Surveys in Mathematics and its Applications

ISSN 1842-6298 (electronic), 1843-7265 (print)
Volume **5** (2010), 17 – 34

ON ANOTHER TWO CRYPTOGRAPHIC IDENTITIES IN UNIVERSAL OSBORN LOOPS

T. G. Jaiyéọlá and J. O. Adéníran

Abstract. In this study, by establishing an identity for universal Osborn loops, two other identities (of degrees 4 and 6) are deduced from it and they are recognized and recommended for cryptography in a similar spirit in which the cross inverse property (of degree 2) has been used by Keedwell following the fact that it was observed that universal Osborn loops that do not have the 3-power associative property or weaker forms of; inverse property, power associativity and diassociativity to mention a few, will have cycles (even long ones). These identities are found to be cryptographic in nature for universal Osborn loops and thereby called cryptographic identities. They were also found applicable to security patterns, arrangements and networks which the CIP may not be applicable to.

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. Furthermore, 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. We write xy instead of $x \cdot y$, and stipulate that $\cdot$ has lower priority than juxtaposition among factors to be multiplied. For instance, $x \cdot yz$ stands for $x(yz)$. For each $x \in L$, the elements $x^{\rho} = xJ_{\rho}, x^{\lambda} = xJ_{\lambda} \in L$ such that $xx^{\rho} = e = x^{\lambda}x$ are called the right, left inverses of x respectively. $x^{\lambda^2} = (x^{\lambda})^{\lambda}$ and $x^{\rho^2} = (x^{\rho})^{\rho}$.

Definition 1. *A loop $(G, \cdot, /, \backslash, e)$ is a set G together with three binary operations $(\cdot)$, $(/)$, $(\backslash)$ and one nullary operation e such that*

(i) $x \cdot (x\backslash y) = y$, $(y/x) \cdot x = y$ *for all* $x, y \in G$,

2000 Mathematics Subject Classification: 20NO5; 08A05.
Keywords: Universal Osborn loops; Cryptography.

(ii) $x\backslash(x \cdot y) = y,\ (y \cdot x)/x = y$ *for all* $x, y \in G$ *and*

(iii) $x\backslash x = y/y$ *or* $e \cdot x = x$ *for all* $x, y \in G$.

We also stipulate that $(/)$ and $(\backslash)$ have higher priority than $(\cdot)$ among factors to be multiplied. For instance, $x \cdot y/z$ and $x \cdot y\backslash z$ stand for $x(y/z)$ and $x \cdot (y\backslash z)$ respectively.

The left and right translation maps of G, L_x and R_x respectively can be defined by

$$yL_x = x \cdot y \qquad \text{and} \qquad yR_x = y \cdot x.$$

Let

$$x\backslash y = yL_x^{-1} = y\mathbb{L}_x \qquad \text{and} \qquad x/y = xR_y^{-1} = x\mathbb{R}_y.$$

L is called a weak inverse property loop (WIPL) if and only if it obeys the weak inverse property (WIP);

$$xy \cdot z = e \text{ implies } x \cdot yz = e \text{ for all } x, y, z \in L$$

while L is called a cross inverse property loop (CIPL) if and only if it obeys the cross inverse property (CIP);

$$xy \cdot x^{\rho} = y.$$

The triple $\alpha = (A, B, C)$ of bijections on a loop $(L, \cdot)$ is called an autotopism of the loop if and only if

$$xA \cdot yB = (x \cdot y)C \text{ for all } x, y \in L.$$

Such triples form a group $AUT(L, \cdot)$ called the autotopism group of $(L, \cdot)$. In case the three bijections are the same i.e $A = B = C$, then any of them is called an automorphism and the group $AUM(L, \cdot)$ which such forms is called the automorphism group of $(L, \cdot)$. For an overview of the theory of loops, readers may check [36, 7, 9, 13, 22, 38, 25].

Osborn [35], while investigating the universality of WIPLs discovered that a universal WIPL $(G, \cdot)$ obeys the identity

$$yx \cdot (z\theta_y \cdot y) = (y \cdot xz) \cdot y \text{ for all } x, y, z \in G \tag{1.1}$$

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

A loop that necessarily and sufficiently satisfies this identity is called an Osborn loop.

Eight years after Osborn's [35] 1960 work on WIPL, in 1968, Huthnance Jr. [24] studied the theory of generalized Moufang loops. He named a loop that obeys (1.1) 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 [10]. Basarab [3, 4, 5] and Basarab and

Belioglo [6] dubbed a loop $(G,\cdot)$ satisfying any of the following equivalent identities an Osborn loop:

$$OS_2 \ : \ x(yz\cdot x) = (x^{\lambda}\backslash y)\cdot zx \tag{1.2}$$

$$OS_3 \ : \ (x\cdot yz)x = xy\cdot (zE_x^{-1}\cdot x) \tag{1.3}$$

$$\text{where } E_x = R_xR_{x^{\rho}} = (L_xL_{x^{\lambda}})^{-1} = R_xL_xR_x^{-1}L_x^{-1} \text{ for all } x,y,z\in G$$

and the binary operations '\' and '/' are respectively defines as ; $z = x\cdot y$ if and only if $x\backslash z = y$ if and only if $z/y = x$ for all $x,y,z\in G$.

It will look confusing if both Basarab's and Huthnance's definitions of an Osborn loop are both adopted because an Osborn loop of Basarab is not necessarily a universal WIPL(Osborn loop of Huthnance). So in this work, Huthnance's definition of an Osborn loop will be dropped while we shall stick to that of Basarab which was actually adopted by M. K. Kinyon [28] who revived the study of Osborn loops in 2005 at a conference tagged "Milehigh Conference on Loops, Quasigroups and Non-associative Systems" held at the University of Denver, where he presented a talk titled "A Survey of Osborn Loops".

Let $t = x^{\lambda}\backslash y$ in OS_2, then $y = x^{\lambda}t$ so that we now have an equivalent identity

$$x[(x^{\lambda}y)z\cdot x] = y\cdot zx.$$

Huthnance [24] was able to deduce some properties of E_x relative to (1.1). $E_x = E_{x^{\lambda}} = E_{x^{\rho}}$. So, since $E_x = R_xR_{x^{\rho}}$, then $E_x = E_{x^{\lambda}} = R_{x^{\lambda}}R_x$ and $E_x = (L_{x^{\rho}}L_x)^{-1}$. So, we now have the following equivalent identity defining an Osborn loop.

$$\mathrm{OS}_0 \ : \ x(yz\cdot x) = x(yx^{\lambda}\cdot x)\cdot zx \tag{1.4}$$

Definition 2. *A loop $(Q,\cdot)$ is called:*

(a) *a 3 power associative property loop(3-PAPL) if and only if $xx\cdot x = x\cdot xx$ for all $x\in Q$.*

(b) *a left self inverse property loop(LSIPL) if and only if $x^{\lambda}\cdot xx = x$ for all $x\in Q$.*

(c) *a right self inverse property loop(RSIPL) if and only if $xx\cdot x^{\rho} = x$ for all $x\in Q$.*

The identities describing the most popularly known varieties of Osborn loops are given below.

