УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ” - ШТИП
ФАКУЛТЕТ ЗА ИНФОРМАТИКА

ISSN 1857- 8691

ГОДИШЕН ЗБОРНИК
2012
YEARBOOK
2012

ГОДИНА 1 **VOLUME I**

GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“ – ШТИП
ФАКУЛТЕТ ЗА ИНФОРМАТИКА

ГОДИШЕН ЗБОРНИК
2012
YEARBOOK
2012

ГОДИНА 1 МАРТ, 2013 VOLUME I

GOCE DELCEV UNIVERSITY – STIP
FACULTY OF COMPUTER SCIENCE

ГОДИШЕН ЗБОРНИК
ФАКУЛТЕТ ЗА ИНФОРМАТИКА
YEARBOOK
FACULTY OF COMPUTER SCIENCE

За издавачот:
Проф д-р Владо Гичев

Редакција и администрација
Универзитет „Гоце Делчев“-Штип
Факултет за информатика
ул. „Крсте Мисирков“ 10-А
п. фах 201, 2000 Штип
Р. Македонија

Address of the editorial office
Goce Delcev University – Stip
Faculty of Computer Science
Krste Misirkov 10-A
PO box 201, 2000 Štip,
R. of Macedonia

СОДРЖИНА
CONTENT

ON THE APPLICATION OF KEEDWELL CROSS INVERSE QUASIGROUP TO CRYPTOGRAPHY

Jaíyéọlá Tèmítọpé Gbọláhàn

jaiyeolatemitope@yahoo.com, tjayeola@oauife.edu.ng

Department of Mathematics, Faculty of Science, Obafemi Awolowo University, Ile Ife 220005, Nigeria

On the 50th Anniversary of Obafemi Awolowo University

Abstract: In 1999, A. D. Keedwell found cross inverse property quasigroups (CIPQs) applicable to J. H. Ellis's original schema for a public key encryption. The present study devices a mechanism of changing the use of the Keedwell CIPQs against attack on a system(as required by the author). This is done as follows. The holomorphic structure of automorphic inverse property quasigroups (loops) [AIPQs (AIPLs)] and cross inverse property quasigroups (loops) [CIPQs (CIPLs)] are investigated. Necessary and sufficient conditions for the holomorph of a quasigroup(loop) to be an AIPQ (AIPL) or CIPQ (CIPL) are established. It is shown that if the holomorph of a quasigroup(loop) is a AIPQ(AIPL) or CIPQ (CIPL), then the holomorph is isomorphic to the quasigroup(loop). Hence, the holomorph of a quasigroup(loop) is an AIPQ (AIPL) or CIPQ (CIPL) if and only if its automorphism group is trivial and the quasigroup(loop) is a AIPQ(AIPL) or CIPQ (CIPL). Furthermore, it is discovered that if the holomorph of a quasigroup(loop) is a CIPQ (CIPL), then the quasigroup (loop) is a flexible unipotent CIPQ(flexible CIPL of exponent 2). By constructing two isotopic quasigroups(loops) U and V such that their automorphism groups are not trivial, it is shown that U is a AIPQ or CIPQ (AIPL or CIPL) if and only if V is a AIPQ or CIPQ (AIPL or CIPL). Explanations are given on how these CIPQs can be incorporated into the encryption scheme of Keedwell for higher security using a computer.

Keywords: holomorph of loops, automorphic inverse property loops (AIPLs), cross inverse property loops (CIPLs), automorphism group, cryptography

1 Introduction and Preliminaries

Let L be a non-empty set. Define a binary operation $(\cdot)$ on L. If $x \cdot y \in L$ for all $x, y \in L$, $(L,\cdot)$ is called a groupoid. If the equations: $a \cdot x = b \quad and \quad y \cdot a = b$

have unique solutions for x and y respectively, then $(L,\cdot)$ is called a quasigroup. Let J_ρ be a permutation on L with inverse mapping J_λ i.e. $J_\rho^{-1} = J_\lambda$ and for each $x \in L$, let $x^\rho = xJ_\rho$ and $x^\lambda = xJ_\lambda$. Also, let

$$x^{\lambda^i} = \underbrace{((x^\lambda)^\lambda)^{\cdots}}_{i-times} \; and \; x^{\rho^i} = \underbrace{((x^\rho)^\rho)^{\cdots}}_{i-times} \; for \; i \geq 1.$$

