On A Cryptographic Identity In Osborn Loops *†

T. G. Jaiyéọlá‡
Department of Mathematics,
Obafemi Awolowo University,
Ile Ife 220005, Nigeria.
jaiyeolatemitope@yahoo.com
tjayeola@oauife.edu.ng

J. O. Adéníran
Department of Mathematics,
University of Abeokuta,
Abeokuta 110101, Nigeria.
ekenedilichineke@yahoo.com
adeniranoj@unaab.edu.ng

Abstract

This study digs out some new algebraic properties of an Osborn loop that will help in the future to unveil the mystery behind the middle inner mappings $T_{(x)}$ of an Osborn loop. These new algebraic properties, will open our eyes more to the study of Osborn loops like CC-loops which has received a tremendious attention in this 21^{st} and VD-loops whose study is yet to be explored. In this study, some algebraic properties of non-WIP Osborn loops have been investigated in a broad manner. Huthnance was able to deduce some algebraic properties of Osborn loops with the WIP i.e universal weak WIPLs. So this work exempts the WIP. Two new loop identities, namely left self inverse property loop(LSIPL) identity and right self inverse property loop(RSLPL) are introduced for the first time and it is shown that in an Osborn loop, they are equivalent. A CC-loop is shown to be power associative if and only if it is a RSLPL or LSIPL. Among the few identities that have been established for Osborn loops, one of them is recognized and recommended for cryptography in a similar spirit in which the cross inverse property has been used by Keedwell following the fact that it was observed that 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). These identity is called an Osborn cryptographic identity(or just a cryptographic identity).

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 ;

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

*2000 Mathematics Subject Classification. Primary 20NO5 ; Secondary 08A05
†**Keywords and Phrases :** Osborn loops, cryptography
‡All correspondence to be addressed to this author.

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. $x^{\lambda^i} = (x^\lambda)^\lambda$ and $x^{\rho^i} = (x^\rho)^\rho$ for $i \geq 1$. 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 [32, 7, 8, 12, 21, 34].

Osborn [31], while investigating the universality of WIPLs discovered that a universal WIPL $(G,\cdot)$ obeys the identity

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

$$\text{where } \theta_y = L_yL_{y^\lambda} = R^{-1}_{y^\rho}R^{-1}_y = L_yR_yL^{-1}_yR^{-1}_y.$$

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

Eight years after Osborn's [31] 1960 work on WIPL, in 1968, Huthnance Jr. [23] 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 [9]. Basarab [3, 4, 5] and Basarab and Belioglo [6] dubbed a loop $(G,\cdot)$ satisfying any of the following equivalent identities an Osborn loop:

$$OS_2 \ : \ x(yz\cdot x) = (x^\lambda\backslash y)\cdot zx \tag{2}$$

$$OS_3 \ : \ (x\cdot yz)x = xy\cdot(zE^{-1}_x\cdot x) \tag{3}$$

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

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 [25] 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 [23] was able to deduce some properties of E_x relative to (1). $E_x = E_{x^\lambda} = E_{x^\rho}$. So, since $E_x = R_x R_{x^\rho}$, 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 identities defining an Osborn loop.

$$OS_2 \ : \ x[(x^\lambda y)z \cdot x] = y \cdot zx \tag{4}$$

$$OS_3 \ : \ (x \cdot yz)x = xy \cdot [(x^\lambda \cdot xz) \cdot x] \tag{5}$$

Definition 1.1 *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 1.2 *A loop $(Q, \cdot)$ is called:*

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

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

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*

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

hold in Q.

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

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

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 [29] has studied them.

In the multiplication group $\mathcal{M}(G,\cdot)$ 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 1.1 *(Kinyon [25])*
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, $R^{-1}_{(x,y)} = [L^{-1}_{y^\rho}, R^{-1}_x] = L_{(y^\lambda,x^\lambda)}$ $\forall\ x,y \in G$.

