On Middle Universal m-Inverse Quasigroups And Their Applications To Cryptography *†

Tèmítọ́pẹ́ Gbọ́láhàn Jaíyéọlá‡
Department of Mathematics,
Obafemi Awolowo University, Ile Ife, Nigeria.
jaiyeolatemitope@yahoo.com, tjayeola@oauife.edu.ng

Abstract

This study presents a special type of middle isotopism under which m-inverse quasigroups are isotopic invariant. A sufficient condition for an m-inverse quasigroup that is specially isotopic to a quasigroup to be isomorphic to the quasigroup isotope is established. It is shown that under this special type of middle isotopism, if n is a positive even integer, then, a quasigroup is an m-inverse quasigroup with an inverse cycle of length nm if and only if its quasigroup isotope is an m-inverse quasigroup with an inverse cycle of length nm. But when n is an odd positive integer. Then, if a quasigroup is an m-inverse quasigroup with an inverse cycle of length nm, its quasigroup isotope is an m-inverse quasigroup with an inverse cycle of length nm if and only if the two quasigroups are isomorphic. Hence, they are isomorphic m-inverse quasigroups. Explanations and procedures are given on how these results can be used to apply m-inverse quasigroups to cryptography, double cryptography and triple cryptography.

1 Introduction

Let L be a non-empty set. Define a binary operation $(\cdot)$ on L : If $x \cdot y \in L$ for all $x, y \in L$, $(L, \cdot)$ is called a groupoid. If the system of equations ;

$$a \cdot x = b \qquad \text{and} \qquad y \cdot a = b$$

have unique solutions for x and y respectively, then $(L, \cdot)$ is called a quasigroup. For each $x \in L$, the elements $x^{\rho} = xJ_{\rho}, x^{\lambda} = xJ_{\lambda} \in L$ such that $xx^{\rho} = e$ and $x^{\lambda}x = e$ are called the right, left inverses of x respectively. Now, if there exists a unique element $e \in L$ called the identity element such that for all $x \in L$, $x \cdot e = e \cdot x = x$, $(L, \cdot)$ is called a loop.

*2000 Mathematics Subject Classification. Primary 20NO5 ; Secondary 08A05
†**Keywords and Phrases :** m-inverse quasigroups, $\mathcal{T}_m$ condition,length of inverse cycles, cryptography
‡All correspondence to be addressed to this author.

Karklinüsh and Karkliň [11] introduced m-inverse loops. A loop is an m-inverse loop(m-IL) if and only if it obeys any of the equivalent conditions

$$(xy)J_\rho^m \cdot xJ_\rho^{m+1} = yJ_\rho^m \qquad \text{and} \qquad xJ_\lambda^{m+1} \cdot (yx)J_\lambda^m = yJ_\lambda^m.$$

Keedwell and Shcherbacov [11] originally defined an m-inverse quasigroup(m-IQ) as a quasigroup that obeys the identity $(xy)J^m \cdot xJ^{m+1} = yJ^m$ such that J is a permutation. For the sake of this present study, we shall take $J = J_\rho$ and so m-IQs obey the equivalent identities that define m-ILs.

m-IQs and m-ILs are generalizations of WIPLs and CIPLs, which corresponds to $m = -1$ and $m = 0$ respectively. After the study of m-inverse loops by Keedwell and Shcherbacov [10], they have also generalized them to quasigroups called (r, s, t)-inverse quasigroups in [12] and [13]. Keedwell and Shcherbacov [10] investigated the existence of m-inverse quasigroups and loops with long inverse cycle such that $m \geq 1$.They were able to establish that the direct product of two m-inverse quasigroups is an m-inverse quasigroup.

Consider $(G, \cdot)$ and $(H, \circ)$ been two distinct groupoids(quasigroups, loops). Let A, B and C be three distinct non-equal bijective mappings, that maps G onto H. The triple $\alpha = (A, B, C)$ is called an isotopism of $(G, \cdot)$ onto $(H, \circ)$ if and only if

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

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

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

As observed by Osborn [14], a loop is a WIPL and an AIPL if and only if it is a CIPL. The past efforts of Artzy [1, 4, 3, 2], Belousov and Tzurkan [5] and recent studies of Keedwell [10], Keedwell and Shcherbacov [11, 12, 13] are of great significance in the study of WIPLs, AIPLs, CIPQs and CIPLs, their generalizations(i.e m-inverse loops and quasigroups, (r,s,t)-inverse quasigroups) and applications to cryptography.