Now, if there exists a unique element $e \in L$ called the identity element such that for all $x \in L$, $x \cdot e = e \cdot x = x$, $(L,\cdot)$ is called a loop. Hence, in a loop, if x^ρ and x^λ obey the relations $xx^\rho = e$ and $x^\lambda x = e$ respectively, they are called the right and left inverses of x respectively.

For a loop $(L,\cdot)$, recall the classic definition of its Holomorph. Let $Hol(L) = L \times Aut(L)$ and with multiplication defined on it as follows:

$$(x,\alpha)(y,\beta) = (x \cdot \alpha(y), \alpha\beta).$$

But because we shall be mapping from the left, we shall adopt the definition of a loop in Bruck [8]. Let the set $H = H(L) = Hol(L) = Aut(L) \times L$. If we define ' $\circ$ ' on H such that $(\alpha,x) \circ (\beta,y) = (\alpha\beta, x\beta \cdot y) \; \forall \; (\alpha,x),(\beta,y) \in Hol(L),$ then $(Hol(L),\circ)$ is a loop as shown in Bruck [8] and is called the Holomorph of $(L,\cdot)$.

Definition 1. *A loop(quasigroup) is a weak inverse property loop (quasigroup)[WIPL(WIPQ)] if and only if it obeys the identity* $x(yx)^\rho = y^\rho \quad or \quad (xy)^\lambda x = y^\lambda$.

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

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

A loop (quasigroup) is an automorphic inverse property loop (quasigroup) [AIPL(AIPQ)] if and only if it obeys the identity $(xy)^{\rho} = x^{\rho} y^{\rho}$ *or* $(xy)^{\lambda} = x^{\lambda} y^{\lambda}$

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

If $(G,\cdot) = (H,\circ)$, then the triple $\alpha = (A,B,C)$ of bijections on $(G,\cdot)$ is called an autotopism of the groupoid (quasigroup, loop) $(G,\cdot)$. Such triples form a group $AUT(G,\cdot)$ called the autotopism group of $(G,\cdot)$. Furthermore, if $A = B = C$, then A is called an automorphism of the groupoid(quasigroup, loop) $(G,\cdot)$. Such bijections form a group $Aut(G,\cdot)$ called the automorphism group of $(G,\cdot)$.

As observed by Osborn [21], a loop is a WIPL and an AIPL if and only if it is a CIPL. The past efforts of Artzy [3, 6, 5, 4], Belousov and Curkan [7] and recent studies of Keedwell [17], Keedwell and Shcherbacov [18, 19, 20] are of great significance in the study of WIPLs, AIPLs, CIPQs and CIPLs, their generalizations(i.e m-inverse loops and quasigroups, (r,s,t)-inverse quasigroups) and applications to cryptography.

Interestingly, Adeniran [1] and Robinson [22], Adeniran et. al. [2], Chiboka and Solarin [10], Bruck [8], Bruck and Paige [9], Robinson [23], Huthnance [15] and Adeniran [1] have respectively studied the holomorphs of Bol loops, central loops, conjugacy closed loops, inverse property loops, A-loops, extra loops, weak inverse property loops, Osborn loops and Bruck loops. Huthnance [15] showed that if $(L,\cdot)$ is a loop with holomorph $(H,\circ)$, $(L,\cdot)$ is a WIPL if and only if $(H,\circ)$ is a WIPL. The holomorphs of an AIPL and a CIPL were first studied by Jaiyéọlá in [16].

For the purpose of applying CIPQs to cryptography, Keedwell [17] needed to construct CIPQs with long inverse cycles. He constructed the following CIPQ which we shall specifically call Keedwell CIPQ and explained in much detail

how a CIPQ with a specified long inverse cycle may be constructed and stored economically in a computer.