Definition 3. *A loop $(Q,\cdot)$ is called:*

(a) *a VD-loop if and only if*

$$(\cdot)_x = (\cdot)^{L_x^{-1}R_x} \qquad \text{and} \qquad {}_x(\cdot) = (\cdot)^{R_x^{-1}L_x}$$

i.e $R_x^{-1}L_x \in PS_{\lambda}(Q,\cdot)$ with companion $c = x$ and $L_x^{-1}R_x \in PS_{\rho}(Q,\cdot)$ with companion $c = x$ for all $x\in Q$ where $PS_{\lambda}(Q,\cdot)$ and $PS_{\rho}(Q,\cdot)$ are respectively the left and right pseudo-automorphism groups of Q. Basarab [5]

(b) *a Moufang loop if and only if the identity*

$$(xy)\cdot(zx) = (x\cdot yz)x$$

holds in Q.

(c) *a conjugacy closed loop(CC-loop) if and only if the identities*

$$x\cdot yz = (xy)/x\cdot xz \qquad \text{and} \qquad zy\cdot x = zx\cdot x\backslash(yx)$$

hold in Q.

(d) *a universal WIPL if and only if the identity*

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

holds in Q *and all its isotopes.*

All these three varieties of Osborn loops and universal WIPLs are universal Osborn loops. CC-loops and VD-loops are G-loops. G-loops are loops that are isomorphic to all their loop isotopes. Kunen [32] has studied them.

In the multiplication group $\mathcal{M}\text{ult}(Q)$ of a loop $(G,\cdot)$ are found three important permutations, namely, the right, left and middle inner mappings $R_{(x,y)} = R_xR_yR_{xy}^{-1}$, $L_{(x,y)} = L_xL_yL_{yx}^{-1}$ and $T_{(x)} = R_xL_x^{-1}$ respectively which form the right inner mapping group $\text{Inn}_{\lambda}(G)$, left inner mapping group $\text{Inn}_{\rho}(G)$ and the middle inner mapping $\text{Inn}_{\mu}(G)$. In a Moufang loop G, $R_{(x,y)}, L_{(x,y)}, T_{(x)} \in PS_{\rho}(G)$ with companions $(x,y),(x^{-1},y^{-1}),x^{-3} \in G$ respectively.

Theorem 4. *(Kinyon [28])*
Let G *be an Osborn loop.* $R_{(x,y)} \in PS_{\rho}(G)$ *with companion* $(xy)^{\lambda}(y^{\lambda}\backslash x)$ *and* $L_{(x,y)} \in PS_{\lambda}(G)\ \forall\ x,y \in G$. *Furthermore,* $R_{(x,y)}^{-1} = [L_{y^{\rho}}^{-1}, R_x^{-1}] = L_{(y^{\lambda},x^{\lambda})}\ \forall\ x,y \in G$.

The second part of Theorem 4 is trivial for Moufang loops. For CC-loops, it was first observed by Drápal and then later by Kinyon and Kunen [31].

Theorem 5. *Let* G *be an Osborn loop.* $Inn_{\rho}(G) = Inn_{\lambda}(G)$.

Still mysterious are the middle inner mappings $T_{(x)}$ of an Osborn loop. In a Moufang loop, $T_{(x)} \in PS_{\rho}$ with a companion x^{-3} while in a CC-loop, $T_{(x)} \in PS_{\lambda}$ with companion x. So, Kinyon [28] possessed a question asking of which group(whether PS_{ρ} and PS_{λ}) to which $T_{(x)}$ belongs to in case of an arbitrary Osborn loop and what its companion will be.

Theorem 6. *(Kinyon [28])*
In an Osborn loop G *with centrum* $C(G)$ *and center* $Z(G)$*:*

1. *If* $T_{(a)} \in AUM(G)$, *then* $a \cdot aa = aa \cdot a \in N(G)$. *Thus, for all* $a \in C(G)$, $a^3 \in Z(G)$.

2. *If* $(xx)^\rho = x^\rho x^\rho$ *holds, then* $x^{\rho\rho\rho\rho\rho\rho} = x$ *for all* $x \in G$.

Some basic loop properties such as flexibility, left alternative property(LAP), left inverse property(LIP), right alternative property(RAP), right inverse property(RIP), anti-automorphic inverse property(AAIP) and the cross inverse property(CIP) have been found to force an Osborn loop to be a Moufang loop. This makes the study of Osborn loops more challenging and care must be taking not to assume any of these properties at any point in time except the WIP, automorphic inverse property and some other generalizations of the earlier mentioned loop properties(LAP, LIP, e.t.c.).

Lemma 7. *An Osborn loop that is flexible or which has the LAP or RAP or LIP or RIP or AAIP is a Moufang loop. But an Osborn loop that is commutative or which has the CIP is a commutative Moufang loop.*

Theorem 8. *(Basarab, [4])*
If an Osborn loop is of exponent 2, then it is an abelian group.

Theorem 9. *(Huthnance [24])*
Let G *be a WIPL.* G *is a universal WIPL if and only if* G *is an Osborn loop.*

Lemma 10. *(Lemma 2.10, Huthnance [24])*
Let L *be a WIP Osborn loop. If* $a = x^\rho x$, *then for all* $x \in L$:

$$xa = x^{\lambda^2},\ ax^\lambda = x^\rho,\ x^\rho a = x^\lambda,\ ax = x^{\rho^2},\ xa^{-1} = ax,\ a^{-1}x^\lambda = x^\lambda a,\ a^{-1}x^\rho = x^\rho a.$$

or equivalently

$$J_\lambda : x \mapsto x \cdot x^\rho x,\ J_\rho : x \mapsto x^\rho x \cdot x^\lambda,\ J_\lambda : x \mapsto x^\rho \cdot x^\rho x,\ J_\rho^2 : x \mapsto x^\rho x \cdot x,$$

$$x(x^\rho x)^{-1} = (x^\rho x)x,\ (x^\rho x)^{-1}x^\lambda = x^\lambda \cdot x^\rho x,\ (x^\rho x)^{-1}x^\rho = x^\rho(x^\rho x).$$

Consider $(G, \cdot)$ and $(H, \circ)$ been two distinct groupoids or quasigroups or 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

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

So, $(H, \circ)$ is called a groupoid(quasigroup, loop) isotope of $(G, \cdot)$.

