International J.Math. Combin. Vol.3 (2008), 28-33

A Double Cryptography
Using the Smarandache Keedwell Cross Inverse Quasigroup

Tèmítọ́pẹ́ Gbọ́láhàn Jaíyéọlá

(Department of Mathematics of Obafemi Awolowo University, Ile Ife, Nigeria.)

E-mail: tjayeola@oauife.edu.ng

Abstract: The present study further strengthens the use of the Keedwell CIPQ against attack on a system by the use of the Smarandache Keedwell CIPQ for cryptography in a similar spirit in which the cross inverse property has been used by Keedwell. This is done as follows. By constructing two S-isotopic S-quasigroups(loops) U and V such that their Smarandache automorphism groups are not trivial, it is shown that U is a SCIPQ(SCIPL) if and only if V is a SCIPQ(SCIPL). Explanations and procedures are given on how these SCIPQs can be used to double encrypt information.

Key Words: Smarandache holomorph of loops, Smarandache cross inverse property quasigroups(CIPQs), Smarandache automorphism group, cryptography.

AMS(2000): 20NO5, 08A05.

§1. Introduction

1.1 Quasigroups and Loops

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

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

have unique solutions for x and y respectively, then $(L, \cdot)$ is called a quasigroup. For each $x \in L$, the elements $x^\rho = xJ_\rho, x^\lambda = xJ_\lambda \in L$ such that $xx^\rho = e^\rho$ and $x^\lambda x = e^\lambda$ are called the right, left inverses of x respectively. 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. To every loop $(L, \cdot)$ with automorphism group $AUM(L, \cdot)$, there corresponds another loop. Let the set $H = (L, \cdot) \times AUM(L, \cdot)$. If we define '$\circ$' on H such that $(\alpha, x) \circ (\beta, y) = (\alpha\beta, x\beta \cdot y)$ for all $(\alpha, x), (\beta, y) \in H$, then $H(L, \cdot) = (H, \circ)$ is a loop as shown in Bruck [6] and is called the Holomorph of $(L, \cdot)$.

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

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

[1]Received May 6, 2008. Accepted August 18, 2008.

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

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

A loop(quasigroup) is an automorphic inverse property loop(quasigroup)[AIPL(AIPQ)] if and only if it obeys the identity

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

The set $SYM(G,\cdot) = SYM(G)$ of all bijections in a groupoid $(G,\cdot)$ forms a group called the permutation(symmetric) group of the groupoid $(G,\cdot)$. Consider $(G,\cdot)$ and $(H,\circ)$ been two distinct groupoids(quasigroups, loops). Let A, B and C be three distinct non-equal bijective mappings, that maps 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 $AUM(G,\cdot)$ called the automorphism group of $(G,\cdot)$.

As observed by Osborn [17], a loop is a WIPL and an AIPL if and only if it is a CIPL. The past efforts of Artzy [1]-[4], Belousov and Tzurkan [5] and recent studies of Keedwell [12], Keedwell and Shcherbacov [13]-[15] 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, Huthnance [7] 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. But the holomorphic structure of AIPL and a CIPL has just been revealed by Jaíyéọlá [11].

In the quest for the application of CIPQs with long inverse cycles to cryptography, Keedwell [12] constructed the following CIPQ which we shall specifically call Keedwell CIPQ.

Theorem 1.1 *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 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],[4] 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 application, it is assumed that the message to be transmitted can be represented as single element x of a quasigroup $(L, \cdot)$ and that this is enciphered by multiplying by another element y of L so that the encoded message is yx. At the receiving end, the message is deciphered by multiplying by the right inverse y^ρ of y. If a left(right) inverse quasigroup is used and the left(right) inverse of x is x^λ (x^ρ), then the left(right) inverse of x^λ (x^ρ) is necessarily x. But if a CIPQ is used, this is not necessary the situation. This fact makes an attack on the system more difficult in the case of CIPQs.