Theorem 1. *(Keedwell CIPQ) Let* $(G,\cdot)$ *be an abelian group of order* n *such that* $n+1$ *is composite. Define a binary operation* $'\circ'$ *on the elements of* G *by the relation* $a\circ b=a^r b^s$, *where* $rs=n+1$. *Then* $(G,\circ)$ *is a CIPQ and the right crossed inverse of the element* a *is* a^u, *where* $u=(-r)^3$.

The author also gave examples and detailed explanation and procedures of the use of this CIPQ for cryptography. Cross inverse property quasigroups have been found appropriate for cryptography because of the fact that the left(right) inverse of x^λ (x^ρ) is not necessarily x unlike in left and right inverse property loops where $(x^\lambda)^\lambda=x$ and $(x^\rho)^\rho=x$. 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 $x_k^\rho=x_{k+1} \bmod n$. The number n is called the length of the cycle. The origin of the idea of cycles can be traced back to Artzy [3, 6] 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 CIPLs. We shall call these "Cycle Theorems" for now.

In Keedwell [17], the author showed that a CIPQ provides a means of applying directly J. H. Ellis's original schema for a public key encryption system in which the receiver takes part in the encryption process. See J. H. Ellis [12], [13] and [14].

A few years later, the same idea was propounded by W. Diffie and M. E. Hellman [11]. Their work was probably independent of that of Ellis because Ellis was prevented by the Official Secrets Act from publishing his ideas or any of their proposed subsequent implementations described in [13]. On the other hand, the paper of Diffie and Hellman and the subsequent practical implementations of it are very well known.

We shall now highlight the relevant part of [13] as recorded by Keedwell [17]:

1. Suppose the recipient has two tables T_1 and T_3 while the sender has one, T_2 . These machine tables are not secret and may be supposed to be

possessed by the interceptor. T_1 takes an input k and produces an output x. T_2 takes inputs x and p giving an output z. T_3 takes inputs z and k. All these quantities are large numbers of the same magnitude. We can think of T_1 as a linear table of simple list, while T_2 and T_3 are square tables.

2. In operation, p is the message which is to be sent and k is a random number, chosen by the recipient. He enciphers k by T_1 to get x which he sends. The sender uses x to encipher p with T_2 to get z, the cipher text, which he sends back. Now, the recipient uses k to decipher z by means of T_3. It is clearly possible for the entries of T_3 to give p under these circumstances, we have achieved our objective.

3. If the numbers are large enough and T_1 and T_2 sufficiently random to avoid working backwards, p cannot be found without knowing k. In public encryption terms, x is the public encipherment key and k is the private decipherment key.

Let $(L,\circ)$ be a CIPQ with long inverse cycle $(a,a^{\lambda},a^{\lambda^2},a^{\lambda^3},\cdots,a^{\lambda^{t-1}})$ of length t and suppose that both the sender S and the receiver R are provided with apparatus which will compute $x\circ y$ for any given $x,y\in L$. The latin square representing this quasigroup acts as the look up tables T_2 and T_3 and the long inverse cycle of the quasigroup serves as the third look up table T_1.

The receiver R selects randomly one element $a^{(u)}\in L$ of the long inverse cycle and uses it to obtain $a^{(u)}J^{-1}=a^{(u-1)}$ which he sends to S who has a message $m\in L$ which he wishes to transmit to R. S uses $a^{(u-1)}$ to encipher m as $a^{(u-1)}\circ m$ which he sends back to R. Now R uses $a^{(u)}$ to decipher $a^{(u-1)}\circ m$ as $(a^{(u-1)}\circ m)\circ a^{(u)}=m$. Here, $a^{(u-1)}$ is the public encipherment key, $a^{(u)}$ is the private decipherment key.

According to Keedwell [17], the systems described by Ellis is not a public key encryption system as presently understood because a new key k is chosen for each new message (or part massge) which is to be sent.

