Revista Colombiana de Matemáticas
Volumen 44(2010)2, páginas 79-89

On Middle Universal Weak and Cross Inverse Property Loops with Equal Length of Inverse Cycles

Sobre la propiedad débil universal media y cruce inverso de lazos con igual longitud de ciclos inversos

Jaiyeola Temitope Gbolahan

Obafemi Awolowo University, Ile Ife, Nigeria

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. It is shown that under this special type of middle isotopism, whenever n is a positive even integer, a finite WIPL has an inverse cycle of length n if and only if its isotope is a finite WIPL with an inverse cycle of length n. But, when n is an odd positive integer and a loop (or its isotope) is a finite WIPL with only e and inverse cycles of length n, then its isotope (or the loop) is a finite WIPL with only e and inverse cycles of length n if and only if they are isomorphic. Hence, both are isomorphic CIPLs. Explanations and procedures are given on how these results can be used to apply CIPLs to cryptography.

Key words and phrases. Cross inverse property loops (CIPLs), Weak inverse property loops (WIPLs), Inverse cycles.

2000 Mathematics Subject Classification. 20NO5, 08A05.

Resumen. Este estudio presenta un tipo especial de isotopismo intermedio bajo el cual la propiedad inversa débil (WIP) es una invariante isotópica de lazos. Se establece una condición suficiente que para un WIPL, que es especialmente isotópico a un lazo, sea isomorfo al lazo isotópico. Se demuestra que bajo este tipo especial de isotopismo intermedio, cuando n es un entero positivo par, un WIPL finito tiene un ciclo inverso de longitud n si y sólo si su isótopo es un WIPL finito con un ciclo inverso de longitud n. Pero, cuando n es un entero positivo impar y un lazo (o su isótopo) es un WIPL finito con sólo e y un ciclo

inverso de longitud n, entonces su isótopo (o el lazo) es un WIPL finito con sólo e y un ciclo inverso de longitud n si y sólo si ellos son isomorfos. Por lo tanto, ambos son CIPLs isomorfos. Explicaciones y procedimientos están dados en como esos resultados pueden ser usados para aplicar CIPLs a criptografía.

Palabras y frases clave. Lazos con propiedad inversa de cruce (CIPLs), lazos con propiedad inversa débil (WIPLs), ciclos inversos.

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 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 $x^\rho = xJ_\rho \in L$ and $x^\lambda = xJ_\lambda \in L$ such that $xx^\rho = e^\rho$ and $x^\lambda x = e^\lambda$ are called the right and left inverse elements of x respectively. Here, $e^\rho \in L$ and $e^\lambda \in L$ satisfy the relations $xe^\rho = x$ and $e^\lambda x = x$ for all $x \in L$ and are respectively called the right and left identity elements. 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.

A loop is called an extra loop if and only if it obeys the identity

$$(xy \cdot z)x = x(y \cdot zx).$$

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

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

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

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

A loop is an automorphism inverse property loop (AIPL) if and only if it obeys the identity

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

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

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

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 $\mathrm{AUT}(G, \cdot)$ 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 $\mathrm{AUM}(G, \cdot)$ called the automorphism group of $(G, \cdot)$.

The past efforts of Artzy [1, 4, 3, 2], Belousov and Curkan [5] and current works of Keedwell [7], Keedwell and Shcherbacov [8, 9, 10, 11] are of great significance in the study of WIPLs, AIPLs and CIPLs, their generalizations (i.e. m-inverse loops and quasigroups, (r, s, t)-inverse quasigroups and (α, β, γ)-inverse quasigroups) and applications to cryptography. The universality of WIPLs and CIPLs have been addressed by Osborn [14] and Artzy [2] respectively. From the literature review stated above, it can be seen that neither WIPL nor CIPL have 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. Explanations and procedures are given on how the results here can be used to apply CIPLs to cryptography.

2. Preliminaries

Definition 1. Let L be a loop. A mapping $\alpha \in \mathrm{SYM}(L)$ (where $\mathrm{SYM}(L)$ is the group of all bijections on L) which obeys the identity $x^\rho = \big[(x\alpha)^\rho\big]\alpha$ is called a weak right inverse permutation. Their set is represented by $S_\rho(L)$.

