L^*_{xBJ^{*-s}}J^{*r}$.*

Proof. Since $(A,B,C): G \to H$ is an isotopism from $(G,\cdot)$ onto $(H,\circ)$, then

$$xA \circ yB = (xy)C \quad \forall\ x,y \in G. \tag{1}$$

Consequently, we have the identities

$$L_x = BL^*_{xA}C^{-1} \Leftrightarrow R_x = AR^*_{xB}C^{-1}. \tag{2}$$

If $(G,\cdot)$ is an (r,s,t)-inverse quasigroup, then

$$L_xJ^rR_{xJ^s} = J^t \Leftrightarrow R_xJ^{-t}L_{xJ^{-s}} = J^{-r}. \tag{3}$$

Hence,

$$L_x = J^tR^{-1}_{xJ^s}J^{-r} \Leftrightarrow R_x = J^{-r}L^{-1}_{xJ^{-s}}J^t \quad \forall\ x \in G. \tag{4}$$

Similarly, If $(H,\circ)$ is an (r,s,t)-inverse quasigroup, then

$$L^*_u = J^{*t}R^{*-1}_{uJ^{*s}}J^{*-r} \Leftrightarrow R^*_u = J^{*-r}L^{*-1}_{uJ^{*-s}}J^{*t} \quad \forall\ u \in H \tag{5}$$

Applying (4) and (5) to (2), we obtain

$$J^tR^{-1}_{xJ^s}J^{-r} = BJ^{*t}R^{*-1}_{xAJ^s}J^{*-r}C^{-1} \Leftrightarrow J^{-r}L^{-1}_{xJ^{-s}}J^t = AJ^{*-r}L^{*-1}_{xBJ^{*-s}}J^{*t}C^{-1}. \tag{6}$$

Taking inverse of both sides of the identities, we have

$$J^rR_{xJ^s}J^{-t} = CJ^{*r}R^*_{xAJ^s}J^{*-t}B^{-1} \Leftrightarrow J^{-t}L_{xJ^{-s}}J^r = CJ^{*-t}L^*_{xBJ^{*-s}}J^{*r}A^{-1}. \tag{7}$$

Therefore,

$$J^rR_{xJ^s}J^{-t}B = CJ^{*r}R^*_{xAJ^{*s}}J^{*-t} \Leftrightarrow J^{-t}L_{xJ^{-s}}J^rA = CJ^{*-t}L^*_{xBJ^{*-s}}J^{*r}. \tag{8}$$

The result follows immediately □

Theorem 3.8. *Let $(G,\cdot)$ and $(H,\circ)$ be isotopic (r,s,t)-inverse loops, with identity elements e_G and e_H respectively, under the isotopism $(A,B,C): G \to H$, then*

1. $(G,\cdot) \cong (H,\circ) \Leftrightarrow (J^{-r}L^{-1}_{bJ^{-s}}J^t, J^tR^{-1}_{aJ^s}J^{-r}, CJ^{*t-r}C^{-1}) \in ATP(G,\cdot)$ *where $a = e_HA^{-1}$ and $b = e_HB^{-1}$ are in G.*
2. $(G,\cdot) \cong (H,\circ) \Leftrightarrow (J^{*-r}L^*_{bJ^{*-s}}J^{*r}, J^{*r}R^*_{aJ^{*s}}J^{*-t}, C^{-1}J^{r-t}C) \in ATP(H,\circ)$ *where $a = e_GA$ and $b = e_GB$ are in H.*

Proof. Put $x = e_H A^{-1} \in G$ in $J^r R_{xJ^s} J^{-t} B = CJ^{*r} R^*_{xAJ^{*s}} J^{*-t}$ of equation (8) of Lemma 3.7. Therefore, $J^r R_{e_H A^{-1} J^s} J^{-t} B = CJ^{*r-t} \Leftrightarrow B = J^t R^{-1}_{aJ^s} J^{-r} CJ^{*r-t}$, where $a = e_H A^{-1}$. Now, put $x = e_H B^{-1}$ in $J^{-t} L_{xJ^{-s}} J^r A = CJ^{*-t} L^*_{xBJ^{*-s}} J^{*r}$ in (8) of Lemma 3.7, to obtain $J^{-t} L_{e_H B^{-1} J^{-s}} J^r A = CJ^{*r-t} \Leftrightarrow A = J^{-r} L^{-1}_{bJ^{-s}} J^t CJ^{*r-t}$. Therefore, the isotopism $(A, B, C) : G \to H$ becomes

$$(A, B, C) = (J^{-r} L^{-1}_{bJ^{-s}} J^t CJ^{*r-t}, J^t R^{-1}_{aJ^s} J^{-r} CJ^{*r-t}, C).$$