1.2 Smarandache Quasigroups and Loops

The study of Smarandache loops was initiated by W. B. Vasantha Kandasamy in 2002. In her book [19], she defined a Smarandache loop(S-loop) as a loop with at least a subloop which forms a subgroup under the binary operation of the loop. In [9], the present author defined a Smarandache quasigroup(S-quasigroup) to be a quasigroup with at least a non-trivial associative subquasigroup called a Smarandache subsemigroup (S-subsemigroup). Examples of Smarandache quasigroups are given in Muktibodh [16]. In her book, she introduced over 75 Smarandache concepts on loops. In her first paper [20], on the study of Smarandache notions in algebraic structures, she introduced Smarandachely left(right) alternative loops, Bol loops, Moufang loops, and Bruck loops. In [8], the present author introduced Smarandachely inverse property loops(IPL) and weak inverse property loops(WIPL).

A quasigroup(loop) is called a *Smarandache certain quasigroup(loop)* if it has at least a non-trivial subquasigroup(subloop) with the certain property and the latter is referred to as the *Smarandache certain subquasigroup(subloop)*. For example, a loop is called a *Smarandache CIPL(SCIPL)* if it has at least a non-trivial subloop that is a CIPL and the latter is referred to as the *Smarandache CIP-subloop*. By an *initial S-quasigroup* L with an initial S-subquasigroup L', we mean L and L' are pure quasigroups, i.e. they do not obey a certain property(not of any variety).

If L is a S-groupoid with a S-subsemigroup H, then the set $SSYM(L, \cdot) = SSYM(L)$ of all bijections A in L such that $A : H \to H$ forms a group called the *Smarandache permutation(symmetric) group of the S-groupoid*. In fact, $SSYM(L) \leqslant SYM(L)$.

Definition 1.1 *Let $(L, \cdot)$ and $(G, \circ)$ be two distinct groupoids that are isotopic under a triple (U, V, W). Now, if $(L, \cdot)$ and $(G, \circ)$ are S-groupoids with S-subsemigroups L' and G' respectively such that $A : L' \to G'$, where $A \in \{U, V, W\}$, then the isotopism $(U, V, W) : (L, \cdot) \to (G, \circ)$ is called a Smarandache isotopism(S-isotopism).*

Thus, if $U = V = W$, then U is called a Smarandache isomorphism. Hence we write $(L, \cdot) \gtrsim (G, \circ)$.

But if $(L, \cdot) = (G, \circ)$, then the autotopism (U, V, W) is called a Smarandache autotopism (S-autotopism) and they form a group $SAUT(L, \cdot)$ which will be called the Smarandache autotopism group of $(L, \cdot)$. Observe that $SAUT(L, \cdot) \leqslant AUT(L, \cdot)$. Furthermore, if $U = V = W$, then U is called a Smarandache automorphism of $(L, \cdot)$. Such Smarandache permutations form a group

$SAUM(L,\cdot)$ called the Smarandache automorphism group(SAG) of $(L,\cdot)$.

Now, set $H_S = (L,\cdot) \times SAUM(L,\cdot)$. If we define '$\circ$' on H_S such that $(\alpha,x)\circ(\beta,y) = (\alpha\beta, x\beta\cdot y)$ for all $(\alpha,x),(\beta,y) \in H_S$, then $H_S(L,\cdot) = (H_S,\circ)$ is a S-quasigroup(S-loop) with S-subgroup $(H',\circ)$ where $H' = L' \times SAUM(L)$ and thus will be called the *Smarandache Holomorph(SH)* of $(L,\cdot)$.

The aim of the present study is to further strengthen the use of the Keedwell CIPQ against attack on a system by the use of the Smarandache Keedwell CIPQ for cryptography in a similar spirit in which the cross inverse property has been used by Keedwell. This is done as follows. By constructing two S-isotopic S-quasigroups(loops) U and V such that their Smarandache automorphism groups are not trivial, it is shown that U is a SCIPQ(SCIPL) if and only if V is a SCIPQ(SCIPL). Explanations and procedures are given on how these SCIPQs can be used to double encrypt information.

§2. Preliminary Results

Definition 2.1(Smarandachely Keedwell CIPQ) *Let Q be an initial S-quasigroup with an initial S-subquasigroup P. Q is called a Smarandachely Keedwell CIPQ(SKCIPQ) if P is isomorphic to the Keedwell CIPQ, say under a mapping ϕ.*

The following results that have recently been established are of paramount importance to prove the main result in this paper.

