ON ANOTHER TWO CRYPTOGRAPHIC IDENTITIES IN UNIVERSAL OSBORN LOOPS

T. G. Jaiyéolá 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;

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

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

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

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

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

\[
yL_x = x \cdot y \quad \text{and} \quad yR_x = y \cdot x.
\]

Let

\[
x \setminus y = yL_x^{-1} = yL_x \quad \text{and} \quad x/y = xR_y^{-1} = xR_y.
\]

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

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

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

\[
x \cdot x^\rho = y.
\]

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

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

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

\[
y \cdot x \cdot (z \theta_y \cdot y) = (y \cdot xz) \cdot y \quad \text{for all} \quad x, y, z \in G
\]

where \( \theta_y = L_yL_y^\lambda = R_y^{-1}R_y^{-1} = L_yR_yL_y^{-1}R_y^{-1} \).

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:

\[
\begin{align*}
\text{OS}_2 &: \ x(yz \cdot x) = (x^\lambda y) \cdot zx \\
\text{OS}_3 &: \ (x \cdot yz)x = xy \cdot (zE^{-1} \cdot x)
\end{align*}
\]

where \(E_x = R_x R_x^\rho = (L_x L_x^\lambda)^{-1} = R_x L_x R_x^{-1} L_x^{-1}\) for all \(x, y, z \in G\)

and the binary operations ’\(\backslash\)’ 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 \(t = x^\lambda y\) in \(\text{OS}_2\), 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 \(E_x = R_x R_x^\rho\), 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 identity defining an Osborn loop.

\[
\text{OS}_0 : \ x(yz \cdot x) = x(yx^\lambda \cdot x) \cdot zx
\]

**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

\[
(\cdot)_x = (\cdot)^{L_x^{-1}R_x} \quad \text{and} \quad x(\cdot) = (\cdot)^{R_x^{-1}L_x}
\]

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]

******************************************************************************

Surveys in Mathematics and its Applications 5 (2010), 17 – 34

http://www.utmjiu.ro/math/sma
(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

\[x \cdot yz = (xy)/x \cdot xz\]

and

\[zy \cdot x = zx \cdot x \\setminus (yx)\]

hold in \(Q\).

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

\[x(yx)\rho = y\rho \quad \text{or} \quad (xy)^\lambda x = y^\lambda\]

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 \(\text{Mult}(Q)\) of a loop \((G, \cdot)\) are found three important permutations, namely, the right, left and middle inner mappings \(R(x,y) = R_x R_y R_{xy}^{-1}\), \(L(x,y) = L_x L_y L_{yx}^{-1}\) and \(T(x) = R_x L_x^{-1}\) respectively which form the right inner mapping group \(\text{Inn}_\rho(G)\), left inner mapping group \(\text{Inn}_\lambda(G)\) 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 \((xy)^\lambda(y^\lambda \setminus x)\) and \(L(x,y) \in PS_\lambda(G)\) \(\forall x, y \in G\). Furthermore, \(R(x,y) = [L_{y^{-1}}, R_x^{-1}] = L_{(y^\lambda x^\lambda)} \forall x, y \in G\).

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. \(\text{Inn}_\rho(G) = \text{Inn}_\lambda(G)\).

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 \(PS_\rho\) and \(PS_\lambda\)) 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 \(Z(G)\):

**************************************************************************

Surveys in Mathematics and its Applications 5 (2010), 17 – 34
http://www.utgjiu.ro/math/sma
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 \( (xx)^p = x^p x^p \) holds, then \( x^{oppopp} = x \) 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 taken 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 \( a = x^p x \), then for all \( x \in L \):

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

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

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

*****************************************************************************

Surveys in Mathematics and its Applications 5 (2010), 17 – 34

http://www.utgjiu.ro/math/sma
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

\[
x \cdot y = xR_g \circ yL_f \quad \forall \, x, y \in G
\]

or

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

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 \( \alpha \) 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 \( P \) also has the property \( P \), then the formal is called a universal \( P \) loop. So, we can now restate Theorem 11 as:

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

Surveys in Mathematics and its Applications 5 (2010), 17 – 34

http://www.utgjiu.ro/math/sma
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 \((Q, \cdot, \setminus, /)\) be a quasigroup. If \(Q(a, b, \circ) \equiv Q(c, d, \ast)\) for any \(a, b, c, d \in Q\), then \(Q(f, g, \Theta) \equiv Q((f \cdot b)\Theta/d, c\setminus(a \cdot g)\Theta, \ast)\) for any \(a, b, c, d, f, g \in Q\). If \((Q, \cdot)\) is a loop, then \((f \cdot b)\Theta/d = [f \cdot (a \setminus (c \Theta^{-1}))] \Theta\) and \(c \setminus (a \cdot g)\Theta = [(d \Theta^{-1} / b) \cdot g] \Theta\) for any \(a, b, c, d, f, g \in Q\).