In the quest for the application of CIPQs with long inverse cycles to cryptography, Keedwell [10] constructed the a CIPQ. The author also gave examples and detailed explanation and procedures of the use of this CIPQ for cryptography. Cross inverse property quasigroups have been found appropriate for cryptography because of the fact that the left and

right inverses x^{λ} and x^{ρ} of an element x do not coincide unlike in left and right inverse property loops, hence this gave rise to what is called 'cycle of inverses' or 'inverse cycles' or simply 'cycles' i.e finite sequence of elements $x_1, x_2, \cdots, x_n$ such that $x_k^{\rho} = x_{k+1} \mod n$. The number n is called the length of the cycle. The origin of the idea of cycles can be traced back to Artzy [1, 4] where he also found there existence in WIPLs apart form CIPLs. In his two papers, he proved some results on possibilities for the values of n and for the number m of cycles of length n for WIPLs and especially CIPLs. We call these "Cycle Theorems" for now.

The universality of WIPLs and CIPLs have been addressed by OSborn [14] and Artzy [2] respectively. Artzy showed that isotopic CIPLs are isomorphic. In 1970, Basarab [7] later continued the work of Osborn of 1961 on universal WIPLs by studying isotopes of WIPLs that are also WIPLs after he had studied a class of WIPLs([6]) in 1967. Osborn [14], while investigating the universality of WIPLs discovered that a universal WIPL $(G, \cdot)$ obeys the identity

$$yx \cdot (zE_y \cdot y) = (y \cdot xz) \cdot y \ \forall \ x, y, z \in G \tag{1}$$

where $E_y = L_y L_{y^{\lambda}} = R_{y^{\rho}}^{-1} R_y^{-1} = L_y R_y L_y^{-1} R_y^{-1}$.

Eight years after Osborn's [14] 1960 work on WIPL, in 1968, Huthnance Jr. [9] studied the theory of generalized Moufang loops. He named a loop that obeys (1) a generalized Moufang loop and later on in the same thesis, he called them M-loops. On the other hand, he called a universal WIPL an Osborn loop and this same definition was adopted by Chiboka [8].

From the literature review stated above, it can be seen that neither WIPLs nor CIPLs has been shown to be isotopic invariant. In fact, it is yet to be shown that there exist a special type of isotopism(e.g left, right or middle isotopism) under which the WIP or CIP is isotopic invariant. Aside this, there has never been any investigation into the isotopy of m-inverse quasigroups and loops.

The aim of the present study is to present a special type of middle isotopism under which m-inverse quasigroups are isotopic invariant. A sufficient condition for an m-inverse quasigroup that is specially isotopic to a quasigroup to be isomorphic to the quasigroup isotope is established. It is shown that under this special type of middle isotopism, if n is a positive even integer, then, a quasigroup is an m-inverse quasigroup with an inverse cycle of length nm if and only if its quasigroup isotope is an m-inverse quasigroup with an inverse cycle of length nm. But when n is an odd positive integer. Then, if a quasigroup is an m-inverse quasigroup with an inverse cycle of length nm, its quasigroup isotope is an m-inverse quasigroup with an inverse cycle of length nm if and only if the two quasigroups are isomorphic. Hence, they are isomorphic m-inverse quasigroups. Explanations and procedures are given on how these results can be used to apply m-inverse quasigroups to cryptography, double cryptography and triple cryptography.

2 Preliminaries

Definition 2.1 *Let L be a quasigroup and $m \in \mathbb{Z}$. Let $x^{\rho^m} = xJ_\rho^m$ and $x^{\lambda^m} = xJ_\lambda^m$ for all $x \in L$. A mapping $\alpha \in SYM(L)$(where $SYM(L)$ is the group of all bijections on L) which obeys the identity $x^{\rho^m} = [(x\alpha)^{\rho^m}]\alpha$ is called a m-weak right inverse permutation. Their set is represented by $S_{(\rho,m)}(L)$.*

Similarly, if α obeys the identity $x^{\lambda^m} = [(x\alpha)^{\lambda^m}]\alpha$ it is called a m-weak left inverse permutation. Their set is represented by $S_{(\lambda,m)}(L)$

If α satisfies both, it is called an m-weak inverse permutation. Their set is represented by $S'_m(L)$.