If $C = I$ is the identity map on G so that $H = G$, then the triple $\alpha = (A, B, I)$ is called a principal isotopism of $(G, \cdot)$ onto $(G, \circ)$ and $(G, \circ)$ is called a principal isotope of $(G, \cdot)$. Eventually, the equation of relationship now becomes

$$x \cdot y = xA \circ yB \ \forall\ x, y \in G$$

which is easier to work with. But if $A = R_g$ and $B = L_f$, for some $f, g \in G$, the relationship now becomes

$$x \cdot y = xR_g \circ yL_f \ \forall \ x, y \in G$$

or

$$x \circ y = xR_g^{-1} \cdot yL_f^{-1} \ \forall \ x, y \in G.$$

With this new form, the triple $\alpha = (R_g, L_f, I)$ is called an f, g-principal isotopism of $(G, \cdot)$ onto $(G, \circ)$, f and g are called translation elements of G or at times written in the pair form (g, f), while $(G, \circ)$ is called an f, g-principal isotope of $(G, \cdot)$.

The last form of α above gave rise to an important result in the study of loop isotopes of loops.

Theorem 11. *(Bruck [7])*
Let $(G, \cdot)$ and $(H, \circ)$ be two distinct isotopic loops. For some $f, g \in G$, there exists an f, g-principal isotope $(G, *)$ of $(G, \cdot)$ such that $(H, \circ) \cong (G, *)$.

With this result, to investigate the isotopic invariance of an isomorphic invariant property in loops, one simply needs only to check if the property in consideration is true in all f, g-principal isotopes of the loop. A property is isotopic invariant if whenever it holds in the domain loop i.e $(G, \cdot)$ then it must hold in the co-domain loop i.e $(H, \circ)$ which is an isotope of the formal. In such a situation, the property in consideration is said to be a universal property hence the loop is called a universal loop relative to the property in consideration as often used by Nagy and Strambach [34] in their algebraic and geometric study of the universality of some types of loops. For instance, if every loop isotope of a loop with property $\mathcal{P}$ also has the property $\mathcal{P}$, then the formal is called a universal $\mathcal{P}$ loop. So, we can now restate Theorem 11 as :

Theorem 12. *Let $(G, \cdot)$ be a loop with an isomorphic invariant property $\mathcal{P}$. $(G, \cdot)$ is a universal $\mathcal{P}$ loop if and only if every f, g-principal isotope $(G, *)$ of $(G, \cdot)$ has the $\mathcal{P}$ property.*

Definition 13. *(Universal Osborn Loop) A loop is called a universal Osborn loop if all its loop isotopes are Osborn loops.*

The aim of this study is to identify some identities that are appropriate for cryptography in universal Osborn loops. These identities hold in universal Osborn loops like CC-loops, introduced by Goodaire and Robinson [20, 21], whose algebraic structures have been studied by Kunen [33] and some recent works of Kinyon and Kunen [29, 31], Phillips et. al. [30], Drápal [14, 15, 16, 18], Csörgő et. al. [12, 19, 11] and VD-loops whose study is yet to be explored. In this study, by establishing an identity for universal Osborn loops, two other identities(of degrees 4 and 6) are deduced from it and they are recognized and recommended for cryptography in a

similar spirit in which the cross inverse property(of degree 2) has been used by Keedwell following the fact that it was observed that universal Osborn loops that do not have the 3-power associative property or weaker forms of; inverse property, power associativity and diassociativity to mention a few, will have cycles(even long ones). These identities are found to be cryptographic in nature for universal Osborn loops and thereby called cryptographic identities. They were also found applicable to security patterns, arrangements and networks which the CIP may not be applicable to.

We shall make use of the following results.

Results of Bryant and Schneider [8]

Theorem 14. *Let $(Q,\cdot,\backslash,/)$ be a quasigroup. If $Q(a,b,\circ)\overset{\theta}{\cong}Q(c,d,*)$ for any $a,b,c,d\in Q$, then $Q(f,g,\circledcirc)\overset{\theta}{\cong}Q\big((f\cdot b)\theta/d, c\backslash(a\cdot g)\theta,\star\big)$ for any $a,b,c,d,f,g\in Q$. If $(Q,\cdot)$ is a loop, then*

$(f\cdot b)\theta/d=[f\cdot(a\backslash c\theta^{-1})]\theta$ *and* $c\backslash(a\cdot g)\theta=[(d\theta^{-1}/b)\cdot g]\theta$ *for any* $a,b,c,d,f,g\in Q$.

2 Main Results

2.1 Identities In Universal Osborn Loops

Theorem 15. *Let $(Q,\cdot,\backslash,/)$ be an Osborn loop, $(Q,\circ)$ an arbitrary principal isotope of $(Q,\cdot)$ and $(Q,*)$ some principal isotopes of $(Q,\cdot)$. Let*

$$\phi(x,u,v)=(u\backslash([(uv)/(u\backslash(xv))]v))$$

and $\gamma=\gamma(x,u,v)=\mathbb{R}_vR_{[u\backslash(xv)]}\mathbb{L}_uL_x$ for all $x,u,v\in Q$, then $(Q,\cdot,\backslash,/)$ is a universal Osborn loop if and only if the commutative diagram

$$\begin{array}{ccc} & & (Q,*) \\ & \overset{(R_{\phi(x,u,v)},L_u,I)}{\nearrow} & \Big\downarrow{\scriptstyle (\gamma,\gamma,\gamma)}\ \textit{isomorphism} \\ (Q,\cdot) & \underset{\textit{principal isotopism}}{\xrightarrow{(R_v,L_x,I)}} & (Q,\circ) \end{array} \tag{2.1}$$

holds.