### 2 Main Results

**2.1 Identities In Universal Osborn Loops**

**Theorem 15.** Let \((Q, \cdot, \setminus, /)\) be an Osborn loop, \((Q, \circ)\) an arbitrary principal isotope of \((Q, \cdot)\) and \((Q, \ast)\) some principal isotopes of \((Q, \cdot)\). Let 
\[ \phi(x, u, v) = (u \setminus [(uv)/(u \setminus (xv))])v \]
and \(\gamma = \gamma(x, u, v) = R_uL_uR_vL_v\) for all \(u, v \in Q\), then \((Q, \cdot, \setminus, /)\) is a universal Osborn loop if and only if the commutative diagram

\[
\begin{array}{ccc}
(Q, \cdot) & \xrightarrow{(R_{(x,u,v)}L_uL_v, I)} & (Q, \circ) \\
\gamma & \xleftarrow{(R_{x,L_x}, L_x, I)} & \xrightarrow{(\gamma, \gamma, \gamma)} \text{isomorphism}
\end{array}
\]

holds.

**Proof.** Let \(Q = (Q, \cdot, \setminus, /)\) be an Osborn loop with any arbitrary principal isotope \(\Omega = (Q, \Lambda, \setminus, /)\) such that
\[ x \Lambda y = xR_u^{-1} \cdot yL_u^{-1} = (x/v) \cdot (u \setminus y) \forall u, v \in Q. \]
If \(Q\) is a universal Osborn loop then, \(\Omega\) is an Osborn loop. \(\Omega\) obeys identity OS0 implies
\[ x \Lambda [(y \Lambda z) \Lambda x] = \{x \Lambda [(y \Lambda x^N) \Lambda x]\} \Lambda (z \Lambda x) \]
where $x^\lambda = xJ_\lambda$ is the left inverse of $x$ in $Q$. The identity element of the loop $Q$ is $uv$. So,

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

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

Thus, using the fact that

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

$Q$ is an Osborn loop if and only if

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

Do the following replacements:

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

we have

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

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

Writing identity $OS_0'$ in autotopic form, we will obtain the fact that the triple $$(\alpha(x, u, v), \beta(x, u, v), \gamma(x, u, v)) \in AUT(Q)$$ for all $x, u, v \in Q$ where $\alpha(x, u, v) = R_{u\cup [u\backslash (u\cup (u\backslash x))]v} \cup \cup L_x \cup uv \cup \cup L_u \cup \cup u\cup \cup [u\cup (u\backslash x)]v$ and $\gamma(x, u, v) = \cup \cup L_u \cup \cup L_x$ are elements of $\mathcal{M}ult(Q)$. The triple

$$(\alpha(x, u, v), \beta(x, u, v), \gamma(x, u, v)) = \left( R_{(u\backslash ((uv)/(u\backslash x))]v} \cup v, L_u \cup L_x, \gamma \right)$$

can be written as the following compositions

$$\left( R_{(u\backslash ((uv)/(u\backslash x))]v} \cup v, L_u \cup L_x, I \right) \gamma \cup \cup v, (\cup \cup v, L_x, I).$$

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

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

Then, the composition above can be expressed as:

$$(Q, \cdot) \xrightarrow{(R_{\phi(x, u, v)}, L_u, I)} (Q, \ast) \xrightarrow{(\gamma, \gamma, \gamma)} (Q, \circ) \xrightarrow{(\cup \cup v, L_x, I)} (Q, \cdot).$$
The proof of the converse is as follows. Let $Q = (Q, \cdot, \backslash, /)$ be an Osborn loop. Assuming that the composition in equation (2.1) holds, then doing the reverse of the proof of necessity, $(\alpha(x, u, v), \beta(x, u, v), \gamma(x, u, v)) \in AUT(Q)$ for all $x, u, v \in Q$ which means that $Q$ obeys identity $OSI^0_0$, hence, it will be observed that equation (2.2) is true for any arbitrary $u, v$-principal isotope $Q = (Q, \cdot, \backslash, /)$ of $Q$. So, every $f, g$-principal isotope $Q$ of $Q$ is an Osborn loop. Following Theorem 12, $Q$ is a universal Osborn loop if and only if $Q$ is an Osborn loop.