For a present-day public key implementation of the idea, the author found it necessary to keep secret the algorithm for obtaining the right cross inverse of each element of L. So the implementation might be carried out as follows:

A key distribution centre would be established. Each user would have a computer programmed to calculate $x \circ y$ for every pair $x, y \in L$. Only the key distribution centre would have knowledge of the long inverse cycle and would use it to distribute a public key $a_i^{(u)}$ and a private key $a_i^{(u+1)}$ to each user U_i. When user U_i wished to send a message m to user U_j, he would send $a_j^{(u)} \circ m$ which U_j could decipher using his private key $a_j^{(u+1)}$.

However, *this scheme is not very secure* unless a mechanism is set up by which the CIPQ $(L,\circ)$ is changed fairly frequently. The system is more effective if implemented as a one-time pad which is in effect what Ellis was describing. For example, it might be used

(i) for sending a message $m = m_1 m_2 \ldots m_r$ in which each portion of the message has its own enciphering and deciphering keys; or

(ii) for key exchange without the intervention of key distribution centre in the following way:

The sender S selects arbitrarily(using physical random number generator) an element $a^{(u)}$ of the CIPQ $(L,\circ)$ and sends both $a^{(u)}$ and the enciphered key or message $a^{(u)} \circ m$. The receiver R uses his knowledge of the algorithm for obtaining $a^{(u+1)}$ from $a^{(u)}$ (as given in Theorem 1.1, for instance) and hence he computes $(a^{(u)} \circ m) \circ a^{(u+1)} = m$.

The aim of the present study is to device a mechanism of constructing a CIPQ which can be used fairly frequently to replace the CIPQ in the above encryption process in order for it to be well secured against attack. This is done as follows.

1. The holomorphic structure of AIPQs(AIPLs) and CIPQs(CIPLs) are investigated. Necessary and sufficient conditions for the holomorph of a quasigroup(loop) to be an AIPQ(AIPL) or CIPQ(CIPL) are established. It is shown that if the holomorph of a quasigroup(loop) is a AIPQ(AIPL) or

CIPQ(CIPL), then the holomorph is isomorphic to the quasigroup(loop). Hence, the holomorph of a quasigroup(loop) is an AIPQ(AIPL) or CIPQ(CIPL) if and only if its automorphism group is trivial and the quasigroup(loop) is a AIPQ(AIPL) or CIPQ(CIPL). Furthermore, it is discovered that if the holomorph of a quasigroup(loop) is a CIPQ(CIPL), then the quasigroup(loop) is a flexible unipotent CIPQ (flexible CIPL of exponent 2).

2. By constructing two isotopic quasigroups (loops) U and V such that their automorphism groups are not trivial and are conjugates, it is shown that U is a AIPQ or CIPQ (AIPL or CIPL) if and only if V is a AIPQ or CIPQ (AIPL or CIPL). Explanations and procedures are given on how these CIPQs can be incorporated into the above described encryption process of Keedwell for higher security using a computer.

2 Main Results

2.1 Holomorph of AIPLs and CIPLs

Theorem 2. *Let $(L,\cdot)$ be a quasigroup(loop) with holomorph $H(L)$. $H(L)$ is an AIPQ(AIPL) if and only if*

1. *$Aut(L)$ is an abelian group,*
2. *$(\beta^{-1},\alpha,I)\in AUT(L)\ \forall\ \alpha,\beta\in Aut(L)$ and*
3. *L is a AIPQ(AIPL).*

Proof. A quasigroup(loop) is an automorphic inverse property loop(AIPL) if and only if it obeys the identity $(xy)^{\rho}=x^{\rho}y^{\rho}\ or\ (xy)^{\lambda}=x^{\lambda}y^{\lambda}$.

Using either of the definitions of an AIPQ(AIPL) above, it can be shown that $H(L)$ is a AIPQ(AIPL) if and only if $Aut(L)$ is an abelian group and $(\beta^{-1}J_{\rho},\alpha J_{\rho},J_{\rho})\in AUT(L)\ \forall\ \alpha,\beta\in Aut(L)$. L is isomorphic to a subquasigroup(subloop) of $H(L)$, so L is a AIPQ(AIPL) which implies $(J_{\rho},J_{\rho},J_{\rho})\in AUT(L)$. So, $(\beta^{-1},\alpha,I)\in AUT(L)\ \forall\ \alpha,\beta\in Aut(L)$.