It can be shown that $\alpha \in SYM(L)$ is a m-weak right inverse if and only if it is a m-weak left inverse permutation. So, $S'_m(L) = S_{(\rho,m)}(L) = S_{(\lambda,m)}(L)$. And thus, α is called and m-weak inverse permutation.

Remark 2.1 *Every permutation of order 2 that preserves the right(left) inverse of each element in a m-inverse quasigroup is a m-weak right(left) inverse permutation.*

Throughout, we shall employ the use of the bijections; $J_\rho : x \mapsto x^\rho$, $J_\lambda : x \mapsto x^\lambda$, $L_x : y \mapsto xy$ and $R_x : y \mapsto yx$ for a loop and the bijections; $J'_\rho : x \mapsto x^{\rho'}$, $J'_\lambda : x \mapsto x^{\lambda'}$, $L'_x : y \mapsto xy$ and $R'_x : y \mapsto yx$ for its loop isotope. If the identity element of a loop is e then that of the isotope shall be denoted by e'.

Lemma 2.1 *In a quasigroup, the set of weak inverse permutations that commute form an abelian group.*

Definition 2.2 *($\mathcal{T}$-condition)*

Let $(G,\cdot)$ and $(H,\circ)$ be two distinct quasigroups that are isotopic under the triple (A,B,C). $(G,\cdot)$ obeys the $\mathcal{T}_{(1,m)}$ condition if and only if $A = B$. $(G,\cdot)$ obeys the $\mathcal{T}_{(2,m)}$ condition if and only if $J'^m_\rho = C^{-1}J^m_\rho A = B^{-1}J^m_\rho C$. $(G,\cdot)$ obeys the $\mathcal{T}_{(3,m)}$ condition if and only if $J'^m_\lambda = C^{-1}J^m_\lambda B = A^{-1}J^m_\lambda C$. So, $(G,\cdot)$ obeys the $\mathcal{T}_m$ condition if and only if it obey $\mathcal{T}_{(1,m)}$ and $\mathcal{T}_{(2,m)}$ conditions or $\mathcal{T}_{(1,m)}$ and $\mathcal{T}_{(3,m)}$ conditions since $\mathcal{T}_{(2,m)} \equiv \mathcal{T}_{(3,m)}$.

It must here by be noted that the $\mathcal{T}_m$-conditions refer to a pair of isotopic loops at a time. This statement might be omitted at times. That is whenever we say a loop $(G,\cdot)$ has the $\mathcal{T}_m$-condition, then this is relative to some isotope $(H,\circ)$ of $(G,\cdot)$

Lemma 2.2 *Let L be a quasigroup. The following are equivalent.*

1. *L is a m-inverse quasigroup.*
2. *$R_x J^m_\lambda L_{xJ^{m+1}_\lambda} = J^m_\lambda$ for all $x \in L$.*
3. *$L_x J^m_\rho R_{xJ^{m+1}_\rho} = J^m_\rho$ for all $x \in L$.*

3 Main Results

Theorem 3.1 *Let $(G,\cdot)$ and $(H,\circ)$ be two distinct quasigroups that are isotopic under the triple (A,B,C).*

1. *If the pair of $(G,\cdot)$ and $(H,\circ)$ obey the $\mathcal{T}_m$ condition, then $(G,\cdot)$ is an m-inverse quasigroup if and only if $(H,\circ)$ is an m-inverse quasigroup.*

2. *If $(G,\cdot)$ and $(H,\circ)$ are m-inverse quasigroups, then $J_\rho^m R_{xJ_\rho^{m+1}} J_\lambda^m B = C J_\rho'^m R'_{xAJ_\rho'^{m+1}} J_\lambda'^m$ and $J_\lambda^m L_{xJ_\lambda^{m+1}} J_\rho^m A = C J_\lambda'^m L'_{xBJ_\lambda'^{m+1}} J_\rho'^m$ for all $x \in G$.*