Proof. Let $\mathcal{Q}=(Q,\cdot,\backslash,/)$ be an Osborn loop with any arbitrary principal isotope $\mathfrak{Q}=(Q,\blacktriangle,\nwarrow,\nearrow)$ such that

$$x\blacktriangle y=xR_v^{-1}\cdot yL_u^{-1}=(x/v)\cdot(u\backslash y)\ \forall\ u,v\in Q.$$

If $\mathcal{Q}$ is a universal Osborn loop then, $\mathfrak{Q}$ is an Osborn loop. $\mathfrak{Q}$ obeys identity OS_0 implies

$$x\blacktriangle[(y\blacktriangle z)\blacktriangle x]=\{x\blacktriangle[(y\blacktriangle x^{\lambda'})\blacktriangle x]\}\blacktriangle(z\blacktriangle x) \tag{2.2}$$

where $x^{\lambda'} = xJ_{\lambda'}$ is the left inverse of x in $\mathfrak{Q}$. The identity element of the loop $\mathfrak{Q}$ is uv. So,

$$x\blacktriangle y = xR_v^{-1} \cdot yL_u^{-1} \text{ implies } y^{\lambda'}\blacktriangle y = y^{\lambda'}R_v^{-1} \cdot yL_u^{-1} = uv \text{ implies}$$

$$y^{\lambda'}R_v^{-1}R_{yL_u^{-1}} = uv \text{ implies } yJ_{\lambda'} = (uv)R_{yL_u^{-1}}^{-1}R_v = (uv)R_{(u\backslash y)}^{-1}R_v = [(uv)/(u\backslash y)]v.$$

Thus, using the fact that

$$x\blacktriangle y = (x/v) \cdot (u\backslash y),$$

$\mathfrak{Q}$ is an Osborn loop if and only if

$$(x/v)\cdot u\backslash\{[(y/v)\cdot(u\backslash z)]/v\cdot(u\backslash x)\} = ((x/v)\cdot u\backslash\{[(y/v)(u\backslash([(uv)/(u\backslash x)]v))]/v\cdot(u\backslash x)\})/v\cdot u\backslash[(z/v)(u\backslash x)].$$

Do the following replacements:

$$x' = x/v \Rightarrow x = x'v,\ z' = u\backslash z \Rightarrow z = uz',\ y' = y/v \Rightarrow y = y'v$$

we have

$$x'\cdot u\backslash\{(y'z')/v\cdot[u\backslash(x'v)]\} = (x'\cdot u\backslash\{[y'(u\backslash([(uv)/(u\backslash(x'v))]v))]/v\cdot[u\backslash(x'v)]\})/v\cdot u\backslash[((uz')/v)(u\backslash(x'v))].$$

This is precisely identity OS_0' below by replacing x', y' and z' by x, y and z respectively.

$$\underbrace{x\cdot u\backslash\{(yz)/v\cdot[u\backslash(xv)]\} = (x\cdot u\backslash\{[y(u\backslash([(uv)/(u\backslash(xv))]v))]/v\cdot[u\backslash(xv)]\})/v\cdot u\backslash[((uz)/v)(u\backslash(xv))]}_{\mathrm{OS}_0'}.$$

Writing identity OS_0' in autotopic form, we will obtain the fact that the triple $\big(\alpha(x,u,v),\beta(x,u,v),\gamma(x,u,v)\big) \in AUT(\mathcal{Q})$ for all $x,u,v \in Q$ where $\alpha(x,u,v) = R_{(u\backslash([(uv)/(u\backslash(xv))]v))}\mathbb{R}_vR_{[u\backslash(xv)]}\mathbb{L}_uL_x\mathbb{R}_v$, $\beta(x,u,v) = L_u\mathbb{R}_vR_{[u\backslash(xv)]}\mathbb{L}_u$ and $\gamma(x,u,v) = \mathbb{R}_vR_{[u\backslash(xv)]}\mathbb{L}_uL_x$ are elements of $\mathcal{M}\mathrm{ult}(Q)$. The triple

$$\big(\alpha(x,u,v),\beta(x,u,v),\gamma(x,u,v)\big) = \Big(R_{(u\backslash([(uv)/(u\backslash(xv))]v))}\gamma\mathbb{R}_v, L_u\gamma\mathbb{L}_x, \gamma\Big)$$

can be written as the following compositions

$$\Big(R_{(u\backslash([(uv)/(u\backslash(xv))]v))}, L_u, I\Big)(\gamma,\gamma,\gamma)(\mathbb{R}_v,\mathbb{L}_x,I).$$

Let $(Q,\circ)$ be an arbitrary principal isotope of $(Q,\cdot)$ and $(Q,*)$ a particular principal isotope of $(Q,\cdot)$ under the isotopism $(R_{\phi(x,u,v)}, L_u, I)$ where

$$\phi(x,u,v) = (u\backslash([(uv)/(u\backslash(xv))]v)).$$

Then, the composition above can be expressed as:

$$(Q,\cdot) \xrightarrow[\text{principal isotopism}]{(R_{\phi(x,u,v)},L_u,I)} (Q,*) \xrightarrow[\text{isomorphism}]{(\gamma,\gamma,\gamma)} (Q,\circ) \xrightarrow[\text{principal isotopism}]{(\mathbb{R}_v,\mathbb{L}_x,I)} (Q,\cdot).$$

The proof of the converse is as follows. Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be an Osborn loop. Assuming that the composition in equation (2.1) holds, then doing the reverse of the proof of necessity, $\big(\alpha(x,u,v), \beta(x,u,v), \gamma(x,u,v)\big) \in AUT(\mathcal{Q})$ for all $x, u, v \in Q$ which means that $\mathcal{Q}$ obeys identity OS'_0 hence, it will be observed that equation (2.2) is true for any arbitrary u,v-principal isotope $\mathfrak{Q} = (Q, \blacktriangle, \nwarrow, \nearrow)$ of $\mathcal{Q}$. So, every f,g-principal isotope $\mathfrak{Q}$ of $\mathcal{Q}$ is an Osborn loop. Following Theorem 12, $\mathcal{Q}$ is a universal Osborn loop if and only if $\mathfrak{Q}$ is an Osborn loop. □

Theorem 16. *A universal Osborn loop $(Q, \cdot, \backslash, /)$ obeys the identity*

$$\underbrace{(u[x\backslash(zv)])/[u\backslash(xv)] \cdot v = (\{u \cdot x\backslash\{z \cdot u\backslash((u/v)[u\backslash(xv)])\}\}/[u\backslash(xv)] \cdot v) \cdot u\backslash([(uv)/(u\backslash(xv))]v).}_{OSI_0^1}$$

for all $x, z, u, v \in Q$.

Furthermore, $\underbrace{z = x \cdot \{[x\backslash(zx)]/x \cdot x^{\lambda}\}x}_{OSI_0^{1.1}}$ *and* $\underbrace{(x^{\lambda} \cdot xy)x^{\lambda} \cdot x = y}_{\text{double left inverse property(DLIP)}}$

are also satisfied for all $x, y, z \in Q$.