Observe that (1) can be decomposed into

$$(A, B, C) = (J^{-r} L^{-1}_{bJ^{-s}} J^t, J^t R^{-1}_{aJ^s} J^{-r}, CJ^{*t-r} C^{-1})(CJ^{*r-t}, CJ^{*r-t}, CJ^{*r-t}).$$

Consequently, if $(CJ^{*r-t}, CJ^{*r-t}, CJ^{*r-t})$ is an isomorphism from $(G, \cdot)$ onto $(H, \circ)$, then $(J^{-r} L^{-1}_{bJ^{-s}} J^t, J^t R^{-1}_{aJ^s} J^{-r}, CJ^{*t-r} C^{-1}) \in \mathrm{ATP}(G, \cdot)$ and conversely. This completes the first part.

The second result is approached similarly, but in this case, we put $x = e_G$ in both identities in (8) of Lemma 3.7. □

Remark 3.9. Theorem 3.8 characterizes isotopy-isomorphy in (r, s, t)-inverse loops.

Theorem 3.10. *Let $(G, \cdot)$ and $(H, \circ)$ be two finite quasigroups, isotopic under the triple (A, B, C) such that they obey the $\mathcal{R}$-condition. If $(G, \cdot)$ is an (r, s, t)-inverse quasigroup with an inverse-cycle of length n, where n is a positive integer, then $(H, \circ)$ is an (r, s, t)-inverse quasigroup with an inverse-cycle of length $n(r + s + t)$ and n is the order of an automorphism of $(H, \circ)$.*

Proof. $(G, \cdot)$ is an (r, s, t)-inverse quasigroup if and only if $(H, \circ)$ is an (r, s, t)-inverse quasigroup follows from Theorem 3.1. Now, $(G, \cdot)$ has an inverse-cycle of length n if and only if $J^n = I_G$, where $I_G : G \to G$ is the identity map on G. From the $\mathcal{R}$-condition, we therefore , have that $J^{*(r+s+t)} = C^{-1} J^{(r+s+t)} C$. We proceed by induction on $n \in \mathbb{Z}^+$ as follows:

$$J^{*2(r+s+t)} = (C^{-1} J^{(r+s+t)} C)(C^{-1} J^{(r+s+t)} C) = C^{-1} J^{2(r+s+t)} C,$$

$$J^{*3(r+s+t)} = (C^{-1} J^{2(r+s+t)} C)(C^{-1} J^{(r+s+t)} C) = C^{-1} J^{3(r+s+t)} C.$$

Suppose for $k \in \mathbb{Z}$, we have $J^{*k(r+s+t)} = C^{-1} J^{k(r+s+t)} C$. Therefore,

$$J^{*(k+1)(r+s+t)} = (C^{-1} J^{k(r+s+t)} C)(C^{-1} J^{(r+s+t)} C) = C^{-1} J^{(k+1)(r+s+t)} C$$

Hence, by mathematical induction, $J^{*n(r+s+t)} = C^{-1}J^{n(r+s+t)}C \; \forall \; n \in \mathbb{Z}^+$. But $J^n = I_G$. So, $J^{*n(r+s+t)} = C^{-1}J^{n(r+s+t)}C = C^{-1}C = I_H$, where I_H is the identity map on H. Therefore, $(H, \circ)$ has an inverse-cycle of length $n(r + s + t)$. Observe that $I_H = J^{*n(r+s+t)} = (J^{*(r+s+t)})^n$. From Lemma 2.9, $J^{*(r+s+t)}$ is an automorphism of $(H, \circ)$. Thus we conclude that n is the order of $J^{*(r+s+t)}$. The proof is complete. □

Remark 3.11. It can be shown in a similar way as in Theorem 3.10 that if $(H, \circ)$ has an inverse-cycle of length n, then $(G, \cdot)$ has an inverse-cycle of length $n(r + s + t)$ and n is the order of the automorphism $J^{(r+s+t)}$ of $(G, \cdot)$.

4. Applications to cryptography

In application, it is assumed that the message to be transmitted can be represented as single element y of an (r, s, t)-inverse quasigroup $(G, \cdot)$ and that this is enciphered by pre-multiplying by another element x of G and then compute $(xy)J^r$ which gives the cipher text. At the receiving end, the message is deciphered by post-multiplying by xJ^s to get yJ^t from which the plain text message y can be extracted.