The second part of Theorem 1.1 is trivial for Moufang loops. For CC-loops, it was first observed by Drápal and then later by Kinyon and Kunen [28].

Theorem 1.2 *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. Kinyon [25], possess a question asking of what can be said in case of an arbitrary Osborn loop.

Theorem 1.3 *(Kinyon [25])*
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 1.1 *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 1.4 *(Basarab, [4])*
If an Osborn loop is of exponent 2, then it is an abelian group.

Theorem 1.5 *(Huthnance [23])*
Let G be a WIPL. G is a universal WIPL if and only if G is an Osborn loop.

Lemma 1.2 *(Lemma 2.10, Huthnance [23])*
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

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

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

The aim of this study is to dig out some new algebraic properties of an Osborn loop that will help in the future to unveil the mystery behind the middle inner mappings $T_{(x)}$ of an Osborn loop. These new algebraic properties, will open our eyes more to the study of Osborn loops like CC-loops, introduced by Goodaire and Robinson [19, 20], whose algebraic structures have been studied by Kunen [30] and some recent works of Kinyon and Kunen [26, 28], Phillips et. al. [27], Drápal [13, 14, 15, 17], Csörgő et. al. [11, 18, 10] and VD-loops whose study is yet to be explored. In this study, the algebraic properties of non-WIP Osborn loops have been investigated in a broad manner. Huthnance [23] was able to deduce some algebraic properties of Osborn loops with the WIP i.e universal WIPLs. So this work exempts the WIP. Two new loop identities, namely left self inverse property loop(LSIPL) identity and right self inverse property loop(RSLPL) are introduced for the first time and it is shown that in an Osborn loop, they are equivalent. A CC-loop is shown to be power associative if and only if it is a RSLPL or LSIPL. Among the few identities that have been established for Osborn loops, one of them is recognized and recommended for cryptography in a similar spirit in which the cross inverse property has been used by Keedwell following the fact that it was observed that 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). These identity is called an Osborn cryptographic identity(or just a cryptographic identity).

2 Main Results

2.1 Some Algebraic Properties Of Osborn Loops

Theorem 2.1 *Let $(L, \cdot)$ be a loop. L is an Osborn loop if and only if $(L_{x^\lambda}, R_x^{-1}, L_x^{-1}R_x^{-1}) \in AUT(L)$. Hence for all $x, y, z \in L$:*

1. $(L_{(x)}, L_{(x)}, L_xT_{(x)}R_x^{-1}) \in AUT(L)$ *for some* $L_{(x)} \in Inn_\lambda(L)$.

2. (a) $T_{(x)}\ :\ x\mapsto\ [(x^\lambda\cdot xy)(x^\lambda\cdot xy^\rho)]x.$
   (b) $T_{(x)}\ :\ x\mapsto\ [(x^\lambda\cdot xz^\lambda)(x^\lambda\cdot xz)]x.$
   (c) $T_{(x)}\ :\ y\mapsto\ x^\lambda y\cdot x$ *i.e* $T_{(x)}:=L_{x^\lambda}R_x.$

3. $yx=x(x^\lambda y\cdot x)$ *i.e* $R_x=L_{x^\lambda}R_xL_x.$

4. $(x^\lambda\cdot xy)(x^\lambda\cdot xy^\rho)=(x^\lambda\cdot xz^\lambda)(x^\lambda xz)=e.$

Proof
By OS_2, L is an Osborn loop if and only if $(L_{x^\lambda},R_x^{-1},L_x^{-1}R_x^{-1})\in AUT(L)$. By OS_3, L is an Osborn loop if and only if $(L_x,L_xL_{x^\lambda}R_x,L_xR_x)\in AUT(L)$.