Proof

1. $(A,B,C) : G \to H$ is an isotopism $\Leftrightarrow xA \circ yB = (x\cdot y)C \Leftrightarrow yBL'_{xA} = yL_xC \Leftrightarrow BL'_{xA} = L_xC \Leftrightarrow L'_{xA} = B^{-1}L_xC \Leftrightarrow$

$$L_x = BL'_{xA}C^{-1} \tag{2}$$

Also, $(A,B,C) : G \to H$ is an isotopism $\Leftrightarrow xAR'_{yB} = xR_yC \Leftrightarrow AR'_{yB} = R_yC \Leftrightarrow R'_{yB} = A^{-1}R_yC \Leftrightarrow$

$$R_y = AR'_{yB}C^{-1} \tag{3}$$

Let G be an m-inverse quasigroup. Applying (2) and (3) to Lemma 2.2 separately, we have : $L_xJ_\rho^m R_{xJ_\rho^{m+1}} = J_\rho^m$, $R_xJ_\lambda^m L_{xJ_\lambda^{m+1}} = J_\lambda^m \Rightarrow (AR'_{xB}C^{-1})J_\lambda^m(BL'_{xJ_\lambda^{m+1}A}C^{-1}) = J_\lambda^m$, $(BL'_{xA}C^{-1})J_\rho^m(AR'_{xJ_\rho^{m+1}B}C^{-1}) = J_\rho^m \Leftrightarrow AR'_{xB}(C^{-1}J_\lambda^m B)L'_{xJ_\lambda^{m+1}A}C^{-1} = J_\lambda^m$, $BL'_{xA}(C^{-1}J_\rho^m A)R'_{xJ_\rho^{m+1}B}C^{-1} = J_\rho^m \Leftrightarrow$

$$R'_{xB}(C^{-1}J_\lambda^m B)L'_{xJ_\lambda^{m+1}A} = A^{-1}J_\lambda^m C,\ L'_{xA}(C^{-1}J_\rho^m A)R'_{xJ_\rho^{m+1}B} = B^{-1}J_\rho^m C. \tag{4}$$

Let $J_\lambda'^m = C^{-1}J_\lambda^m B = A^{-1}J_\lambda^m C$, $J_\rho'^m = C^{-1}J_\rho^m A = B^{-1}J_\rho^m C$. Then, $J'_\lambda = C^{-1}J_\lambda B$, $J'_\rho = C^{-1}J_\rho A$. So, $J_\lambda'^{m+1} = (A^{-1}J_\lambda^m C)(C^{-1}J_\lambda B) = A^{-1}J_\lambda^{m+1}B$, $J_\rho'^{m+1} = (B^{-1}J_\rho^m C)(C^{-1}J_\rho^A) = B^{-1}J_\rho^{m+1}A$.

Then, from (4), and using the $\mathcal{T}_m$-condition, we have

$$R'_{xB}J_\lambda'^m L'_{xJ_\lambda^{m+1}A} = J_\lambda'^m = R'_{xB}J_\lambda'^m L'_{xAJ_\lambda'^{m+1}B^{-1}A} = R'_{xA}J_\lambda'^m L'_{xAJ_\lambda'^{m+1}}, \tag{5}$$

$$L'_{xA}J_\rho'^m R'_{xJ_\rho^{m+1}B} = J_\rho'^m = L'_{xA}J_\rho'^m R'_{xBJ_\rho'^{m+1}A^{-1}B} = L'_{xB}J_\rho'^m R'_{xBJ_\rho'^{m+1}} \tag{6}$$

Thus, by Lemma 2.2, (5) and (6) H is a m-inverse quasigroup. This completes the proof of the forward part. To prove the converse, carry out the same procedure, assuming the $\mathcal{T}_m$ condition and the fact that $(H,\circ)$ is a m-inverse quasigroup.