Proof. By equation (2.1) of Theorem 15, it can be deduced that if $(Q, \circ)$ and $(Q, *)$ are principal isotopes of $(Q, \cdot)$ and $\gamma(x,u,v) = \mathbb{R}_v R_{[u\backslash(xv)]} \mathbb{L}_u L_x$, then

$$(Q, x, v, \circ) \overset{\gamma^{-1}}{\cong} (Q, u, \phi(x,u,v), *) \text{ where } \phi(x,u,v) = (u\backslash([(uv)/(u\backslash(xv))]v)) \quad \text{for all } x, u, v \in Q.$$

Let $Q(z, y, \circledcirc)$ be an arbitrary principal isotope of $(Q, \cdot)$. We now switch to Theorem 14. Let $a = x$, $b = v$, $c = u$, $d = \phi(x,u,v) = (u\backslash([(uv)/(u\backslash(xv))]v))$, $f = z$ and $g = y$. $\theta = \gamma(x,u,v)^{-1} = \mathbb{L}_x L_u \mathbb{R}_{[u\backslash(xv)]} R_v$ while $\theta^{-1} = \gamma(x,u,v) = \mathbb{R}_v R_{[u\backslash(xv)]} \mathbb{L}_u L_x$.

$$(f \cdot b)\theta/d = \{(u[x\backslash(zv)])/[u\backslash(xv)] \cdot v\}/\{u\backslash([(uv)/(u\backslash(xv))]v)\} \text{ and}$$

$$[f \cdot (a\backslash c\theta^{-1})]\theta = \{u \cdot x\backslash\{z \cdot u\backslash((u/v)[u\backslash(xv)])\}\}/[u\backslash(xv)] \cdot v.$$

Thus, $(f \cdot b)\theta/d = [f \cdot (a\backslash c\theta^{-1})]\theta$ if and only if identity OSI_0^1 is obeyed by $(Q, \cdot, \backslash, /)$.

The next formulae after OSI_0^1 derived by putting $u = v = e$ into OSI_0^1. Consequently, $T_{(x)} = \mathbb{L}_x \mathbb{R}_x \mathbb{R}_{x^{\lambda}} R_x$. In an Osborn loop, $T_{(x)} = L_{x^{\lambda}} R_x$, so we have the DLIP. □

2.2 Application Of Two Universal Osborn Loops Identities To Cryptography

Among the few identities that have been established for universal Osborn loops in Theorem 16, we would recommend two of them; $\mathrm{OSI}_0^{1.1}$ and DLIP for cryptography in a similar spirit in which the cross inverse property has been used by Keedwell

[27]. It will be recalled that CIPLs 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, 2] 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.

In Corollary 3.4 of Jaiyéọlá and Adéníran [26], it was established that in a universal Osborn loop, $J_\lambda = J_\rho$, 3-PAP, LSIP and RSIP are equivalent conditions. Furthermore, in a CC-loop, the power associativity property, 3-PAPL, $x^\rho = x^\lambda$, LSIP and RSIPL were shown to be equivalent in Corollary 3.5. Thus, universal Osborn loops without the LSIP or RSIP will have cycles(even long ones). This exempts groups, extra loops, and Moufang loops but includes CC-loops, VD-loops and universal WIPLs. Precisely speaking, non-power associative CC-loops will have cycles. So broadly speaking, universal Osborn loops that do not have the LSIP or RSIP or 3-PAPL or weaker forms of inverse property, power associativity and diassociativity to mention a few, will have cycles(even long ones). The next step now is to be able to identify suitably chosen identities in universal Osborn loops, that will do the job the identity $xy \cdot x^\rho = y$ or its equivalents does in the application of CIPQ to cryptography. These identities will be called Osborn cryptographic identities(or just cryptographic identities).

Definition 17. *(Cryptographic Identity and Cryptographic Functional)*
Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a quasigroup. An identity $w_1(x, x_1, x_2, x_3, \cdots, x_n) = w_2(x, x_1, x_2, x_3, \cdots, x_n)$ where $x \in Q$ is fixed,

$$x_1, x_2, x_3, \cdots, x_n \in Q, x \notin \{x_1, x_2, x_3, \cdots, x_n\}$$

is said to be a cryptographic identity(CI) of the quasigroup $\mathcal{Q}$ if it can be written in a functional form $xF(x_1, x_2, x_3, \cdots, x_n) = x$ such that $F(x_1, x_2, x_3, \cdots, x_n) \in \mathcal{M}ult(\mathcal{Q})$. $F(x_1, x_2, x_3, \cdots, x_n) = F_x$ is called the corresponding cryptographic functional(CF) of the CI at x.

Lemma 18. *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a loop with identity element e and let $CF_x(\mathcal{Q})$ be the set of all CFs in $\mathcal{Q}$ at $x \in Q$. Then, $CF_x(\mathcal{Q}) \leq \mathcal{M}ult(\mathcal{Q})$ and $CF_e(\mathcal{Q}) \leq Inn(\mathcal{Q})$.*

Proof. The proof is easy and can be achieved by simply verifying the group axioms in $CF_x(\mathcal{Q})$ and $CF_e(\mathcal{Q})$.

1. **Closure** Obviously by definition, $CF_x(\mathcal{Q}) \subset \mathcal{M}\text{ult}(\mathcal{Q})$. Let $F_1, F_2 \in CF_x(\mathcal{Q})$. So, $xF_1F_2 = xF_2 = x$ which implies that $F_1F_2 \in CF_x(\mathcal{Q})$.

Associativity Trivial.

Identity $xI = x$. So, $I \in CF_x(\mathcal{Q})$.

Inverse $F \in CF_x(\mathcal{Q}) \Rightarrow xF = x \Rightarrow xF^{-1} = x \Rightarrow F^{-1} \in CF_x(\mathcal{Q})$.

$\therefore CF_x(\mathcal{Q}) \leq \mathcal{M}\text{ult}(\mathcal{Q})$.