Similarly, if α obeys the identity $x^\lambda = \big[(x\alpha)^\lambda\big]\alpha$ 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 permutation if and only if it is a weak left inverse permutation. So, $S'(L) = S_\rho(L) = S_\lambda(L)$.

***Remark* 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. In a loop L, if $\alpha \in \mathrm{SYM}(L)$ is of order 2 and it preserves the right inverse of each element $x \in L$, then $\big[(x\alpha)^\rho\big]\alpha = (x^\rho)\alpha^2 = x^\rho$. A similar proof goes for when $\alpha \in \mathrm{SYM}(L)$ is of order 2 and it preserves the left inverse of each element $x \in L$.

Example 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 ([12]). Hence, they are weak inverse permutations by Remark 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'.

***Remark* 2.** In a loop, the set of weak inverse permutations that commute, form an abelian group.

Closure $\alpha,\beta \in S_\lambda(L)$ $\big(S_\rho(L)\big) \Leftrightarrow J_\lambda = \alpha J_\lambda \alpha$, $J_\lambda = \beta J_\lambda \beta$ ($J_\rho = \alpha J_\rho \alpha$, $J_\rho = \beta J_\rho \beta$). Thus, $J_\lambda = \alpha(\beta J_\lambda \beta)\alpha = (\alpha\beta)J_\lambda(\beta\alpha) = (\alpha\beta)J_\lambda(\alpha\beta) \Leftrightarrow \alpha\beta \in S_\lambda(L)$. Similarly, $J_\rho = \alpha(\beta J_\rho \beta)\alpha = (\alpha\beta)J_\rho(\beta\alpha) = (\alpha\beta)J_\rho(\alpha\beta) \Leftrightarrow \alpha\beta \in S_\rho(L)$. Thence, $S_\lambda(L)$ $\big(S_\rho(L)\big)$ is closed under the composition of maps.

Associativity This is trivially true for mappings in general.

Identity The identity mapping $I \in S_\lambda(L)\big(S_\rho(L)\big)$. This can easily be seen: $IJ_\lambda I = J_\lambda (IJ_\rho I = J_\rho)$.

Inverse Let $\alpha \in S_\lambda(L)\big(S_\rho(L)\big) \Leftrightarrow J_\lambda = \alpha J_\lambda \alpha$ ($J_\rho = \alpha J_\rho \alpha$) $\Leftrightarrow J_\lambda^{-1} = (\alpha J_\lambda \alpha)^{-1}$ $\big(J_\rho^{-1} = (\alpha J_\rho \alpha)^{-1}\big) \Leftrightarrow J_\lambda^{-1} = \alpha^{-1}J_\lambda^{-1}\alpha^{-1}$ ($J_\rho^{-1} = \alpha^{-1}J_\rho^{-1}\alpha^{-1}$) $\Leftrightarrow J_\rho = \alpha^{-1}J_\rho\alpha^{-1}$ ($J_\lambda = \alpha^{-1}J_\lambda\alpha^{-1}$) $\Leftrightarrow \alpha^{-1} \in S_\lambda(L)$ $\big(S_\rho(L)\big)$.

Applying this fact to extra loops and considering Example 1, it can be concluded that in an extra loop L, the Boolean groups $\mathrm{Inn}_\lambda(L), \mathrm{Inn}_\rho(L) \leq S'(L)$. $\mathrm{Inn}_\lambda(L)$ and $\mathrm{Inn}_\rho(L)$ are the left and right inner mapping groups respectively. They have been investigated in [13] and [12]. These deductions can not 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. ($\mathcal{T}$-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 (i.e. $(G,\cdot)$ is middle isotopic to $(H,\circ)$) 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 hereby 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 1. *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) $L_x J_\lambda R_x = J_\lambda \forall x \in L$.

Definition 3. Let G be a quasigroup. A 'cycle of inverses' or 'inverse cycles' or simply 'cycles' is a finite sequence of elements $x_1, x_2, \ldots, x_n \in G$ such that $x_k^\rho = x_{k+1}$, $k+1$ taken modulo n. The number n is called the length of the cycle.