Corollary 1. *Let $(L,\cdot)$ be a quasigroup(loop) with holomorph $H(L)$. $H(L)$ is a CIPQ(CIPL) if and only if*

1. *$Aut(L)$ is an abelian group,*
2. *$(\beta^{-1},\alpha,I)\in AUT(L)\ \forall\ \alpha,\beta\in Aut(L)$ and*
3. *L is a CIPQ(CIPL).*

Proof. A quasigroup (loop) is a CIPQ (CIPL) if and only if it is a WIPQ (WIPL) and an AIPQ (AIPL). L is a WIPQ (WIPL) if and only if $H(L)$ is a WIPQ(WIPL).

If $H(L)$ is a CIPQ(CIPL), then $H(L)$ is both a WIPQ(WIPL) and a AIPQ(AIPL) which implies 1., 2., and 3. of Theorem 2. Hence, L is a CIPQ(CIPL). The converse follows by just doing the reverse. □

Corollary 2. *Let $(L,\cdot)$ be a quasigroup(loop) with holomorph $H(L)$. If $H(L)$ is an AIPQ (AIPL) or CIPQ (CIPL), then $H(L)\cong L$.*

Proof. By 2. of Theorem 2, $(\beta^{-1},\alpha,I)\in AUT(L)\ \forall\ \alpha,\beta\in Aut(L)$ implies $x\beta^{-1}\cdot y\alpha = x\cdot y$ which means $\alpha=\beta=I$ by substituting $x=e$ and $y=e$. Thus, $Aut(L)=\{I\}$ and so $H(L)\cong L$.

Theorem 3. *The holomorph of a quasigroup (loop) L is a AIPQ (AIPL) or CIPQ (CIPL) if and only if $Aut(L)=\{I\}$ and L is a AIPQ(AIPL) or CIPQ (CIPL).*

Proof. This is established using Theorem 2, Corollary 1 and Corollary 2.

Theorem 4. *Let $(L,\cdot)$ be a quasigroups (loop) with holomorph $H(L)$. $H(L)$ is a CIPQ (CIPL) if and only if $Aut(L)$ is an abelian group and any of the following is true for all $x,y\in L$ and $\alpha,\beta\in Aut(L)$:*

1. $(x\beta \cdot y)x^{\rho} = y\alpha$. *2.* $x\beta \cdot yx^{\rho} = y\alpha$. *3.* $(x^{\lambda}\alpha^{-1}\beta\alpha \cdot y\alpha)\cdot x = y$.

4. $x^{\lambda}\alpha^{-1}\beta\alpha \cdot (y\alpha \cdot x) = y$.

Proof. This is achieved by simply using the four equivalent identities that define a CIPQ (CIPL):

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

Corollary 3. *Let* $(L,\cdot)$ *be a quasigroups(loop) with holomorph* $H(L)$. *If* $H(L)$ *is a CIPQ (CIPL) then the following are equivalent to each other*

1. $(\beta^{-1}J_{\rho},\alpha J_{\rho},J_{\rho}) \in AUT(L)\ \forall\ \alpha,\beta \in Aut(L)$.
2. $(\beta^{-1}J_{\lambda},\alpha J_{\lambda},J_{\lambda}) \in AUT(L)\ \forall\ \alpha,\beta \in Aut(L)$.
3. $(x\beta \cdot y)x^{\rho} = y\alpha$. 4. $x\beta \cdot yx^{\rho} = y\alpha$.
5. $(x^{\lambda}\alpha^{-1}\beta\alpha \cdot y\alpha)\cdot x = y$. 6. $x^{\lambda}\alpha^{-1}\beta\alpha \cdot (y\alpha \cdot x) = y$.

Hence, $(\beta,\alpha,I),(\alpha,\beta,I),(\beta,I,\alpha),(I,\alpha,\beta) \in AUT(L)\ \forall\ \alpha,\beta \in Aut(L)$.