2. Obviously by definition, $CF_e(\mathcal{Q}) \subset \text{Inn}(\mathcal{Q})$. The procedure of the proof that $CF_e(\mathcal{Q}) \leq \text{Inn}(\mathcal{Q})$ is similar to that for $CF_x(\mathcal{Q}) \leq \mathcal{M}\text{ult}(\mathcal{Q})$

□

Definition 19. *(Degree of Cryptographic Identity and Cryptographic Functional)* *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a quasigroup and $\mathcal{I}$ an identity in $\mathcal{Q}$. If $\mathcal{I}$ is a CI with CF F, then the functions $F_1, F_2, F_3, \cdots F_n \in \mathcal{M}ult(Q)$ are called the n-components of F, written $F = (F_1, F_2, F_3, \cdots, F_n)$ if $F = F_1 \circ F_2 \circ F_3 \circ \cdots \circ F_n$. The maximum $n \in \mathbb{Z}^+$ such that $F = F_1 \circ F_2 \circ F_3 \circ \cdots \circ F_n$ is called the degree of F or I.*

Example 20. *Consider a CIPQ L. The identity $\mathcal{I} : xy \cdot x^\rho = y$ is a CI at any point $y \in L$ with CF $F(x) = F_y = L_x R_{x^\rho}$. It can be seen that $F(x) = F_1(x)F_2(x)$ where $F_1(x) = L_x$ and $F_2(x) = R_{x^\rho}$, thus, $F(x) = (L_x, R_{x^\rho})$. $\mathcal{I}$ is of degree 2. Note that an F of rank 1 is the identity mapping I.*

Lemma 21. *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a quasigroup and $\mathcal{I}$ an identity in $\mathcal{Q}$. If $\mathcal{I}$ is a CI with CF F at any point $x \in Q$ such that $F = (F_1, F_2)$, then $F_1 \in CF_x(\mathcal{Q})$ if and only if $F_2 \in CF_x(\mathcal{Q})$.*

Proof. $F = (F_1, F_2)$ implies that $xF = xF_1F_2 = x$. Thus, $F_1 \in CF_x(\mathcal{Q}) \Leftrightarrow xF_2 = x \Leftrightarrow F_2 \in CF_x(\mathcal{Q})$. □

Lemma 22. *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a quasigroup and $\mathcal{I}$ an identity in $\mathcal{Q}$. If $\mathcal{I}$ is a CI with CF F at any point $x \in Q$ such that $F = (F_1, F_2, F_3, \cdots, F_n)$, then $F_1, F_2, F_3, \cdots, F_{n-1} \in CF_x(\mathcal{Q})$ implies $F_n \in CF_x(\mathcal{Q})$.*

Proof. $F = (F_1, F_2, F_3, \cdots, F_n)$ implies that $xF = xF_1F_2F_3 \cdots F_n = x$. Thus, $F_1, F_2, F_3, \cdots, F_{n-1} \in CF_x(\mathcal{Q}) \Rightarrow xF_n = x \Rightarrow F_n \in CF_x(\mathcal{Q})$. □

Lemma 23. *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a quasigroup.*

1. *$T_{(x)} \in CF_z(\mathcal{Q})$ if and only if $z \in C(x)$ for all $x, z \in Q$,*
2. *$R_{(x,y)} \in CF_z(\mathcal{Q})$ if and only if $z \in N_\lambda(x, y)$ for all $x, y, z \in Q$,*
3. *$L_{(x,y)} \in CF_z(\mathcal{Q})$ if and only if $z \in N_\rho(x, y)$ for all $x, y, z \in Q$,*

where $N_\lambda(x, y) = \{z \in Q \mid zx \cdot y = z \cdot xy\}$, $N_\rho(x, y) = \{z \in Q \mid y \cdot xz = yx \cdot z\}$ and $C(z) = \{y \in Q \mid zy = yz\}$.

Proof. 1. $T_{(x)} \in CF_y(\mathcal{Q}) \Leftrightarrow yT_{(x)} = y \Leftrightarrow yR_x = yL_x \Leftrightarrow yx = xy \Leftrightarrow y \in C(x)$.

2. $R_{(x,y)} \in CF_z(\mathcal{Q}) \Leftrightarrow zR_{(x,y)} = z \Leftrightarrow zR_xR_y = zR_{xy} \Leftrightarrow zx \cdot y = z \cdot xy \Leftrightarrow z \in N_\lambda(x,y)$.

3. $L_{(x,y)} \in CF_z(\mathcal{Q}) \Leftrightarrow zL_{(x,y)} = z \Leftrightarrow zL_xL_y = zL_{yx} \Leftrightarrow y \cdot xz = yx \cdot z \Leftrightarrow z \in N_\rho(x,y)$.

□

Lemma 24. *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a left universal Osborn loop. Then, the identities $OSI_0^{1.1}$ and DLIP are CIs with degrees 6 and 4 respectively.*

Proof. From Theorem 16:

$\mathbf{OSI_0^{1.1}}$ is $z = x\cdot\{[x\backslash(zx)]/x\cdot x^\lambda\}x$, which can be put in the form $z = zR_x\mathbb{L}_x\mathbb{R}_xR_{x^\lambda}R_xL_x$. Thus, $\mathrm{OSI}_0^{1.1}$ is a CI with CF $F(x) = R_x\mathbb{L}_x\mathbb{R}_xR_{x^\lambda}R_xL_x$ of degree 6.

DLIP is $x^\lambda \cdot xy)x^\lambda \cdot x = y$, which can be put in the form $yL_xL_{x^\lambda}R_{x^\lambda}R_x = y$. Thus, $\mathrm{OSI}_0^{1.1}$ is a CI with CF $F(x) = L_xL_{x^\lambda}R_{x^\lambda}R_x$ of degree 4.

□

2.3 Discussions

Since the identities $\mathrm{OSI}_0^{1.1}$ and DLIP have degrees 6 and 4 respectively, then they are "stronger" than the CIPI which has a degree of 2 and hence will posse more challenge for an attacker(than the CIPI) to break into a system. As described by Keedwell, for a CIP, it is assumed that the message to be transmitted can be represented as single element x of a CIP quasigroup and that this is enciphered by multiplying by another element y of the CIPQ so that the encoded message is yx. At the receiving end, the message is deciphered by multiplying by the inverse of y. But for the identities $\mathrm{OSI}_0^{1.1}$ and DLIP, procedures of enciphering and deciphering are more than one in a universal Osborn loop. For instance, if the CFs of identities $\mathrm{OSI}_0^{1.1}$ and DLIP are F and G, respectively such that $F = F_1F_2$ and $G = G_1G_2$ where

$$F_1 = R_x\mathbb{L}_x\mathbb{R}_x,\ F_2 = R_{x^\lambda}R_xL_x,\ G_1 = L_xL_{x^\lambda} \text{ and } G_2 = R_{x^\lambda}R_x.$$

If it is assumed that the message to be transmitted can be represented as single element y of a universal Osborn loop and that this is enciphered by transforming with F_1 or G_1 so that the encoded message is xF_1 or xG_1. At the receiving end, the message is deciphered by transforming by F_2 or G_2. Note that the components of F and G are not necessarily unique. This gives room for any choice of set of components. F_1 or G_1 will be called the sender's functional component(SFC) while F_2 or G_2 will be called the receiver's functional component(RFC).