1. Hence, $(L_{(x)},L_{(x)},L_xT_{(x)}R_x^{-1})\in AUT(L)$ where $L_{(x)}=L_xL_{x^\lambda}\in \text{Inn}_\lambda(L)$.
   The autotopism $(L_{(x)},L_{(x)},L_xT_{(x)}R_x^{-1})$ implies $[(x^\lambda\cdot xy)\cdot(x^\lambda\cdot xz)]x=(x\cdot yz)T_{(x)}$.

2. (a) So with $z=y^\rho$, $xT_{(x)}=[(x^\lambda\cdot xy)\cdot(x^\lambda\cdot xy^\rho)]x$.
   (b) Similarly, with $y=z^\lambda$, $xT_{(x)}=[(x^\lambda\cdot xz^\lambda)\cdot(x^\lambda\cdot xz)]x$.
   (c) With $y=e$ or $z=e$, $(xz)T_{(x)}=(x^\lambda\cdot xz)x$ which implies that $yT_{(x)}=(x^\lambda\cdot y)x$ or $zT_{(x)}=(x^\lambda\cdot z)x$ respectively.

3. Recall that $T_{(x)}=R_xL_x^{-1}$. Using this and $T_{(x)}=L_{x^\lambda}R_x$, $R_x=L_{x^\lambda}R_xL_x$.

4. Observe that $xT_{(x)}=x$, so by (b)i. and (b)ii. the claim is true.

Lemma 2.1 *Let $(L,\cdot)$ be an Osborn loop. The following are true.*

1. $(x^\lambda\cdot xy)^\rho=x^\lambda\cdot xy^\rho$, $(x^\lambda\cdot xy^\rho)^\lambda=(x^\lambda\cdot xy^\lambda)^\rho$.

2. $J_\rho\ :\ x\ \mapsto x^\lambda x^\lambda\cdot x$, $J_\rho^2\ :\ x\mapsto xx\cdot x^\rho$, $J_\lambda\ :\ x\mapsto\ (x^\lambda)^\lambda\cdot x^\lambda x^\rho$, $J_\lambda^2\ :\ x\mapsto\ x^\lambda\cdot xx$, $J_\lambda\ :\ x\mapsto\ (x^\lambda\cdot xx^\lambda)^2(x^\lambda\cdot xx)$, $J_\lambda\ :\ x\mapsto\ (x^\lambda x^\lambda\cdot x)^\lambda(x^\lambda x^\lambda\cdot x)^2$, $J_\lambda^3\ :\ x\ \mapsto x^\lambda\cdot xx^\lambda$

3.
$$x^\lambda\cdot xx^{\rho^2}=x,\qquad (x\cdot x^\rho x^\rho)^\lambda=x\cdot x^\rho x=(x\cdot x^\rho x^\lambda)^\rho,$$
$$(x^\lambda\cdot xx)^\lambda=x^\lambda\cdot xx^\lambda,\qquad x^{\lambda^3}\cdot x^{\lambda^2}x=x^\lambda\cdot xx,$$
$$(x^{\lambda^2}\cdot x^\lambda x^\rho)^{\lambda^2}\cdot(x^{\lambda^2}\cdot x^\lambda x^\rho)^\lambda(x^{\lambda^2}\cdot x^\lambda x^\rho)^\rho=x^\lambda\cdot xx,\qquad (x^\lambda\cdot xx^\lambda)^2(x^\lambda\cdot xx)=x^{\lambda^2}\cdot x^\lambda x^\rho,$$
$$(x^\lambda x^\lambda\cdot x)^\lambda(x^\lambda x^\lambda\cdot x)^2=(x^\lambda\cdot xx^\lambda)^2(x^\lambda\cdot xx),$$
$$(x^{\lambda^2}\cdot x^\lambda x^\rho)^\lambda(x^{\lambda^2}\cdot x^\lambda x^\rho)^2=x^\lambda\cdot xx^\lambda,\qquad (x^{\lambda^2}\cdot x^\lambda x^\rho)^\lambda=(x^{\lambda^2}\cdot x^\lambda x^\lambda)^\rho,$$
$$(x^\lambda\cdot xx)^{\lambda^2}\cdot(x^\lambda\cdot xx)^\lambda(x^\lambda\cdot xx)^\rho=x^\lambda\cdot xx^\lambda.$$