2. If $(H, \circ)$ is a m-inverse quasigroup, then

$$L'_x J'^m_\rho R'_{xJ'^{m+1}_\rho} = J'^m_\rho \Leftrightarrow R'_x J'^m_\lambda L'_{xJ'^{m+1}_\lambda} = J'^m_\lambda \ \forall \ x \in H \tag{7}$$

while since G is a m-inverse quasigroup,

$$L_x J^m_\rho R_{xJ^{m+1}_\rho} = J^m_\rho \Leftrightarrow R_x J^m_\lambda L_{xJ^{m+1}_\lambda} = J^m_\lambda \ \forall \ x \in G \tag{8}$$

From (7),

$$R'_x = J'^m_\lambda L'^{-1}_{xJ'^{m+1}_\lambda} J'^m_\rho \Leftrightarrow L'_x = J'^m_\rho R'^{-1}_{xJ'^{m+1}_\rho} J'^m_\lambda \ \forall \ x \in H \tag{9}$$

while from (8),

$$R_x = J^m_\lambda L^{-1}_{xJ^{m+1}_\lambda} J^m_\rho \Leftrightarrow L_x = J^m_\rho R^{-1}_{xJ^{m+1}_\rho} J^m_\lambda \ \forall \ x \in G. \tag{10}$$

The fact that G and H are isotopic implies that

$$L_x = BL'_{xA}C^{-1} \ \forall \ x \in G \ and \tag{11}$$

$$R_x = AR'_{xB}C^{-1} \ \forall \ x \in G. \tag{12}$$

So, using (9) and (10) in (11) we get

$$J^m_\rho R^{-1}_{xJ^{m+1}_\rho} J^m_\lambda = BJ'^m_\rho R'^{-1}_{xAJ'^{m+1}_\rho} J'^m_\lambda C^{-1} \ \forall \ x \in G \tag{13}$$

while using (9) and (10) in (12) we get

$$J^m_\lambda L^{-1}_{xJ^{m+1}_\lambda} J^m_\rho = AJ'^m_\lambda L'^{-1}_{xBJ'^{m+1}_\lambda} J'^m_\rho C^{-1} \ \forall \ x \in G. \tag{14}$$

Thus, (13) becomes

$$J^m_\rho R_{xJ^{m+1}_\rho} J^m_\lambda = CJ'^m_\rho R'_{xAJ'^{m+1}_\rho} J'^m_\lambda B^{-1} \Leftrightarrow J^m_\rho R_{xJ^{m+1}_\rho} J^m_\lambda B = CJ'^m_\rho R'_{xAJ'^{m+1}_\rho} J'^m_\lambda \ \forall \ x \in G$$

while (14) becomes

$$J^m_\lambda L_{xJ^{m+1}_\lambda} J^m_\rho = CJ'^m_\lambda L'_{xBJ'^{m+1}_\lambda} J'^m_\rho A^{-1} \Leftrightarrow J^m_\lambda L_{xJ^{m+1}_\lambda} J^m_\rho A = CJ'^m_\lambda L'_{xBJ'^{m+1}_\lambda} J'^m_\rho \ \forall \ x \in G.$$

These completes the proof.

Theorem 3.2 *Let $(G, \cdot)$ and $(H, \circ)$ be two distinct quasigroups that are isotopic under the triple (A, B, C) such that they obey the $\mathcal{T}_m$ condition.*

1. *If n is an even positive integer. Then, $(G, \cdot)$ is a m-inverse quasigroup with an inverse cycle of length nm if and only if $(H, \circ)$ is a m-inverse quasigroup with an inverse cycle of length nm.*

2. *If n is an odd positive integer. Then, if $(G,\cdot)$ or $(H,\circ)$ is an m-inverse quasigroup with an inverse cycle of length nm then, $(H,\circ)$ or $(G,\cdot)$ is an m-inverse quasigroup with an inverse cycle of length nm if and only if $(G,\cdot)\cong(H,\circ)$.*

Proof
The fact that $(G,\cdot)$ is a m-inverse quasigroup if and only if $(H,\circ)$ is a m-inverse quasigroup has been proved in Theorem 3.1.