2.4 Many Receivers

So far, we have considered how to secure information in a situation whereby there is just one sender and one receiver(this is the only case which the CIP is useful for). There are some other advanced and technical information dissemination patterns(which the CIP may not be applicable to) in institutions and organization such as financial institutions in which the information or data to be sent must pass through some other parties(who are not really cautious of the sensitive nature of the incoming information) before it gets to the main receiver. For instance, let us consider a network structure of an organization which has n terminals. Say terminals A_i, $1 \leq i \leq n$. Imagine that terminal A_1 wants to get a secured information across to terminal A_n such that the information must pass through terminals $A_2, A_3, \cdots, A_{n-1}$. Then, we need a CI $\mathcal{I}$ with CF F of degree n so that $F = (F_1, F_2, F_3, \cdots, F_n)$. Thus, by making F_i to be A_i's functional component, then if the information x is not to be known by $A_2, A_3, \cdots, A_{n-1}$, we would make use of a F which does not obey the hypothesis of Lemma 22. That is, $F_1, F_2, F_3, \cdots, F_{n-1} \notin CF_x$. But if it is the other way round, an F which obeys the hypothesis of Lemma 22 must be sort for. The advantage of a CF F of higher degrees $n \geq 3$ over the CIPI relative to the number of attackers is illustrated below.

$$A_1 \xrightarrow[\uparrow \text{Attacker } 1 \uparrow]{F_1 \text{ Secured}} A_2 \xrightarrow[\uparrow \text{Attacker } 2 \uparrow]{F_2 \text{ Secured}} A_3 \cdots \rightarrow \cdots A_{n-1} \xrightarrow[\uparrow \text{Attacker } n-1 \uparrow]{F_n \text{ Secured}} A_n.$$

Let us now illustrate with an example, the use of universal Osborn loops for cryptography. But before then, it must be mentioned that experts have found it very difficult to construct a non-universal Osborn loop. According to Michael Kinyon during our personal contact with him, there are two difficulties with using software for looking for non-universal Osborn loops. One is that non-Moufang, non-CC Osborn loops are very sparse: they do not start to show up until order 16(and the two of order 16 happen to be G-loops.) The other difficulty is that once you start to pass about order 16, the software slows down considerably. One of the two Osborn loops that are G-loops constructed by Kinyon is shown in Table 2.

Example 25. *We shall now use the universal Osborn loop(it is a G-loop) of order* 16 *in Table 2 to illustrate encoding and decoding.*

Message: *OSBORN.*

CI: *DLIP.*

CF: $G(x) = L_x L_{x^\lambda} R_{x^\lambda} R_x$

Degree of CF: *4.*

Encipherer: $x = 16,\ x^\lambda = 16^\lambda = 10.$

LETTER	ENCIPHERING $y' = yG_1$	DECIPHERING $y'G_1G_2 = y$	DECODED LETTER
B	$10(16 \cdot 7) = 7$	$(7 \cdot 10)16 = 7$	7
N	$10(16 \cdot 9) = 12$	$(12 \cdot 10)16 = 9$	9
O	$10(16 \cdot 11) = 9$	$(9 \cdot 10)16 = 11$	11
R	$10(16 \cdot 12) = 10$	$(10 \cdot 10)16 = 12$	12
S	$10(16 \cdot 13) = 16$	$(16 \cdot 10)16 = 13$	13

Table 1: A Table of cryptographic Process using identity DLIP in a universal Osborn loop

SFC: $G_1 = L_x L_{x^\lambda}$.

RFC: $G_2 = R_{x^\lambda} R_x$.

Representation(y): $B \leftrightarrow 7$, $N \leftrightarrow 9$, $O \leftrightarrow 11$, $R \leftrightarrow 12$, $S \leftrightarrow 13$.

The information to be transmitted is "OSBORN". The encoded message is

$$(9, 16, 7, 9, 10, 12)$$

while the message decoded is $(11, 13, 7, 11, 12, 9)$. *The computation for this is as shown in Table 1.*

References

[1] R. Artzy, *On loops with a special property*, Proc. Amer. Math. Soc. **6** (1955), 448–453. MR0069804(16,1083e). Zbl 0066.27101.

[2] R. Artzy, *Inverse-Cycles in Weak-Inverse Loops*, Proc. Amer. Math. Soc. **68**, 2 (1978), 132–134. MR0463340 (57#3293). Zbl 0353.20059.

[3] A. S. Basarab, *The Osborn loop*, Studies in the theory of quasigroups and loops, **193** (1973) Shtiintsa, Kishinev, 12–18. MR0369591 (51#5824).

[4] A. S. Basarab, *Osborn's $\mathcal{G}$-loop*, Quasigroups and Related Systems **1** (1994), 51–56. MR1327945 (96e:20098). Zbl 0951.20506.

[5] A. S. Basarab, *Generalised Moufang G-loops*, Quasigroups and Related Systems **3** (1996), 1–6. MR1745960. Zbl 0944.20051.

[6] A. S. Basarab and A. I. Belioglo, *UAI Osborn loops*, Quasigroups and loops, Mat. Issled. **51** (1979), 8–13. MR0544327 (80h:20103b). Zbl 0439.20051.

[7] R. H. Bruck, *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1966. Zbl 0141.01401.

[8] B. F. Bryant and H. Schneider, *Principal loop-isotopes of quasigroups*, Canad. J. Math. **18** (1966), 120–125. MR0188333 (32#5772). Zbl 0132.26405.

[9] O. Chein, H. O. Pflugfelder and J. D. H. Smith, *Quasigroups and loops : Theory and applications*, Heldermann Verlag, 1990. MR1125806 (93g:20133). Zbl 0719.20036.

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

[11] P. Csörgő, *Extending the structural homomorphism of LCC loops*, Comment. Math. Univ. Carolinae **46** (2005) 3, 385–389. MR2174517 (2006g:20114). Zbl 1106.20051.

[12] P. Csörgő and A. Drápal, *Left conjugacy closed loops of nilpotency class 2*, Results Math. **47** (2005), 242–265. MR2153496 (2006b:20095). Zbl 1097.20053.

[13] J. Dene and A. D. Keedwell, *Latin squares and their applications*, the English University press Lts, 1974. MR0351850 (50 #4338). Zbl 0283.05014.