Lemma 2. *(Lemma, Artzy [4]) Let a WIPL consist only of e and inverse cycles of length n. If n is odd, J_ρ is an automorphism, and the loop is a CIPL.*

3. Main Results

Theorem 1. *Let $(G,\cdot)$ and $(H,\circ)$ be two distinct loops that are isotopic under the triple (A,B,C).*

(1) Let 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 $\Leftrightarrow xA \circ yB = (x \cdot y)C \Leftrightarrow yBL'_{xA} = yL_xC \Leftrightarrow BL'_{xA} = L_xC \Leftrightarrow L'_{xA} = B^{-1}L_xC \Leftrightarrow$

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

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

$$R_y = AR'_{yB}C^{-1} \tag{2}$$

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

$$R'_{xB}(C^{-1}J_\rho B)L'_{xA} = A^{-1}J_\rho C, L'_{xA}(C^{-1}J_\lambda A)R'_{xB} = B^{-1}J_\lambda C. \tag{3}$$

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 (3) and by Lemma 1, 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

$$R'_y J'_\rho L'_y = J'_\rho, \qquad \forall y \in H \tag{4}$$

while since G is a WIPL,

$$R_x J_\rho L_x = J_\rho, \qquad \forall x \in G. \tag{5}$$

The fact that G and H are isotopic implies that

$$L_x = BL'_{xA}C^{-1}, \qquad \forall x \in G \tag{6}$$

and

$$R_x = AR'_{xB}C^{-1}, \qquad \forall x \in G. \tag{7}$$

From (4),

$$R'_y = J'_\rho L'^{-1}_y J'_\lambda, \qquad \forall y \in H \tag{8}$$

and

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

while from (5),

$$R_x = J_\rho L_x^{-1} J_\lambda, \qquad \forall x \in G \tag{10}$$

and

$$L_x = J_\lambda R_x^{-1} J_\rho, \qquad \forall x \in G. \tag{11}$$

So, using (9) and (11) in (6) we get

$$J_\lambda R_x J_\rho B = CJ'_\lambda R'_{xA} J'_\rho, \qquad \forall x \in G \tag{12}$$

while using (8) and (10) in (7) we get

$$J_\rho L_x J_\lambda A = CJ'_\rho L'_{xB} J'_\lambda, \qquad \forall x \in G. \tag{13}$$

☑

Theorem 2. *Let $(G, \cdot)$ and $(H, \circ)$ be two distinct finite loops that are isotopic under the triple (A, B, C) such that they obey the $\mathcal{T}$ condition.*

(1) Let n be 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) Let n be an odd positive integer and $(G,\cdot)$ a WIPL with only e and inverse cycles of length n. Then, $(H,\circ)$ is a WIPL with only e and inverse cycles of length n if and only if $(G,\cdot) \cong (H,\circ)$. Hence, $(G,\cdot)$ and $(H,\circ)$ are isomorphic CIPLs.

(3) Let n be an odd positive integer and $(H,\circ)$ a WIPL with only e and inverse cycles of length n. Then, $(G,\cdot)$ is a WIPL with only e and inverse cycles of length n if and only if $(G,\cdot) \cong (H,\circ)$. Hence, $(G,\cdot)$ 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 1.

(1) It will now be shown that $(G,\cdot)$ has an inverse cycle of length n if and only if $(H,\circ)$ has 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:

$$
\begin{aligned}
J_\rho^2 &= CJ'_\rho B^{-1} AJ'_\rho C^{-1} = CJ'^2_\rho C^{-1},\\
J_\rho^4 &= CJ'^2_\rho C^{-1} CJ'^2_\rho C^{-1} = CJ'^4_\rho C^{-1},\\
J_\rho^6 &= CJ'^4_\rho C^{-1} CJ'^2_\rho C^{-1} = CJ'^6_\rho C^{-1},\\
J_\rho^8 &= CJ'^6_\rho C^{-1} CJ'^2_\rho C^{-1} = CJ'^8_\rho C^{-1}\\
&\vdots\\
J_\rho^m &= CJ'^{m-2}_\rho C^{-1} CJ'^2_\rho C^{-1} = CJ'^m_\rho C^{-1},\\
J_\rho^{m+2} &= CJ'^m_\rho C^{-1} CJ'^2_\rho C^{-1} = CJ'^{m+2}_\rho C^{-1}\\
&\vdots\\
J_\rho^n &= CJ'^{n-2}_\rho C^{-1} CJ'^2_\rho C^{-1} = CJ'^n_\rho C^{-1},\\
J_\rho^{n+2} &= CJ'^n_\rho C^{-1} CJ'^2_\rho C^{-1} = CJ'^{n+2}_\rho C^{-1}.
\end{aligned}
$$

So, $J_\rho^n = CJ'^n_\rho C^{-1}$ 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:

$$\begin{aligned}
J_\rho^2 &= CJ'_\rho B^{-1}AJ'_\rho C^{-1} = CJ'^2_\rho C^{-1},\\
J_\rho^3 &= CJ'^2_\rho C^{-1}CJ'_\rho B^{-1} = CJ'^3_\rho B^{-1}\\
J_\rho^4 &= CJ'^2_\rho C^{-1}CJ'^2_\rho C^{-1} = CJ'^4_\rho C^{-1},\\
J_\rho^5 &= CJ'^4_\rho C^{-1}CJ'_\rho B^{-1} = CJ'^5_\rho B^{-1}\\
&\vdots\\
J_\rho^m &= CJ'^{m-2}_\rho C^{-1}CJ'^2_\rho C^{-1} = CJ'^m_\rho C^{-1},\\
J_\rho^{m+1} &= CJ'^m_\rho C^{-1}CJ'_\rho B^{-1} = CJ'^{m+1}_\rho B^{-1}\\
&\vdots\\
J_\rho^k &= CJ'^{k-2}_\rho C^{-1}CJ'^2_\rho C^{-1} = CJ'^k_\rho C^{-1},\\
J_\rho^{k+1} &= CJ'^k_\rho C^{-1}CJ'_\rho B^{-1} = CJ'^{k+1}_\rho B^{-1}.
\end{aligned}$$

So, $J_\rho^n = CJ'^n_\rho B^{-1}$ for all odd $n \in \mathbb{Z}^+$. Thus, whenever $n \in \mathbb{Z}^+$ is odd, if $|J_\rho| = n$ then, $|J'_\rho| = n$ implies that $J_\rho^n = CJ'^n_\rho B^{-1}$ which implies $I = CB^{-1}$ which implies that $B = C$, hence, $A = B = C$, thence, $(G,\cdot) \cong (H,\circ)$. Conversely, if $|J_\rho| = n$ and $(G,\cdot) \cong (H,\circ)$, then $B = C$ and so $J_\rho^n = CJ'^n_\rho B^{-1}$ implies that $I = BJ'^n_\rho B^{-1}$ which implies $|J'_\rho| = n$ which justifies the claim. By Lemma 2, G and H are CIPLs.

(3) Let n be an odd positive integer, then going by the inductive process in (2) above, $J_\rho^n = CJ'^n_\rho B^{-1}$ for all odd $n \in \mathbb{Z}^+$. Thus, whenever $n \in \mathbb{Z}^+$ is odd, if $|J'_\rho| = n$ then, $|J_\rho| = n$ implies that $J_\rho^n = CJ'^n_\rho B^{-1}$ which implies $I = CB^{-1}$ which implies that $B = C$, hence, $A = B = C$, thence, $(G,\cdot) \cong (H,\circ)$. Conversely, if $|J'_\rho| = n$ and $(G,\cdot) \cong (H,\circ)$, then $B = C$ and so $J_\rho^n = CJ'^n_\rho B^{-1}$ implies that $J_\rho^n = BIB^{-1}$ which implies $|J_\rho| = n$ which justifies the claim. By Lemma 2, G and H are CIPLs. ☑

Corollary 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 exist $\alpha,\beta \in S'(G)$ i.e. α and β are weak inverse permutations, and

(2) $J'_\rho = J'_\lambda \Leftrightarrow J_\rho = J_\lambda$.