Proof. The equivalence of the six conditions follows from Theorem 4 and the proof of Theorem 2. The last part is simple.

Corollary 4. *Let* $(L,\cdot)$ *be a quasigroup(loop) with holomorph* $H(L)$. *If* $H(L)$ *is a CIPQ (CIPL) then,* L *is a flexible unipotent CIPQ (flexible CIPL of exponent* 2*).*

Proof. It is observed that $J_{\rho} = J_{\lambda} = I$. Hence, the conclusion follows. □

Example 2.1 *Let* $(L,\cdot)$ *be an abelian group with* $Inn_{\rho}(L)$ *-holomorph* $H(L)$. $H(L)$ *is an abelian group.*

Proof. In an extra loop L, $Inn_{\rho}(L) = Inn_{\lambda}(L) \le Aut(L)$ is a boolean group, hence it is abeilan group. An abelian group is a commutative extra loop. A commutative extra loop is a CIPL. So by Corollary 1, $H(L)$ is a CIPL. $H(L)$ is a group since L is a group. A group is a CIPL if and only it is abelian. Thus, $H(L)$ is an abelian group.

Remark 1. *The holomorphic structure of loops such as extra loop, Bol-loop, C-loop, CC-loop and A-loop have been found to be characterized by some special types of automorphisms such as*

1. *Nuclear automorphism(in the case of Bol-,CC- and extra loops),*
2. *central automorphism(in the case of central and A-loops).* □

By Theorem 2 and Corollary 1, the holomorphic structure of AIPLs and CIPLs is characterized by commutative automorphisms. The abelian group in Example 1 is a boolean group.

2.2 A Pair of AIPLs and CIPLs

Theorem 5. *Let* $U = (L,\oplus)$ *and* $V = (L,\otimes)$ *be quasigroups such that* $Aut(U)$ *and* $Aut(V)$ *are conjugates in* $SYM(L)$ *i.e there exists a* $\psi \in SYM(L)$ *such that for any* $\gamma \in Aut(V)$, $\gamma = \psi^{-1}\alpha\psi$ *where* $\alpha \in Aut(U)$. *Then,* $H(U) \cong H(V)$ *if and only if* $x\delta \otimes y\gamma = (x\beta \oplus y)\delta \; \forall \; x, y \in L, \beta \in Aut(U)$ *and some* $\delta, \gamma \in Aut(V)$. *Hence:*

1. $\gamma \in Aut(U)$ if and only if $(I, \gamma, \delta) \in AUT(V)$.

2. if U is a loop, then; (a) $L_{e\delta} \in Aut(V)$. (b) $\beta \in Aut(V)$ if and only if $R_{e\gamma} \in Aut(V)$.

where e is the identity element in U and L_x, R_x are respectively the left and right translations mappings of $x \in V$.

3. if $\delta = I$, then $|Aut(U)| = |Aut(V)| = 3$ and so $Aut(U)$ and $Aut(V)$ are boolean groups.

4. if $\gamma = I$, then $|Aut(U)| = |Aut(V)| = 1$.

Proof.

1. Let $H(L,\oplus) = (H,\circ)$ and $H(L,\otimes) = (H,\mathrm{e})$. $H(U) \cong H(V)$ if and

only if there exists a bijection $\phi: H(U) \to H(V)$ such that $[(\alpha,x)\circ(\beta,y)]\phi = (\alpha,x)\phi \circ (\beta,y)\phi$. Define $(\alpha,x)\phi = (\psi^{-1}\alpha\psi, x\psi^{-1}\alpha\psi)\ \forall\ (\alpha,x)\in(H,\circ)$ where $\psi \in SYM(L)$.