1. It will now be shown that $(G,\cdot)$ has an inverse cycle of length nm if and only if $(H,\circ)$ has an inverse cycle of length nm. An m-inverse quasigroup $(G,\cdot)$ has an inverse cycle of length nm if and only if $|J_\rho^m|=n$. Recall that $J_\rho'^m=C^{-1}J_\rho^m A$ and $J_\rho'^m=B^{-1}J_\rho^m C$ if and only if $CJ_\rho'^m A^{-1}=J_\rho^m$ and $BJ_\rho'^m C^{-1}=J_\rho^m$. Consider the following inductive process.

$$J_\rho^{2m}=\underbrace{CJ_\rho'^m A^{-1}BJ_\rho'^m C^{-1}}_{2=2\times1}=CJ_\rho'^{2m}C^{-1}\ ,J_\rho^{4m}=\underbrace{CJ_\rho'^{2m}C^{-1}CJ_\rho'^{2m}C^{-1}}_{4=2\times2}=CJ_\rho'^{4m}C^{-1}$$
$$J_\rho^{6m}=\underbrace{CJ_\rho'^{4m}C^{-1}CJ_\rho'^{2m}C^{-1}}_{6=2\times3}=CJ_\rho'^{6m}C^{-1}\ ,J_\rho^{8m}=\underbrace{CJ_\rho'^{6m}C^{-1}CJ_\rho'^{2m}C^{-1}}_{8=2\times4}=CJ_\rho'^{8m}C^{-1}$$
$$\vdots\qquad\qquad\vdots$$
$$J_\rho^{qm}=\underbrace{CJ_\rho'^{(q-2)m}C^{-1}CJ_\rho'^{2m}C^{-1}}_{q=2\times k}=CJ_\rho'^{qm}C^{-1}\ ,J_\rho^{(q+2)m}=\underbrace{CJ_\rho'^{qm}C^{-1}CJ_\rho'^{2m}C^{-1}}_{q+2=2\times(k+1)}=CJ_\rho'^{(q+2)m}C^{-1}$$
$$\vdots\qquad\qquad\vdots$$
$$J_\rho^{nm}=\underbrace{CJ_\rho'^{(n-2)m}C^{-1}CJ_\rho'^{2m}C^{-1}}_{n=2\times(q+1)}=CJ_\rho'^{nm}C^{-1}\ ,J_\rho^{(n+2)m}=\underbrace{CJ_\rho'^{nm}C^{-1}CJ_\rho'^{2m}C^{-1}}_{n+2=2\times(q+2)}=CJ_\rho'^{(n+2)m}C^{-1}.$$

So, $J_\rho^{nm}=CJ_\rho'^{nm}C^{-1}$ for all even $n\in\mathbb{Z}^+$. Thus, $|J_\rho|=nm$ if and only if $|J_\rho'|=nm$ which justifies the claim.

2. Let n be an odd positive integer.

$$J_\rho^{2m}=\underbrace{CJ_\rho'^m A^{-1}BJ_\rho'^m C^{-1}}_{2=2\times1}=CJ_\rho'^{2m}C^{-1}\ ,J_\rho^{3m}=\underbrace{CJ_\rho'^{2m}C^{-1}CJ_\rho'^m A^{-1}}=CJ_\rho'^{3m}A^{-1}$$
$$J_\rho^{4m}=\underbrace{CJ_\rho'^{2m}C^{-1}CJ_\rho'^{2m}C^{-1}}_{4=2\times2}=CJ_\rho'^{4m}C^{-1},\ J_\rho^{5m}=\underbrace{CJ_\rho'^{4m}C^{-1}CJ_\rho'^m A^{-1}}=CJ_\rho'^{5m}A^{-1}$$
$$\vdots\qquad\qquad\vdots$$
$$J_\rho^{qm}=\underbrace{CJ_\rho'^{(q-2)m}C^{-1}CJ_\rho'^{2m}C^{-1}}=CJ_\rho'^{qm}C^{-1}\ ,J_\rho^{(q+1)m}=\underbrace{CJ_\rho'^{qm}C^{-1}CJ_\rho'^m A^{-1}}=CJ_\rho'^{(q+1)m}A^{-1}$$
$$\vdots\qquad\qquad\vdots$$
$$J_\rho^{nm}=\underbrace{CJ_\rho'^{(n-2)m}C^{-1}CJ_\rho'^{2m}C^{-1}}=CJ_\rho'^{nm}C^{-1}\ ,J_\rho^{(n+1)m}=\underbrace{CJ_\rho'^{nm}C^{-1}CJ_\rho'^m A^{-1}}=CJ_\rho'^{(n+1)m}A^{-1}.$$