Proof. By Theorem 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. *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 1, $\alpha = \beta$, hence the conclusion. ☑

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

***Remark* 3.** Theorem 3 describes isotopic WIP loops that are isomorphic by the $\mathcal{T}$ condition (for a special case).

3.1. Application to Cryptography

In application, it is assumed that the message to be transmitted can be represented as a single element x of a loop $(G,\cdot)$ and that this is encrypted by multiplying by another element y of G so that the encrypted message is yx. At the receiving end, the message is decrypted 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 1, H is a WIPL but by Theorem 2, H does not have only e and inverse cycles of length n and so it is not a CIPL.

So, according to Theorem 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 system is the pair $\{(A,B,C),\mathcal{T}\}$.

Thus whenever a set of information or messages is to be transmitted, the sender will encrypt in G (as described earlier on) and then encrypt again with $\{(A,B,C),\mathcal{T}\}$ to get a WIPL 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 $\{(A^{-1},B^{-1},C^{-1}),\mathcal{T}\}$) to get G and then decrypt again (as described earlier on) to get the plain texts. 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). It's 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

Karklin'š and Karklin' [6] 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 [8], they have also generalized them to quasigroups called (r, s, t)-inverse quasigroups and (α, β, γ)-inverse quasigroups in [9], [10] and [11]. It will be interesting to study the universality of m-inverse loops, (r, s, t)-inverse quasigroups and (α, β, γ)-inverse quasigroups. These will generalize the works of J. M. Osborn and R. Artzy on universal WIPLs and CIPLs respectively.

References

[1] R. Artzy, *On Loops with Special Property*, Proc. Amer. Math. Soc. **6** (1955), 448–453.

[2] ———, *Crossed Inverse and Related Loops*, Trans. Amer. Math. Soc. **91** (1959), no. 3, 480–492.

[3] ———, *On Automorphic-Inverse Properties in Loops*, Proc. Amer. Math. Soc. **10** (1959), no. 4, 588–591.

[4] ———, *Inverse-Cycles in Weak-Inverse Loops*, Proc. Amer. Math. Soc. **68** (1978), no. 2, 132–134.

[5] V. D. Belousov and B. V. Curkan, *Crossed Inverse Quasigroups(CI-Quasigroups)*, Izv. Vyss. Uceb. Zaved. Mat. **82** (1969), 21–27.

[6] B. B. Karklin's and V. B. Karklin', *Inverse Loops*, vol. 39, ch. Nets and Quasigroups, pp. 82–86, Mat. Issl., 1976.

[7] A. D. Keedwell, *Crossed-Inverse Quasigroups with Long Inverse Cycles and Applications to Cryptography*, Australas. J. Combin. **20** (1999), 241–250.

[8] A. D. Keedwell and V. A. Shcherbacov, *On m-Inverse Loops and Quasigroups with a Long Inverse Cycle*, Australas. J. Combin. **26** (2002), 99–119.

[9] ———, *Construction and Properties of* (r, s, t)*-Inverse Quasigroups I*, Discrete Math. **266** (2003), 275–291.

[10] ———, *Construction and Properties of* (r, s, t)*-Inverse Quasigroups II*, Discrete Math. **288** (2004), 61–71.

[11] ———, *Quasigroups with an Inverse Property and Generalized Parastrophic Identities*, Quasigroups and Related Systems **13** (2005), 109–124.

[12] M. K. Kinyon and K. Kunen, *The Structure of Extra Loops*, Quasigroups and Related Systems **12** (2004), 39–60.

[13] M. K. Kinyon, K. Kunen, and J. D. Phillips, *Diassociativity in Conjugacy Closed Loops*, Comm. Alg. **32** (2004), 767–786.

[14] J. M. Osborn, *Loops with the Weak Inverse Property*, Pac. J. Math. **10** (1961), 295–304.

(Recibido en julio de 2008. Aceptado en junio de 2010)

Department of Mathematics
Obafemi Awolowo University
Ile Ife
Nigeria
e-mail: tjayeola@oauife.edu.ng