2. $H(U) \cong H(V) \Leftrightarrow (\alpha\beta, x\beta \oplus y)\phi = (\psi^{-1}\alpha\psi, x\psi^{-1}\alpha\psi) \circ (\psi^{-1}\beta\psi, y\psi^{-1}\beta\psi) \Leftrightarrow$
$(\psi^{-1}\alpha\beta\psi, (x\beta \oplus y)\psi^{-1}\alpha\beta\psi) = (\psi^{-1}\alpha\beta\psi, x\psi^{-1}\alpha\beta\psi \otimes y\psi^{-1}\beta\psi) \Leftrightarrow$
$(x\beta \oplus y)\psi^{-1}\alpha\beta\psi = x\psi^{-1}\alpha\beta\psi \otimes y\psi^{-1}\beta\psi \Leftrightarrow x\delta \otimes y\gamma = (x\beta \oplus y)\delta$
where $\delta = \psi^{-1}\alpha\beta\psi$, $\gamma = \psi^{-1}\beta\psi$.

3. Note that, $\gamma L_{x\delta} = L_{x\beta}\delta$ and $\delta R_{y\gamma} = \beta R_y \delta\ \forall\ x, y \in L$. So, when U is a loop, $\gamma L_{e\delta} = \delta$ and $\delta R_{e\gamma} = \beta\delta$. These can easily be used to prove the remaining part of the theorem.

Theorem 6. *Let $U = (L,\oplus)$ and $V = (L,\otimes)$ be quasigroups(loops) that are isotopic under the triple of the form $(\beta^{-1}\delta, \gamma, \delta)$ for all $\beta \in Aut(U)$ and some $\delta, \gamma \in Aut(V)$ such that their automorphism groups are non-trivial and are conjugates in $SYM(L)$ i.e there exists a $\psi \in SYM(L)$ such that for any $\gamma \in Aut(V)$, $\gamma = \psi^{-1}\alpha\psi$ where $\alpha \in Aut(U)$. Then, U is a AIPQ or CIPQ(AIPL or CIPL) if and only if V is a AIPQ or CIPQ(AIPL or CIPL).*

Proof. Let U be an AIPQ or CIPQ (AIPL or CIPL), then since $H(U)$ has a subquasigroup (subloop) that is isomorphic to U and that subquasigroup (subloop) is isomorphic to a subquasigroup(subloop) of $H(V)$ which is isomorphic to V , V is a AIPQ or CIPQ(AIPL or CIPL). The proof for the converse is similar. □

2.3 Application to Cryptography

Let the Keedwell CIPQ be the quasigroup U in Theorem 5. Definitely, its automorphism group is non-trivial because as shown in Theorem 2 of Keedwell [17], for any CIPQ, the mapping $J_\rho : x \to x^\rho$ is an automorphism. This mapping will be trivial only if U is unipotent. For instance, in Example 2.1 of Keedwell [17], the CIPQ $(G,\circ)$ obtained is unipotent because it was

constructed using the cyclic group $C_5 = < c : c^5 = e >$ and defined as $a \circ b = a^3 b^2$. But in Example 2.2, the CIPQ is not unipotent as a result of using the cyclic group $C_{11} = < c : c^{11} = e >$. Thus the choice of a Keedwell CIPQ which suits our purpose in this work for a cyclic group of order n is one in which $rs = n+1$ and $r + s \neq n$. Now that we have seen a sample for the choice of U, the quasigroup V can then be obtained as shown in Theorem 5. By Theorem 6, V is a CIPQ.

After the use of the latin square of the CIPQ U as look up tables T_2 and T_3 and its long inverse cycle T_1, for a guaranteed secured period of time, U needed to be changed according to Keedwell [17] for better security. So, we can now replace U with V which is also a CIPQ. This replacement can be computerized and incorporated into the computerization of encryption process with U since V is gotten from U via isotopy. Now, according to Theorem 5, by the choice of the mappings $\alpha, \beta \in Aut(U)$ and $\psi \in SYM(L)$ to get the mappings δ, γ, a CIPQ V can be produced following Theorem 5 using the isotopism $(\beta^{-1}\delta, \gamma, \delta)$ of Theorem 6. Note that the automorphism groups of $U = (L, \oplus)$ and $V = (L, \otimes)$ are not trivial since by Theorem 3, $H(U)$ is a CIPQ if and only if $Aut(U)$ is trivial and U is a CIPQ ($H(V)$ is a CIPQ if and only if $Aut(V)$ is trivial and V is a CIPQ). And in Theorem 5 and Theorem 6, we need just U being a CIPQ and $H(U) \cong H(V)$ but not $H(U)$ and $H(V)$ being CIPQs.