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
3	3	4	1	2	7	8	5	6	11	12	9	10	15	16	13	14
4	4	3	2	1	8	7	6	5	12	11	10	9	16	15	14	13
5	5	6	8	7	1	2	4	3	13	14	16	15	10	9	11	12
6	6	5	7	8	2	1	3	4	14	13	15	16	9	10	12	11
7	7	8	6	5	3	4	2	1	15	16	14	13	12	11	9	10
8	8	7	5	6	4	3	1	2	16	15	13	14	11	12	10	9
9	9	10	11	12	15	16	13	14	5	6	7	8	3	4	1	2
10	10	9	12	11	16	15	14	13	6	5	8	7	4	3	2	1
11	11	12	9	10	13	14	15	16	8	7	6	5	2	1	4	3
12	12	11	10	9	14	13	16	15	7	8	5	6	1	2	3	4
13	13	14	16	15	12	11	9	10	1	2	4	3	7	8	6	5
14	14	13	15	16	11	12	10	9	2	1	3	4	8	7	5	6
15	15	16	14	13	10	9	11	12	4	3	1	2	6	5	7	8
16	16	15	13	14	9	10	12	11	3	4	2	1	5	6	8	7

Table 2: The first Osborn loop of order 16 that is a G-loop

[14] A. Drápal, *Conjugacy closed loops and their multiplication groups*, J. Alg. **272** (2004), 838–850. MR2028083 (2004i:20125). Zbl 1047.20049.

[15] A. Drápal, *Structural interactions of conjugacy closed loops*, Trans. Amer. Math. Soc. **360** (2008), 671–689. MR2346467 (2009a:20118). Zbl 1144.20043.

[16] A. Drápal, *On multiplication groups of left conjugacy closed loops*, Comment. Math. Univ. Carolinae **45** (2004), 223–236. MR2075271 (2005e:20102) Zbl 1101.20035.

[17] A. Drápal, *On extraspecial left conjugacy closed loops*, J. Alg. **302** (2) (2006), 771–792. MR2293781 (2008b:20081). Zbl 1109.20056.

[18] A. Drápal (2004), *On left conjugacy closed loops with a nucleus of index two*, Abh. Math. Sem. Univ. Hamburg **74** (2004), 205–221. MR2112832 (2005k:20173). Zbl 1084.20043.

[19] P. Csörgő and A. Drápal, *On left conjugacy closed loops in which the left multiplication group is normal*, Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg, **76** (2006) 17–34. MR2293429 (2008g:20150). Zbl 1128.20052.

[20] E. G. Goodaire and D. A. Robinson, *A class of loops which are isomorphic to all loop isotopes*, Can. J. Math. **34** (1982), 662–672. MR0663308 (83k:20079). Zbl 0467.20052.

[21] E. G. Goodaire and D. A. Robinson, *Some special conjugacy closed loops*, Canad. Math. Bull. **33** (1990), 73–78. MR1036860(91a:20077). Zbl 0661.20046.

[22] E. G. Goodaire, E. Jespers and C. P. Milies (1996), *Alternative loop rings*, NHMS(184), Elsevier, 1996.MR1433590(98e:17041). Zbl 0878.17029.

[23] R. L. Jr. Griess, *Code loops*, J. Alg. **100** (1986), 224–234.MR0839580 (87i:20124). Zbl 0589.20051.

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

[25] T. G. Jaíyéọlá, *A study of new concepts in Smarandache quasigroups and loops*, ProQuest Information and Learning (ILQ), Ann Arbor, USA, 2009. MR2489953. Zbl 1159.20035.

[26] T. G. Jaiyéọlá and J. O. Adéníran, *New identities in universal Osborn loops*, Quasigroups And Related Systems, Vol. 17 (2009). MR2536708. Zbl pre05578166.

[27] A. D. Keedwell, *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Combin. **20** (1999), 241—250. MR1723878 (2000h:20123). Zbl 0935.20061.

[28] M. K. Kinyon, *A survey of Osborn loops*, Milehigh conference on loops, quasigroups and non-associative systems, University of Denver, Denver, Colorado, 2005.

[29] M. K. Kinyon, K. Kunen, *The structure of extra loops*, Quasigroups and Related Systems **12** (2004), 39–60. MR2130578 (2006a:20121). Zbl 1076.20065.

[30] M. K. Kinyon, K. Kunen, J. D. Phillips, *Diassociativity in conjugacy closed loops*, Comm. Alg. 32 (2004), 767–786. MR2101839 (2005h:20159). Zbl 1077.20076 .

[31] M. K. Kinyon, K. Kunen, *Power-associative conjugacy closed loops*, J. Alg. **304** (2) (2006), 679–711. MR2264275 (2007h:20075). Zbl 1109.20057.

[32] K. Kunen, *G-loops and Permutation Groups*, J. Alg. **220** (1999), 694–708. MR1717366(2000j:20133). Zbl 0944.20056.

[33] K. Kunen, *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. **352** (2000), 2889–2911. MR1615991(2000j:20132). Zbl 0962.20048.

[34] P. T. Nagy and K. Strambach, *Loops as invariant sections in groups, and their geometry*, Canad. J. Math. **46** (1994), no. 5, 1027–1056. MR1295130 (95h:20088). Zbl 0814.20055.

[35] J. M. Osborn, *Loops with the weak inverse property*, Pac. J. Math. **10** (1961), 295–304. MR0111800 (22 #2660). Zbl 0091.02101.

[36] H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Sigma series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990. MR1125767 (93g:20132). Zbl 0715.20043.

[37] J. D. Phillips, *A short basis for the variety of WIP PACC-loops*, Quasigroups and Related Systems **1** (2006) 14, 73–80. MR2268827. Zbl 1123.20063.

[38] W. B. Vasantha Kandasamy, *Smarandache loops*, Department of Mathematics, Indian Institute of Technology, Madras, India, 2002. MR1958775 (2004a:20076). Zbl 1050.20045.

T. G. Jaiyéọlá
Obafemi Awolowo University,
Department of Mathematics,

Ile Ife 220005, Nigeria.
e-mail: jaiyeolatemitope@yahoo.com,tjayeola@oauife.edu.ng
http://www.oauife.edu.ng/faculties/science/mth/research.htm#jaiyeola

J. O. Adéníran
University of Agriculture,
Department of Mathematics,
Abeokuta 110101, Nigeria.
e-mail: ekenedilichineke@yahoo.com, adeniranoj@unaab.edu.ng
http://www.unaab.edu.ng/attachments/435_DR.%20Adeniran.pdf