4.
$$(x\cdot x^\rho y^\rho)^\lambda=(x\cdot x^\rho y^\lambda)^\rho,\qquad (x^\lambda\cdot xy^{\rho^2})^\lambda=(x^\lambda\cdot xy)^\rho,$$
$$(x^{\lambda^2}\cdot x^\lambda y^\rho)^\lambda=(x^{\lambda^2}\cdot x^\lambda y^\lambda)^\rho,\qquad (x^\lambda\cdot xy)^\lambda=(x^\lambda\cdot xy^{\lambda^2})^\rho.$$

5. $|J_\lambda| = 2$ *iff* $|J_\rho| = 2$ *iff* $J_\lambda = J_\rho$ *iff* L *is a LSIPL iff RSIPL*

Proof
The whole these is gotten by intuitive use of (b), (c) and (d) of Theorem 2.1.

Corollary 2.1 *Let L be a CC-loop. The following are equivalent.*

1. *L is a power associativity loop*
2. *L is a 3-PAPL.*
3. *L obeys* $x^\rho = x^\lambda$ *for all* $x \in L$.
4. *L is a LSIPL.*
5. *L is a RSIPL.*

Proof
The proof the equivalence of the first three is shown in Lemma 3.20 of [30] and mentioned in Lemma 1.2 of [33]. The proof of the equivalence of the last two and the first three can be deduced from the last result of Lemma 2.1.

Remark 2.1 *This new algebraic definition gives more insight into the algebraic properties of Osborn loop. Particularly, it can be used to fine tune some recent equations on CC-loop as shown in works of Kunen, Kinyon, Phillips and Drapal; [27, 26, 28], [13, 14], [30]. In fact, in [27, 30], the authors focussed on the mapping* $E_x = R_x R_{x^\rho} = \theta_x^{-1}$ *where* $\theta_x = L_x L_{x^\lambda}$ *and were able to established study its algebraic properties in a CC-loop. So we can see that the investigations of* E_x *in CC-loops by Kunen, Kinyon and Phillips is a bit in line with what Huthnance [23] did with* θ_x *in a universal WIPL and WIP Osborn loop. In this work, attention has been paid primarily on Osborn loops. So this study is a general overview of the earlier ones. The identities LSIPL and RSIPL are appearing for the first time.*

2.2 Application Of An Osborn Loop Identity To Cryptography

Among the few identities that have been established for Osborn loops in Theorem 2.1, we would recommend one of them for cryptography in a similar spirit in which the cross inverse property has been used by Keedwell [24]. 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 the course of this study(Lemma 2.1), it has been established that in an Osborn loop, $J_\lambda = J_\rho$, LSIP and RSIP are equivalent conditions. Therefore, in a CC-loop, the power associativity property, 3-PAPL, $x^\rho = x^\lambda$, LSIP and RSIPL are equivalent. Thus, 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 and following some of the identities in Lemma 2.1, 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 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 2.1 *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a quasigroup. An identity $w_1(x, x_1, x_2, x_3, \cdots) = w_2(x, x_1, x_2, x_3, \cdots)$ where $x \in Q$ is fixed, $x_1, x_2, x_3, \cdots \in Q$, $x \notin \{x_1, x_2, x_3, \cdots\}$ is said to be a cryptographic identity(CI) of the loop $\mathcal{Q}$ if it can be written in a functional form $xF(x_1, x_2, x_3, \cdots) = x$ such that $F(x_1, x_2, x_3, \cdots) \in \mathcal{M}ult(\mathcal{Q})$. $F(x_1, x_2, x_3, \cdots) = F_x$ is called the corresponding cryptographic functional(CF) of the CI at x.*