**Theorem 16.** A universal Osborn loop $(Q, \cdot, \backslash, /)$ obeys the identity
\[(u[x\\backslash(zv)]/[u\backslash(xv)] \cdot v = ([u \cdot x[z \cdot u/(u\backslash(xv))]])/[u\backslash(xv)] \cdot v \cdot u/((uv)/(u\backslash(xv)))v)\]
for all $x, z, u, v \in Q$.

Furthermore, $z = x \cdot \{(x\backslash(zx))/x \cdot x^λ\}x$ and $λ \cdot x = y$

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 $(Q, \ast)$ are principal isotopes of $(Q, \cdot)$ and $γ(x, u, v) = \mathbb{R}_u R_{u\backslash(xv)} L_u L_x$, then
\[(Q, x, u, v, \circ) \bowtie (Q, u, φ(x, u, v), \ast) \text{ where } φ(x, u, v) = (u\backslash((uv)/(u\backslash(xv)))v)\]
for all $x, u, v \in Q$.

Let $Q(z, y, \circ)$ be an arbitrary principal isotope of $(Q, \cdot)$. We now switch to Theorem 14. Let $a = x, b = v, c = u, d = φ(x, u, v) = (u\backslash((uv)/(u\backslash(xv)))v)$, $f = z$ and $g = y$. $θ = γ(x, u, v)^{-1} = L_x L_u R_{u\backslash(xv)} L_v$ while $θ^{-1} = γ(x, u, v) = \mathbb{R}_u R_{u\backslash(xv)} L_u L_x$.

\[(f \cdot b)θ/d = \{([ux\backslash(zv)]/[ux\backslash(xv)] \cdot v)/(u\backslash((uv)/(u\backslash(xv)))v)\} \text{ and } \{f \cdot (a\backslash(cθ^{-1}))θ = \{u \cdot x[z \cdot u/(u\backslash(xv))]})/[u\backslash(xv)] \cdot v.\]

Thus, $(f \cdot b)θ/d = [f \cdot (a\backslash(cθ^{-1}))θ$ if and only if identity $OSI^1_0$ is obeyed by $(Q, \cdot, \backslash, /)$.

The next formulae after $OSI^1_0$ derived by putting $u = v = e$ into $OSI^1_0$. Consequently, $T(x) = L_x \mathbb{R}_x \mathbb{R}_x L_x$. In an Osborn loop, $T(x) = L_x L_x$, 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; $OSI^1_0$ 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 \(x_1^ρ = x_{k+1}\) 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 Jaiyéolá and Adéníran [26], it was established that in a universal Osborn loop, \(J_λ = J_ρ\), 3-PAP, LSIP and RSIP are equivalent conditions. Furthermore, in a CC-loop, the power associativity property, 3-PAPL, \(x^ρ = x^λ\), LSIP and RSIP 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 \(xy·x^ρ = y\) 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 \(Q = (Q, ·, \setminus, /)\) 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 \(Q\) if it can be written in a functional form \(xF(x_1, x_2, x_3, \cdots, x_n) = x\) such that \(F(x_1, x_2, x_3, \cdots, x_n) \in Mult(Q)\). \(F(x_1, x_2, x_3, \cdots, x_n) = F_x\) is called the corresponding cryptographic functional(CF) of the CI at \(x\).

**Lemma 18.** Let \(Q = (Q, ·, \setminus, /)\) be a loop with identity element \(e\) and let \(CF_x(Q)\) be the set of all CFs in \(Q\) at \(x \in Q\). Then, \(CF_x(Q) \leq Mult(Q)\) and \(CF_e(Q) \leq Inn(Q)\).

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

1. **Closure** Obviously by definition, \(CF_x(Q) \subset Mult(Q)\). Let \(F_1, F_2 \in CF_x(Q)\). So, \(xF_1F_2 = xF_2 = x\) which implies that \(F_1F_2 \in CF_x(Q)\).