2.4 Concluding Remarks

The appropriateness of a CIPQ V to replace a CIPQ U follows from the fact that they are isotopic, which is a strong relation. The production of the new look up tables T_1, T_2 and T_3 from the new CIPQ V will be done by the key distribution centre. If the multiplication of elements x, y in $U = (L, \oplus)$ was $x \oplus y$, then the new multiplication of x, y in $V = (L, \otimes)$ will be $x \otimes y = (x\delta^{-1}\beta \oplus y\gamma^{-1})\delta \; where \; \beta \in Aut(U), \delta, \gamma \in Aut(V).$

References

[1] J. O. Adeniran (2005): *On holomorphic theory of a class of left Bol loops*, Al.I.Cuza 51(1), pp. 23--28.

[2] J. O. Adeniran, Y. T. Oyebo and D. Mohammed (2011): *On certain isotopic maps of central loops*, Proyecciones Journal of Mathematics, 30(3), pp. 303-318.

[3] R. Artzy (1955): *On loops with special property*, Proc. Amer. Math. Soc. 6, pp. 448--453.

[4] R. Artzy (1959): *Crossed inverse and related loops*, Trans. Amer. Math. Soc. 91(3), pp. 480--492.

[5] R. Artzy (1959): *On Automorphic-Inverse Properties in Loops*, Proc. Amer. Math. Soc. 10(4), pp. 588--591.

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

[7] V. D. Belousov and B. F. Curkan (1969): *Crossed inverse quasigroups(CI-quasigroups)*, Izv. Vyss. Ucebn; Zaved. Matematika 82, pp. 21--27.

[8] R. H. Bruck (1944): *Contributions to the theory of loops*, Trans. Amer. Math. Soc. 55, pp. 245--354.

[9] R. H. Bruck and L. J. Paige (1956): *Loops whose inner mappings are automorphisms*, The annuals of Mathematics, 63(2), pp. 308--323.

[10] V. O. Chiboka and A. R. T. Solarin (1991): *Holomorphs of conjugacy closed loops*, Scientific Annals of Al.I.Cuza. Univ. 37(3), pp. 277--284.

[11] W. Diffie and M. E. Hellman, (1976): *New directions in cryptography*, IEE Trans. Inform. Theory IT-22, pp. 644--654.

[12] J. H. Ellis, (1970): *The possibility of secure non-secret digtal encryption*, CESG Report.

[13] J. H. Ellis (1987): *The story of non-secret digital encryption*, http://www.cesg.gov.uk/ellisdox.ps.

[14] J. H. Ellis (1987): *The history of Non-Secret Encryption*, http://www.cesg.gov.uk/about/nsecret.htm.

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

[16] T. G. Jaiyé o lá (2008): *An holomorphic study of Smarandache automorphic and cross inverse property loops*, Proceedings of the 4 th International Conference on Number Theory and Smarandache Problems, Scientia Magna Journal, 4(1), pp. 102--108.

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

[18] A. D. Keedwell and V. A. Shcherbacov (2002): *On m-inverse loops and quasigroups with a long inverse cycle*, Australas. J. Combin. 26, pp. 99—119.

[19] A. D. Keedwell and V. A. Shcherbacov (2003): *Construction and properties of* (r,s,t) *-inverse quasigroups I*, Discrete Math. 266, pp. 275—291.

[20] A. D. Keedwell and V. A. Shcherbacov (2004): *Construction and properties of* (r,s,t) *-inverse quasigroups II*, Discrete Math. 288, pp. 61—71.

[21] J. M. Osborn (1961): *Loops with the weak inverse property*, Pac. J. Math. 10,pp. 295--304.

[22] D. A. Robinson (1964): *Bol loops*, Ph.D. thesis, University of Wisconsin, Madison, Wisconsin.

[23] D. A. Robinson (1971): *Holomorphic theory of extra loops*, Publ. Math. Debrecen 18, pp. 59--64.