On Middle Universal Weak and Cross Inverse Property Loops With Equal Length Of Inverse Cycles*†

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 the weak inverse property(WIP) is isotopic invariant in loops. A sufficient condition for a WIPL that is specially isotopic to a loop to be isomorphic to the loop isotope is established. Cross inverse property loops(CIPLs) need not satisfy this sufficient condition. It is shown that under this special type of middle isotopism, if n is a positive even integer, then a WIPL has an inverse cycle of length n if and only if its isotope is a WIPL with an inverse cycle of length n. But, when n is an odd positive integer. If a loop or its isotope is a WIPL with only e and inverse cycles of length n, its isotope or the loop is a WIPL with only e and inverse cycles of length n if and only if they are isomorphic. So, that both are isomorphic CIPLs. Explanations and procedures are given on how these results can be used to apply CIPLs to 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 $xx^{\rho} = e^{\rho}$ and $x^{\lambda}x = e^{\lambda}$ 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 :** cross inverse property loops(CIPLs), weak inverse property loops(WIPLs), inverse cycles

‡All correspondence to be addressed to this author.

A loop(quasigroup) is a weak inverse property loop(quasigroup)[WIPL(WIPQ)] if and only if it obeys the identity

$$x(yx)^{\rho} = y^{\rho} \qquad \text{or} \qquad (xy)^{\lambda}x = y^{\lambda}.$$

A loop(quasigroup) is a cross inverse property loop(quasigroup)[CIPL(CIPQ)] if and only if it obeys the identity

$$xy \cdot x^{\rho} = y \qquad \text{or} \qquad x \cdot yx^{\rho} = y \qquad \text{or} \qquad x^{\lambda} \cdot (yx) = y \qquad \text{or} \qquad x^{\lambda}y \cdot x = y.$$

A loop(quasigroup) is an automorphic inverse property loop(quasigroup)[AIPL(AIPQ)] if and only if it obeys the identity

$$(xy)^{\rho} = x^{\rho}y^{\rho} \; or \; (xy)^{\lambda} = x^{\lambda}y^{\lambda}.$$

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 [16], 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 present 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 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 [16] 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 [16], 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 [16] 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.

The aim of the present study is to present a special type of middle isotopism under which the WIP is isotopic invariant in loops. A sufficient condition for a WIPL that is specially isotopic to a loop to be isomorphic to the loop isotope is established. Cross inverse property loops(CIPLs) need not satisfy this sufficient condition. It is shown that under this special type of middle isotopism, if n is a positive even integer, then a WIPL has an inverse cycle of length n if and only if its isotope is a WIPL with an inverse cycle of length n. But, when n is an odd positive integer. If a loop or its isotope is a WIPL with only e and inverse cycles of length n, its isotope or the loop is a WIPL with only e and inverse cycles of length n if and only if they are isomorphic. So, that both are isomorphic CIPLs. Explanations and procedures are given on how these results can be used to apply CIPLs to cryptography.

2 Preliminaries

Definition 2.1 *Let L be a loop. A mapping $\alpha \in SYM(L)$(where $SYM(L)$ is the group of all bijections on L) which obeys the identity $x^\rho = [(x\alpha)^\rho]\alpha$ is called a weak right inverse permutation. Their set is represented by $S_\rho(L)$.*

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

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

It can be shown that $\alpha \in S(L)$ is a weak right inverse if and only if it is a weak left inverse permutation. So, $S'(L) = S_\rho(L) = S_\lambda(L)$.

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

Example 2.1 *If L is an extra loop, the left and right inner mappings $L(x,y)$ and $R(x,y)$ $\forall\ x,y \in L$ are automorphisms of orders 2 ([14]). Hence, they are weak inverse permutations by Remark 2.1*

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 loop, the set of weak inverse permutations that commute form an abelian group.*

Remark 2.2 *Applying Lemma 2.1 to extra loops and considering Example 2.1, it will be observed that in an extra loop L, the Boolean groups $Inn_\lambda(L), Inn_\rho \leq S'(L)$. $Inn_\lambda(L)$ and $Inn_\rho(L)$ are the left and right inner mapping groups respectively. They have been investigated in [15] and [14]. This deductions can't be drawn for CC-loops despite the fact that the left (right) inner mappings commute and are automorphisms. And this is as a result of the fact that the left(right) inner mappings are not of exponent 2.*