So, $J_\rho^{nm} = CJ_\rho'^{nm}A^{-1}$ for all odd $n \in \mathbb{Z}^+$. Thus, if $|J_\rho| = nm$ or $|J'_\rho| = nm$ then, $|J'_\rho| = nm$ or $|J_\rho| = nm$ if and only if $(G, \cdot) \cong (H, \circ)$ which justifies the claim.

Corollary 3.1 *Let $(G, \cdot)$ and $(H, \circ)$ be two distinct quasigroups that are isotopic under the triple (A, B, C). If G is a m-inverse quasigroup with the $\mathcal{T}_m$ condition, then H is a m-inverse quasigroup and so:*

1. *there exists $\alpha, \beta \in S'_m(G)$ i.e α and β are m-weak inverse permutations and*
2. *$J'_\rho = J'_\lambda \Rightarrow J_\rho^m = J_\lambda^m$ and $J_\rho = J_\lambda \Rightarrow J_\rho'^m = J_\lambda'^m$*

Proof
By Theorem 3.1, $A = B$ and $J_\rho'^m = C^{-1}J_\rho^m A = B^{-1}J_\rho^m C$ or $J_\lambda'^m = C^{-1}J_\lambda^m B = A^{-1}J_\lambda^m C$.

1. $C^{-1}J_\rho^m A = B^{-1}J_\rho^m C \Leftrightarrow J_\rho^m A = CB^{-1}J_\rho^m C \Leftrightarrow J_\rho^m = CB^{-1}J_\rho^m CA^{-1} = CA^{-1}J_\rho^m CA^{-1} = \alpha J_\rho^m \alpha$ where $\alpha = CA^{-1}$. This implies that $\alpha = CA^{-1} \in S'_m(G, \cdot)$.
2. $C^{-1}J_\lambda^m B = A^{-1}J_\lambda^m C \Leftrightarrow J_\lambda^m B = CA^{-1}J_\lambda^m C \Leftrightarrow J_\lambda^m = CA^{-1}J_\lambda^m CB^{-1} = CB^{-1}J_\lambda^m CB^{-1} = \beta J_\lambda^m \beta$ where $\beta = CB^{-1}$. This implies that $\alpha = \beta = CB^{-1} \in S'_m(G, \cdot)$.
3. $J_\rho'^m = C^{-1}J_\rho^m A = B^{-1}J_\rho^m C$, $J_\lambda'^m = C^{-1}J_\lambda^m B$. $J'_\rho = J'_\lambda \Rightarrow J_\rho'^m = J_\lambda'^m \Leftrightarrow C^{-1}J_\rho^m A = C^{-1}J_\lambda^m B = C^{-1}J_\lambda^m A \Leftrightarrow J_\lambda^m = J_\rho^m \Leftrightarrow J_\lambda = J_\rho$.

Lemma 3.1 *Let $(G, \cdot)$ be a m-inverse quasigroup with the $\mathcal{T}_m$ condition and isotopic to another quasigroup $(H, \circ)$. $(H, \circ)$ is a m-inverse quasigroup and G has a weak inverse permutation.*

Proof
From the proof of Corollary 3.1, $\alpha = \beta$, hence the conclusion.

Theorem 3.3 *If two distinct quasigroups are isotopic under the $\mathcal{T}$ condition. And any one of them is a m-inverse quasigroup and has a trivial set of m-weak inverse permutations, then the two quasigroups are both m-inverse quasigroups that are isomorphic.*

Proof
From Lemma 3.1, $\alpha = I$ is a weak inverse permutation. In the proof of Corollary 3.1, $\alpha = CA^{-1} = I \Rightarrow A = C$. Already, $A = B$, hence $(G, \cdot) \cong (H, \circ)$.