*******************************************************************************

Surveys in Mathematics and its Applications 5 (2010), 17 – 34  
http://www.utgjiu.ro/math/sma
Consider a CIPQ (Degree of Cryptographic Identity and Cryptographic Functional) Let
\[ x \cdot I = x. \] So, \( I \in CF_x(Q) \).

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

\[ \therefore CF_x(Q) \leq \text{Mult}(Q). \]

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

**Definition 19.** (Degree of Cryptographic Identity and Cryptographic Functional)

Let \( Q = (Q, \cdot, \backslash, /) \) be a quasigroup and \( \mathcal{I} \) an identity in \( Q \). If \( \mathcal{I} \) is a CI with \( CF \), then the functions \( F_1, F_2, F_3, \ldots F_n \in \text{Mult}(Q) \) are called the \( n \)-components of \( F \), written \( F = (F_1, F_2, F_3, \ldots, F_n) \) 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 \( \mathcal{I} : xy \cdot x^o = y \) is a CI at any point \( y \in L \) with \( CF \ F(x) = F_y = L_xR_{x^o} \). It can be seen that \( F(x) = F_1(x)F_2(x) \) where \( F_1(x) = L_x \) and \( F_2(x) = R_{x^o} \), thus, \( F(x) = (L_x, R_{x^o}) \). \( \mathcal{I} \) is of degree 2. Note that an \( F \) of rank 1 is the identity mapping \( I \).

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

**Proof.** \( F = (F_1, F_2) \) implies that \( xF = xF_1F_2 = x \). Thus, \( F_1 \in CF_x(Q) \Leftrightarrow xF_2 = x \Leftrightarrow F_2 \in CF_x(Q) \). \( \square \)

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

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

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

1. \( T_{(x)} \in CF_x(Q) \) if and only if \( z \in C(x) \) for all \( x, z \in Q \),
2. \( R_{(x,y)} \in CF_x(Q) \) if and only if \( z \in N_{\lambda}(x, y) \) for all \( x, y, z \in Q \),
3. \( L_{(x,y)} \in CF_x(Q) \) 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 \( C(z) = \{ y \in Q \mid yz = yz \} \).
Proof. 1. \( T(x) \in C F_y(Q) \Leftrightarrow y T(x) = y \Leftrightarrow y R_x = y L_x \Leftrightarrow y x = xy \Leftrightarrow y \in C(x) \).

2. \( R_{(x,y)} \in C F_x(Q) \Leftrightarrow z R_{(x,y)} = z \Leftrightarrow z R_x R_y = z R_{xy} \Leftrightarrow z x \cdot y = z \cdot xy \Leftrightarrow z \in N_{\lambda}(x, y) \).

3. \( L_{(x,y)} \in C F_x(Q) \Leftrightarrow z L_{(x,y)} = z \Leftrightarrow z L_x L_y = z L_{yx} \Leftrightarrow y \cdot x z = y x \cdot z \Leftrightarrow z \in N_{\rho}(x, y) \).

Lemma 24. Let \( Q = (Q, \cdot, \backslash, /) \) be a left universal Osborn loop. Then, the identities \( OSI_{01}^{\cdot} \) and DLIP are CIs with degrees 6 and 4 respectively.

Proof. From Theorem 16:

\( OSI_{01}^{\cdot} \) is \( z = x \cdot \{ [x](z x) \} / x \cdot x^{\lambda} \} x \), which can be put in the form \( z = z R_x \backslash x R_x \cdot R_x \cdot L_x \).

Thus, \( OSI_{01}^{\cdot} \) is a CI with CF \( F(x) = R_x \backslash x R_x \cdot R_x \cdot L_x \). of degree 6.

DLIP is \( x^{\lambda} \cdot y x^{\lambda} \cdot x = y \), which can be put in the form \( y L_x L_x \cdot R_x \cdot R_x = y \). Thus, \( OSI_{01}^{\cdot} \) is a CI with CF \( F(x) = L_x L_x \cdot R_x \cdot R_x \) of degree 4.