Lemma 2.2 *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 $CF_e(\mathcal{Q}) \leq Inn(\mathcal{Q})$.*

Lemma 2.3 *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a quasigroup.*

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

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

Lemma 2.4 *Let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be an Osborn loop with identity element e. Then, the identity $yx = x(x^\lambda y \cdot x)$ is a CI with its CF $F_e \in CF_e(\mathcal{Q})$.*

Remark 2.2 *The identity $yx = x(x^\lambda y \cdot x) \Leftrightarrow y = [x(x^\lambda y \cdot x)]/x$ is more "advanced" than the CIPI and hence will posse more challenge for an attacker(even than the CIPI) to break into a systems. 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 identity $y = [x(x^\lambda y \cdot x)]/x$, procedures of enciphering and deciphering are more than one in an Osborn loop.*

References

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

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

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

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

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

[6] A. S. Basarab and A. I. Belioglo (1979), *UAI Osborn loops*, Quasigroups and loops, Mat. Issled. 51, 8–16.

[7] R. H. Bruck (1966), *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 185pp.

[8] O. Chein, H. O. Pflugfelder and J. D. H. Smith (1990), *Quasigroups and loops : Theory and applications*, Heldermann Verlag, 568pp.

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

[10] P. Csörgő (2005), *Extending the structural homomorphism of LCC loops*, Comment. Math. Univ. Carolinae 46, 3, 385–389.

[11] P. Csörgő and A. Drápal (2005), *Left conjugacy closed loops of nilpotency class 2*, Results Math. 47, 242–265.

[12] J. Dene and A. D. Keedwell (1974), *Latin squares and their applications*, the English University press Lts, 549pp.

[13] A. Drápal (2004), *Conjugacy closed loops and their multiplication groups*, J. Alg. 272, 838–850.

[14] A. Drápal, *Structural interactions of conjugacy closed loops*, Trans. Amer. Math. Soc. to appear.

[15] A. Drápal (2004), *On multiplicatipon groups of left conjugacy closed loops*, Comment. Math. Univ. Carolinae 45, 223–236.

[16] A. Drápal (2006), *On extraspecial left conjugacy closed loops*, J. alg. 302(2), 771–792.

[17] A. Drápal (2004), *On left conjugacy closed loops with a nucleus of index two*, Abh. Math. Sem. Univ. Hamburg 74, 205–221

[18] A. Drápal and P. Csörgő , *On left conjugacy closed loops in which the left multiplication group is normal*, Pre-print.

[19] E. G. Goodaire and D. A. Robinson (1982), *A class of loops which are isomorphic to all loop isotopes*, Can. J. Math. 34, 662–672.

[20] E. G. Goodaire and D. A. Robinson (1990), *Some special conjugacy closed loops*, Canad. Math. Bull. 33, 73–78.

[21] E. G. Goodaire, E. Jespers and C. P. Milies (1996), *Alternative loop rings*, NHMS(184), Elsevier, 387pp.

[22] R. L. Jr. Griess (1986), *Code loops*, J. Alg. 100, 224–234.

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

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

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

[26] M. K. Kinyon, K. Kunen (2004), *The structure of extra loops*, Quasigroups and Related Systems 12, 39–60.

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

[28] M. K. Kinyon, K. Kunen (2006), *Power-associative conjugacy closed loops*, J. Alg. 304(2), 679–711.

[29] K. Kunen (1999), *G-loops and Permutation Groups*, J. Alg. 220, 694–708.

[30] K. Kunen (2000), *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. 352, 2889–2911.

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

[32] H. O. Pflugfelder (1990), *Quasigroups and loops : Introduction*, Sigma series in Pure Math. 7, Heldermann Verlag, Berlin, 147pp.

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

[34] W. B. Vasantha Kandasamy (2002), *Smarandache loops*, Department of Mathematics, Indian Institute of Technology, Madras, India, 128pp.