Remark 3.1 *Theorem 3.3 describes isotopic m-inverse quasigroups that are isomorphic by the $\mathcal{T}_m$ condition(for a special case).*

Application To Cryptography In application, it is assumed that the message to be transmitted can be represented as single element y of a m-inverse quasigroup $(G, \cdot)$ and that this is enciphered by pre-multiplying by another element x of G and then compute $(xy)J_\rho^m$ so that the encoded message is $(xy)^{\rho^m}$. At the receiving end, the message is deciphered by post-multiplying by xJ_ρ^{m+1} to get yJ_ρ^m from which the original message y can be extracted from.

Let $(G, \cdot)$ be a m-inverse quasigroup with an inverse cycle of length nm where n is an even positive integer. Let $(H, \circ)$ be a quasigroup that is isotopic to $(G, \cdot)$ under the $\mathcal{T}_m$ condition. Then by Theorem 3.1, H is a m-inverse quasigroup and by Theorem 3.2, H has an inverse cycle of length nm. So, according to Theorem 3.1, by the choice of the triple (A, B, C) been an isotopism from G onto H such that the $\mathcal{T}_m$ condition holds, if G is an m-inverse quasigroup with an inverse cycle of length nm then H is a m-inverse quasigroup with an inverse cycle of length nm. So, the secret key for the systems is the pair $\{(A, B, C), \mathcal{T}_m\}$. Thus whenever a set of information or messages is to be transmitted, the sender will enciphere in G(as described earlier on) and then enciphere again with $\{(A, B, C), \mathcal{T}_m\}$ to get a m-inverse quasigroup with an inverse cycle of length nm H which is the set of encoded messages. At the receiving end, the combined message H is deciphered by using an inverse isotopism(i.e inverse key $\{(A^-, B^{-1}, C^{-1}), \mathcal{T}\}$) to get G and then deciphere again(as described earlier on) to get the messages. The secret key can be changed over time. Futhermore, after enciphering in G and with $\{(A, B, C), \mathcal{T}_m\}$ to get H, enciphering can be done again in H the ways it was done in G.

The method described above is a double(triple) encryption and its a double(triple) protection. It protects each piece of information(element of the quasigroup) and protects the combined information(the quasigroup as a whole). Its like putting on a pair of socks and shoes or putting on under wears and clothes, the body gets better protection.

Thieves and robbers are fond of stealing items and goods and changing there original forms by selling off their various parts to different locations. By doing these, they pose a great challenge and difficulty to security agencies in tracking down the culprits.

4 Conclusion and Future Study

Keedwell and Shcherbacov [12, 13] have also generalized m-inverse quasigroup to quasigroups called (r, s, t)-inverse quasigroups. It will be interesting to study the universality of m-inverse loops and (r, s, t)-inverse quasigroups in general sense. These will generalize the works of J. M. Osborn and R. Artzy on universal WIPLs and CIPLs respectively.

References

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

[2] R. Artzy (1959), *Crossed inverse and related loops*, Trans. Amer. Math. Soc. 91, 3, 480–492.

[3] R. Artzy (1959), *On Automorphic-Inverse Properties in Loops*, Proc. Amer. Math. Soc. 10,4, 588–591.

[4] R. Artzy (1978), *Inverse-Cycles in Weak-Inverse Loops*, Proc. Amer. Math. Soc. 68, 2, 132–134.

[5] V. D. Belousov (1969), *Crossed inverse quasigroups(CI-quasigroups)*, Izv. Vyss. Ucebn; Zaved. Matematika 82, 21–27.

[6] A. S. Basarab (1967), *A class of WIP-loops*, Mat. Issled. 2(2), 3-24.

[7] A. S. Basarab (1970), *Isotopy of WIP loops*, Mat. Issled. 5, 2(16), 3-12.

[8] V. O. Chiboka (1990), *The study of properties and construction of certain finite order G-loops*, Ph.D thesis, Obafemi Awolowo University, Ile-Ife.

[9] E. D. Huthnance Jr.(1968), *A theory of generalised Moufang loops*, Ph.D. thesis, Georgia Institute of Technology.

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

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

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

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

[14] J. M. Osborn (1961), *Loops with the weak inverse property*, Pac. J. Math. 10, 295–304.