Definition 2.2 *($\mathcal{T}$-condition)*
Let $(G,\cdot)$ and $(H,\circ)$ be two distinct loops that are isotopic under the triple (A,B,C). $(G,\cdot)$ obeys the $\mathcal{T}_1$ condition if and only if $A = B$. $(G,\cdot)$ obeys the $\mathcal{T}_2$ condition if and only if $J'_\rho = C^{-1}J_\rho B = A^{-1}J_\rho C$. $(G,\cdot)$ obeys the $\mathcal{T}_3$ condition if and only if $J'_\lambda = C^{-1}J_\lambda A = B^{-1}J_\lambda C$. So, $(G,\cdot)$ obeys the $\mathcal{T}$ condition if and only if it obey $\mathcal{T}_1$ and $\mathcal{T}_2$ conditions or $\mathcal{T}_1$ and $\mathcal{T}_3$ conditions since $\mathcal{T}_2 \equiv \mathcal{T}_3$.

It must here by be noted that the $\mathcal{T}$-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 $\mathcal{T}$-condition, then this is relative to some isotope $(H,\circ)$ of $(G,\cdot)$

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

1. *L is a WIPL*
2. *$R_y J_\rho L_y = J_\rho\ \forall\ y \in L$.*
3. *$L_x J_\lambda R_x = J_\lambda\ \forall\ x \in L$.*

Lemma 2.3 *(Lemma, Artzy [4])*
Let a WIPL consist only of e and inverse cycles of length n. If n is odd, the loop is a CIPL.

3 Main Results

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

1. *If the pair of $(G,\cdot)$ and $(H,\circ)$ obey the $\mathcal{T}$ condition, then $(G,\cdot)$ is a WIPL if and only if $(H,\circ)$ is a WIPL.*
2. *If $(G,\cdot)$ and $(H,\circ)$ are WIPLs, then $J_\lambda R_x J_\rho B = C J'_\lambda R'_{xA} J'_\rho$ and $J_\rho L_x J_\lambda A = C J'_\rho L'_{xB} J'_\lambda$ 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 $\Leftrightarrow xAR'_{yB} = xR_yC \Leftrightarrow AR'_{yB} = R_yC \Leftrightarrow R'_{yB} = A^{-1}R_yC \Leftrightarrow$

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

Applying (2) and (3) to Lemma 2.2 separately, we have : $R_yJ_\rho L_y = J_\rho$, $L_xJ_\lambda R_x = J_\lambda \Rightarrow (AR'_{xB}C^{-1})J_\rho(BL'_{xA}C^{-1}) = J_\rho$, $(BL'_{xA}C^{-1})J_\lambda(AR'_{xB}C^{-1}) = J_\lambda \Leftrightarrow AR'_{xB}(C^{-1}J_\rho B)L'_{xA}C^{-1} = J_\rho$, $BL'_{xA}(C^{-1}J_\lambda A)R'_{xB}C^{-1} = J_\lambda \Leftrightarrow$

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

Let $J'_\rho = C^{-1}J_\rho B = A^{-1}J_\rho C$, $J'_\lambda = C^{-1}J_\lambda A = B^{-1}J_\lambda C$. Then, from (4) and by Lemma 2.2, H is a WIPL if $xB = xA$ and $J'_\rho = C^{-1}J_\rho B = A^{-1}J_\rho C$ or $xA = xB$ and $J'_\lambda = C^{-1}J_\lambda A = B^{-1}J_\lambda C \Leftrightarrow B = A$ and $J'_\rho = C^{-1}J_\rho B = A^{-1}J_\rho C$ or $A = B$ and $J'_\lambda = C^{-1}J_\lambda A = B^{-1}J_\lambda C \Leftrightarrow A = B$ and $J'_\rho = C^{-1}J_\rho B = A^{-1}J_\rho C$ or $J'_\lambda = C^{-1}J_\lambda A = B^{-1}J_\lambda C$. This completes the proof of the forward part. To prove the converse, carry out the same procedure, assuming the $\mathcal{T}$ condition and the fact that $(H,\circ)$ is a WIPL.