Let $(G, \cdot)$ be a (r, s, t)-inverse quasigroup of order $|G| = 3k$ with an inverse cycle of length n where $n, k \in \mathbb{N}$. Let $(H, \circ)$ be a quasigroup that is isotopic to $(G, \cdot)$ under the $\mathcal{R}$ condition. Then by Theorem 3.1, H is a (r, s, t)-inverse quasigroup of order $|H| = 3k$ and by Theorem 3.10, H has an inverse cycle of length $n(r + s + t)$. Going by Theorem 2.5, the (r, s, t)-inverse quasigroup G exists provided $\gcd(k, r + s + t) > 1$ and the inverse cycle of G is of length $\gcd(k, r + s + t)$. Thus, the inverse cycle of H is of length $(r + s + t) \times \gcd(k, r + s + t)$. Consequently, we have the result in Corollary 4.1.

Corollary 4.1. *Let $(G, \cdot)$ and $(H, \circ)$ be two finite quasigroups, isotopic under the triple (A, B, C) such that they obey the $\mathcal{R}$-condition. Let r, s and t be positive integers. If $(G, \cdot)$ is an (r, s, t)-inverse quasigroup of order $3k$ with an inverse-cycle of length $gcd(k, r + s + t) > 1$, then $(H, \circ)$ is an (r, s, t)-inverse quasigroup of order $3k$ with an inverse-cycle of length $gcd\big(k(r + s + t), (r + s + t)^2\big) > 1$. Moreover, $gcd(k, r + s + t) > 1$ is the order of the automorphism $J^{*(r+s+t)}$ of $(H, \circ)$.*

Theorem 3.1 is structured by the choice of the triple (A, B, C) being an isotopism of G onto H such that the $\mathcal{R}$ condition holds. So, the secret key for the system is the pair $\{(A, B, C), \mathcal{R}\}$.

Thus, whenever a set of information or messages is to be transmitted, the sender will encrypt in an (r, s, t)-inverse quasigroup G (as described earlier on) and then encrypt again with $\{(A, B, C), \mathcal{R}\}$ to get a (r, s, t)-inverse quasigroup H which is the set of encrypted messages. At the receiving end, the combined message H is decrypted by using an inverse isotopism (i.e inverse key $\{(A^{-1}, B^{-1}, C^{-1}), \mathcal{R}\}$) to get G and then decrypt again (as described earlier on) to get the plain texts. The secret key can be changed over time.

In the light of Corollary 4.1, the codomain (r, s, t)-inverse quasigroup $(H, \circ)$ has an inverse cycle of longer length than the domain (r, s, t)-inverse quasigroup $(G, \cdot)$.

S/N	k	(r, s, t)	$LIC(G)$	$LIC(H)$	Order $\|G\| = \|H\|$
1	8	(2, 3, 5)	2	20	24
2	10	(2, 3, 7)	2	24	30
3	12	(2, 3, 4)	3	27	36
4	14	(2, 3, 5)	2	20	42
5	15	(2, 3, 4)	3	27	45
6	15	(2, 3, 7)	3	36	45
7	16	(2, 3, 5)	2	20	48
8	16	(2, 3, 7)	4	48	48
9	16	(2, 4, 6)	4	48	48
10	18	(2, 3, 5)	2	20	54
11	18	(2, 3, 10)	3	45	54
12	20	(2, 3, 7)	4	48	60
13	21	(2, 3, 4)	3	27	63
14	21	(2, 3, 7)	3	36	63
15	22	(2, 3, 5)	2	20	66
16	24	(2, 3, 4)	3	27	72
17	24	(2, 3, 10)	3	45	72
18	25	(2, 3, 5)	5	50	75
19	27	(2, 3, 4)	9	81	81
20	28	(2, 3, 15)	4	80	84
21	30	(2, 3, 7)	6	72	90

Possible orders of (r, s, t)-inverse quasigroups and their lengths of inverse cycles based on Corollary 4.1

References

[1] **Artzy, R.**, *On loops with special property*, Proc. Amer. Math. Soc. **6** (1955), 448 – 453.

[2] **Artzy, R.**, *Inverse-cycles in weak-inverse loops*, Proc. Amer. Math. Soc. **68** (1978), no. 2, 132 – 134 .

[3] **Bruck, R.H.**, *A survey of binary systems*, Springer-Verlag, 1958.

[4] **Chein, O., Pflugfelder, H.O. and Smith, J.D.H.**, *Quasigroups and loops: theory and applications*, Heldermann Verlag, 1990.

[5] **Isere, A., Adeniran, J.O, Jaiyéọlá, T.G.**, *Latin quandles and application to cryptography*, Mathematics for Applications, **10** (2021), no. 1, 37 – 53.

[6] **Jaiyéọlá, T.G.**, *A Double cryptography using The Smarandache Keedwell cross inverse quasigroup*, International J. Math. Combin., **3** (2008), 28 – 33.

[7] **Jaiyéọlá, T.G.**, *Some isotopy-isomorphy conditions for m-inverse quasigroups and loops*, Analele Sti. Univ. Ovidius Constanta, Ser. Matematica, **16** (2008), no. 2, 57 – 66.