\( \square \)

2.3 Discussions

Since the identities \( OSI_{01}^{\cdot} \) and DLIP have degrees 6 and 4 respectively, then they are “stronger” than the CIP which has a degree of 2 and hence will posse more challenge for an attacker (than the CIP) 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 \( y x \). At the receiving end, the message is deciphered by multiplying by the inverse of \( y \). But for the identities \( OSI_{01}^{\cdot} \) and DLIP, procedures of enciphering and deciphering are more than one in a universal Osborn loop. For instance, if the CFs of identities \( OSI_{01}^{\cdot} \) and DLIP are \( F \) and \( G \), respectively such that \( F = F_1 F_2 \) and \( G = G_1 G_2 \) where

\[
F_1 = R_x \backslash x R_x, \quad F_2 = R_x \cdot x R_x L_x, \quad G_1 = L_x L_x \cdot x \quad \text{and} \quad G_2 = R_x \cdot x R_x.
\]

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 \( x F_1 \) or \( x G_1 \). 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 organizations 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 \( A_1, A_2, \ldots, A_n \). Imagine that terminal \( A_1 \) wants to get a secured information across to terminal \( A_n \) such that the information must pass through terminals \( A_2, A_3, \ldots, A_{n-1} \). Then, we need a CI \( I \) with CF \( F \) of degree \( n \) so that \( F = (F_1, F_2, F_3, \ldots, F_n) \). Thus, by making \( F_1 \) to be \( A_1 \)'s functional component, then if the information \( x \) is not to be known by \( A_2, A_3, \ldots, A_{n-1} \), we would make use of a \( F \) which does not obey the hypothesis of Lemma 22. That is, \( F_1, F_2, F_3, \ldots, F_{n-1} \notin CF_x \). 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.

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:** \( G(x) = L_x L_{x^2} R_{x^3} R_x \)

**Degree of CF:** 4.

**Encipherer:** \( x = 16, \ x^\lambda = 16^\lambda = 10 \).

******************************************************************************

Surveys in Mathematics and its Applications 5 (2010), 17 - 34

http://www.utgjiu.ro/math/sma
LETTER | ENCIPHERING | DECIPHERING | DECODED LETTER
--- | --- | --- | ---
B | 10(16 · 7) = 7 | (7 · 10)16 = 7 | 7
N | 10(16 · 9) = 12 | (12 · 10)16 = 9 | 9
O | 10(16 · 11) = 9 | (9 · 10)16 = 11 | 11
R | 10(16 · 12) = 10 | (10 · 10)16 = 12 | 12
S | 10(16 · 13) = 16 | (16 · 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


******************************************************************************

Surveys in Mathematics and its Applications 5 (2010), 17 – 34

http://www.utgjiu.ro/math/sma
On Another Two Cryptographic Identities in Universal Osborn Loops


<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>6</td>
<td>5</td>
<td>8</td>
<td>7</td>
<td>10</td>
<td>9</td>
<td>12</td>
<td>11</td>
<td>14</td>
<td>13</td>
<td>16</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>7</td>
<td>8</td>
<td>5</td>
<td>6</td>
<td>11</td>
<td>12</td>
<td>9</td>
<td>10</td>
<td>15</td>
<td>16</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>12</td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>16</td>
<td>15</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>13</td>
<td>14</td>
<td>16</td>
<td>15</td>
<td>10</td>
<td>9</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>14</td>
<td>13</td>
<td>15</td>
<td>16</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>8</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>15</td>
<td>16</td>
<td>14</td>
<td>13</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>16</td>
<td>15</td>
<td>13</td>
<td>14</td>
<td>11</td>
<td>12</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>15</td>
<td>16</td>
<td>13</td>
<td>14</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>9</td>
<td>12</td>
<td>11</td>
<td>16</td>
<td>15</td>
<td>14</td>
<td>13</td>
<td>6</td>
<td>5</td>
<td>8</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>12</td>
<td>9</td>
<td>10</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>14</td>
<td>13</td>
<td>16</td>
<td>15</td>
<td>7</td>
<td>8</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>14</td>
<td>16</td>
<td>15</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>10</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>7</td>
<td>8</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>13</td>
<td>15</td>
<td>16</td>
<td>11</td>
<td>12</td>
<td>10</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>16</td>
<td>14</td>
<td>13</td>
<td>10</td>
<td>9</td>
<td>11</td>
<td>12</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>15</td>
<td>13</td>
<td>14</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>11</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>7</td>
</tr>
</tbody>
</table>

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

******************************************************************************

Surveys in Mathematics and its Applications 5 (2010), 17 – 34
http://www.utgjiu.ro/math/sma


******************************************************************************

Surveys in Mathematics and its Applications 5 (2010), 17 – 34

http://www.utgjiu.ro/math/sma
On Another Two Cryptographic Identities in Universal Osborn Loops


T. G. Jaiyéolá
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