2. If $(H,\circ)$ is a WIPL, then

$$R'_yJ'_\rho L'_y = J'_\rho,\ \forall\ y \in H \tag{5}$$

while since G is a WIPL,

$$R_xJ_\rho L_x = J_\rho\ \forall\ x \in G. \tag{6}$$

The fact that G and H are isotopic implies that

$$L_x = BL'_{xA}C^{-1}\ \forall\ x \in G\ and \tag{7}$$

$$R_x = AR'_{xB}C^{-1}\ \forall\ x \in G. \tag{8}$$

From (5),

$$R'_y = J'_\rho L'^{-1}_y J'_\lambda \ \forall\ y \in H \text{ and} \tag{9}$$

$$L'_y = J'_\lambda R'^{-1}_y J'_\rho \ \forall\ y \in H \tag{10}$$

while from (6),

$$R_x = J_\rho L_x^{-1} J_\lambda \ \forall\ x \in G \text{ and} \tag{11}$$

$$L_x = J_\lambda R_x^{-1} J_\rho \ \forall\ x \in G. \tag{12}$$

So, using (10) and (12) in (7) we get

$$J_\lambda R_x J_\rho B = C J'_\lambda R'_{xA} J'_\rho \ \forall\ x \in G \tag{13}$$

while using (9) and (11) in (8) we get

$$J_\rho L_x J_\lambda A = C J'_\rho L'_{xB} J'_\lambda \ \forall\ x \in G. \tag{14}$$

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

1. *If n is an even positive integer. Then, $(G,\cdot)$ is a WIPL with an inverse cycle of length n if and only if $(H,\circ)$ is a WIPL with an inverse cycle of length n.*
2. *When n is an odd positive integer. If $(G,\cdot)$ or $(H,\circ)$ is a WIPL with only e and inverse cycles of length n, $(H,\circ)$ or $(G,\cdot)$ is a WIPL with only e and inverse cycles of length n if and only if $(G,\cdot) \cong (H,\circ)$. So, $(G,\cdot)$ and $(H,\circ)$ are isomorphic CIPLs.*

Proof

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

1. It will now be shown that $(G,\cdot)$ has an inverse cycle of length n if and only if $(H,\circ)$ is a WIPL with an inverse cycle of length n. A WIPL $(G,\cdot)$ has an inverse cycle of length n if and only if $|J_\rho| = n$. Recall that $J_\rho = CJ'_\rho B^{-1}$ and $J_\rho = AJ'_\rho C^{-1}$. Consider the following inductive process.

$$J_\rho^2 = \underbrace{CJ'_\rho B^{-1} A J'_\rho C^{-1}}_{2=2\times 1} = CJ'^2_\rho C^{-1}\ , J_\rho^4 = \underbrace{CJ'^2_\rho C^{-1} CJ'^2_\rho C^{-1}}_{4=2\times 2} = CJ'^4_\rho C^{-1}$$

$$J_\rho^6 = \underbrace{CJ'^4_\rho C^{-1} CJ'^2_\rho C^{-1}}_{6=2\times 3} = CJ'^6_\rho C^{-1}\ , J_\rho^8 = \underbrace{CJ'^6_\rho C^{-1} CJ'^2_\rho C^{-1}}_{8=2\times 4} = CJ'^8_\rho C^{-1}$$

$$\vdots \qquad\qquad \vdots$$

$$J_\rho^m = \underbrace{CJ'^{m-2}_\rho C^{-1} CJ'^2_\rho C^{-1}}_{m=2\times k} = CJ'^m_\rho C^{-1}\ , J_\rho^{m+2} = \underbrace{CJ'^m_\rho C^{-1} CJ'^2_\rho C^{-1}}_{m+2=2\times(k+1)} = CJ'^{m+2}_\rho C^{-1}$$

$$\vdots \qquad\qquad \vdots$$

$$J_\rho^n = \underbrace{CJ'^{n-2}_\rho C^{-1} CJ'^2_\rho C^{-1}}_{n=2\times(m+1)} = CJ'^n_\rho C^{-1}\ , J_\rho^{n+2} = \underbrace{CJ'^n_\rho C^{-1} CJ'^2_\rho C^{-1}}_{n+2=2\times(m+2)} = CJ'^{n+2}_\rho C^{-1}.$$