[8] **Jaiyéọlá, T.G.**, *A study of new concepts in Smarandache quasigroups and loops*, ProQuest Information and Learning(ILQ), Ann Arbor, 2009.

[9] **Jaiyéọlá, T.G.**, *On middle universal weak and cross inverse property loops with equal length of inverse cycles*, Revista Colombiana Mat., **44** (2010), no. 2, 79 – 89.

[10] **Jaiyéọlá, T.G.**, *On middle universal m-inverse quasigroups and their applications to cryptography*, Analele Univ. Vest Din Timisoara, Ser. Matematica-Informatica, **49** (2011), no. 1, 69 – 87.

[11] **Jaiyéọlá, T.G.**, *On three cryptographic identities in left universal Osborn loops*, J. Discr. Math. Sci. Cryptography, **14** (2011), no. 1, 33 – 50.

[12] **Jaiyéọlá, T.G.**, *On the application of Keedwell cross inverse quasigroup to cryptography*, Yearbook of the Faculty of Computer Science, Goce Delcev University, **1** (2012), no. 1, 264 – 277.

[13] **Jaiyéọlá, T.G.**, *On two cryptographic identities in universal Osborn loops*, J. Discr. Math. Sci. Cryptography, **16** (2013), no. 2 – 3, 95 – 116.

[14] **Jaiyéọlá, T.G. and Adéníran, J.O.**, *Weak inverse property loops and some isotopy-isomorphy properties*, Acta. Univ. Apulensis Math., **18** (2009), no. 2, 19 – 33.

[15] **Jaiyéọlá, T.G. and Adéníran, J.O.**, *On another two cryptographic identities in universal Osborn loops*, Surveys Math. Appl., **5** (2010), 17 – 34.

[16] **Jaiyéọlá, T.G. and Effiong, G.O.**, *Basarab loop and its variance with inverse properties*, Quasigroups and Related Systems **26** (2018), 229 – 238.

[17] **Jaiyéọlá, T.G. and Smarandache, F.**, *Inverse properties in neutrosophic triplet loop and their application to cryptography*, Algorithms, **11** (2018), no. 3, 32.

[18] **Keedwell, A.D.**, *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Combin., **20** (1999), 241 – 250.

[19] **Keedwell, A.D. and Shcherbacov, V.A.** , *On m-inverse loops and quasigroups with a long inverse cycle*, Australas. J. Combin. **26** (2002) 99 – 119.

[20] **Keedwell, A.D. and Shcherbacov, V.A.**, *Construction and properties of (r, s, t)-inverse quasigroups I*, Discr. Math., **266** (2003), 275 – 291.

[21] **Keedwell, A.D. and Shcherbacov, V.A.**, *Construction and properties of (r, s, t)-inverse quasigroups II*, Discr. Math., **288** (2004), 61 – 71.

[22] **Keedwell, A.D. and Shcherbacov, V A.**, *Quasigroups with an inverse property and generalized parastrophic identities*, Quasigroups and Related Systems **13** (2005), 109 – 124.

[23] **Looney, C.**, *On m-inverse loops and quasigroups of order n with a long inverse cycle*, Ph.D. Thesis, Univ. Texas at Arlington, ProQuest LLC, Ann Arbor, MI. 2015.

[24] **Ogunrinade, S.O., Ajala, S.O., Olaleru, J.O. and Jaiyéọlá, T.G.**, *Holomorph of self-distributive quasigroup with key laws*, Intern. J. Math. Analysis and Optimization: Theory and Applications, **2019** (2019), no. 1, 426 – 432.

[25] **Oyebo, Y.T., Jaiyéọlá, T.G. and Adeniran, J.O.**, *A study of the holomorphy of (r, s, t)-inverse loops*, J. Discr. Math. Sci. Cryptography. Published online: 14 Nov 2021.

[26] **Pflugfelder, H.O.**, *Quasigroups and loops: Introduction,* Sigma Series in Pure Math. **7,** Heldermann Verlag, Berlin. 1990.

[27] **Shcherbacov, V.A.**, *Elements of quasigroup theory and applications*, CRC Press, Boca Raton, FL, 2017.

Received August 5, 2022

R. Ilemobade and T.G. Jaiyeola
Department of Mathematics, Obafemi Awolowo University, Ile-Ife, Nigeria
E-mails: richardilemobade@gmail.com,
jaiyeolatemitope@yahoo.com, tjayeola@oauife.edu.ng

G. Olufemi
Department of Mathematics, University of Lagos, Akoka, Yaba, Nigeria.
E-mail: oogeorge@unilag.edu.ng