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

2. Let n be an odd positive integer and consider the following inductive process.

$$J_\rho^2 = \underbrace{CJ'_\rho B^{-1}AJ'_\rho C^{-1}}_{2=2\times 1} = CJ_\rho'^2C^{-1}\ , J_\rho^3 = \underbrace{CJ_\rho'^2C^{-1}CJ'_\rho B^{-1}} = CJ_\rho'^3B^{-1}$$

$$J_\rho^4 = \underbrace{CJ_\rho'^2C^{-1}CJ_\rho'^2C^{-1}}_{4=2\times 2} = CJ_\rho'^4C^{-1},\ J_\rho^5 = \underbrace{CJ_\rho'^4C^{-1}CJ'_\rho B^{-1}} = CJ_\rho'^5B^{-1}$$

$$\vdots \qquad\qquad \vdots$$

$$J_\rho^m = \underbrace{CJ_\rho'^{m-2}C^{-1}CJ_\rho'^2C^{-1}} = CJ_\rho'^mC^{-1}\ , J_\rho^{m+1} = \underbrace{CJ_\rho'^mC^{-1}CJ'_\rho B^{-1}} = CJ_\rho'^{m+1}B^{-1}$$

$$\vdots \qquad\qquad \vdots$$

$$J_\rho^n = \underbrace{CJ_\rho'^{n-2}C^{-1}CJ_\rho'^2C^{-1}} = CJ_\rho'^nC^{-1}\ , J_\rho^{n+1} = \underbrace{CJ_\rho'^nC^{-1}CJ'_\rho B^{-1}} = CJ_\rho'^{n+1}B^{-1}.$$

So, $J_\rho^n = CJ_\rho'^nC^{-1}$ for all odd $n \in \mathbb{Z}^+$. Thus, if $|J_\rho| = n$ or $|J'_\rho| = n$ then, $|J'_\rho| = n$ or $|J_\rho| = n$ if and only if $(G,\cdot) \cong (H,\circ)$ which justifies the claim. By Lemma 2.3, G and H are CIPLs.

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

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

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

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

Lemma 3.1 *Let $(G,\cdot)$ be a WIPL with the $\mathcal{T}$ condition and isotopic to another loop $(H,\circ)$. $(H,\circ)$ is a WIPL 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 loops are isotopic under the $\mathcal{T}$ condition. And any one of them is a WIPL and has a trivial set of weak inverse permutations, then the two loops are both WIPLs 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 WIP loops that are isomorphic by the $\mathcal{T}$ 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 x of a loop $(G, \cdot)$ and that this is enciphered by multiplying by another element y of G so that the encoded message is yx. At the receiving end, the message is deciphered by multiplying by the right inverse y^{ρ} of y.

Let $(G, \cdot)$ be a WIPL with only e and inverse cycles of length n where n is an odd positive integer. So it is a CIPL. Let $(H, \circ)$ be a loop that is isotopic to $(G, \cdot)$ under the $\mathcal{T}$ condition such that $(G, \cdot) \ncong (H, \circ)$. Then by Theorem 3.1, H is a WIPL but by Theorem 3.2, H does not have only e and inverse cycles of length n and so it is not a CIPL. 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 $\mathcal{T}$ condition holds, if G is a CIPL then H is a WIPL that is not a CIPL. So, the secret key for the systems is the pair $\{(A, B, C), \mathcal{T}\}$. Thus whenever a set of information or messages is to be transmitted, the sender will encipher in G(as described earlier on) and then encipher again with $\{(A, B, C), \mathcal{T}\}$ to get a WIPL 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.

The method described above is a double encryption and its a double protection. It protects each piece of information(element of the loop) and protects the combined information(the loop 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.

4 Conclusion and Future Study

Karklinüsh and Karkliň [11] introduced m-inverse loops i.e loops that obey any of the equivalent conditions

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

They are generalizations of WIPLs and CIPLs, which corresponds to $m = -1$ and $m = 0$ respectively. After the study of m-loops by Keedwell and Shcherbacov [10], they have also generalized them to quasigroups called (r, s, t)-inverse quasigroups in [12] and [13]. It will be interesting to study the universality of m-inverse loops and (r, s, t)-inverse quasigroups. 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] M. K. Kinyon, K. Kunen (2004), *The structure of extra loops*, Quasigroups and Related Systems 12, 39–60.

[15] M. K. Kinyon, K. Kunen, J. D. Phillips (2004), *Diassociativity in conjugacy closed loops*, Comm. Alg. 32, 767–786.

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