Theorem 2.1(Jaíyéọlá [10]) *Let $U = (L,\oplus)$ and $V = (L,\otimes)$ be initial S-quasigroups such that $SAUM(U)$ and $SAUM(V)$ are conjugates in $SSYM(L)$ i.e there exists a $\psi \in SSYM(L)$ such that for any $\gamma \in SAUM(V)$, $\gamma = \psi^{-1}\alpha\psi$ where $\alpha \in SAUM(U)$. Then, $H_S(U) \gtrsim H_S(V)$ if and only if $x\delta \otimes y\gamma = (x\beta \oplus y)\delta \ \forall\ x,y \in L,\ \beta \in SAUM(U)$ and some $\delta,\gamma \in SAUM(V)$.*

Theorem 2.2(Jaíyéọlá [11]) *The holomorph $H(L)$ of a quasigroup(loop) L is a Smarandache CIPQ(CIPL) if and only if $SAUM(L) = \{I\}$ and L is a Smarandache CIPQ(CIPL).*

§3. Main Result with Applications

3.1 Main result

Theorem 3.1 *Let $U = (L,\oplus)$ and $V = (L,\otimes)$ be initial S-quasigroups(S-loops) that are S-isotopic under the triple of the form $(\delta^{-1}\beta,\gamma^{-1},\delta^{-1})$ for all $\beta \in SAUM(U)$ and some $\delta,\gamma \in SAUM(V)$ such that their Smarandache automorphism groups are non-trivial and are conjugates in $SSYM(L)$ i.e there exists a $\psi \in SSYM(L)$ such that for any $\gamma \in SAUM(V)$, $\gamma = \psi^{-1}\alpha\psi$ where $\alpha \in SAUM(U)$. Then, U is a SCIPQ(SCIPL) if and only if V is a SCIPQ(SCIPL).*

Proof Following Theorem 2.1, $H_S(U) \gtrsim H_S(V)$. Also, by Theorem 2.2, $H_S(U)(H_S(V))$ is a SCIPQ (SCIPL) if and only if $SAUM(U) = \{I\}(SAUM(V) = \{I\})$ and $U(V)$ is a

SCIPQ(SCIPL).

Now let U be an SCIPQ(SCIPL), then since $H_S(U)$ has a subquasigroup(subloop) that is isomorphic to a S-CIP-subquasigroup(subloop) of U and that subquasigroup (subloop) is isomorphic to a S-subquasigroup(subloop) of $H_S(V)$ which is isomorphic to a S-subquasigroup (subloop) of V, V is a SCIPQ(SCIPL). The proof for the converse is similar. □

3.2 Application To Cryptography

Let the Smarandache Keedwell CIPQ be the SCIPQ U in Theorem 3.1. Definitely, its Smarandache automorphism group is non-trivial because as shown in Theorem 2.1 of Keedwell [12]. For any CIPQ, the mapping $J_\rho \ : \ x \to x^\rho$ is an automorphism. This mapping will be trivial only if the S-CIP-subquasigroup of U is unipotent. For instance, in Example 2.1 of Keedwell [12], the CIPQ $(G, \circ)$ obtained is unipotent because it was constructed using the cyclic group $C_5 =< c : \ c^5 = e >$ and defined as $a \circ b = a^3b^2$. But in Example 2.2, the CIPQ gotten is not unipotent as a result of using the cyclic group $C_{11} =< c : \ c^{11} = e >$. Thus, the choice of a Smarandache 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 initial S-quasigroup V can then be obtained as shown in Theorem 3.1. By Theorem 3.1, V is a SCIPQ.

Now, according to Theorem 2.1, by the choice of the mappings $\alpha, \beta \in SAUM(U)$ and $\psi \in SSYM(L)$ to get the mappings δ, γ, a SCIPQ V can be produced following Theorem 3.1. So, the secret keys for the systems are $\{\alpha, \beta, \psi, \phi\} \equiv \{\delta, \gamma, \phi\}$. Thus whenever a set of information or messages is to be transmitted, the sender will enciphere in the Smarandache Keedwell CIPQ by using specifically the S-CIP-subquasigroup in it(as described earlier on in the introduction) and then enciphere again with $\{\alpha, \beta, \psi, \phi\} \equiv \{\delta, \gamma, \phi\}$ to get a SCIPQ V which is the set of encoded messages. At the receiving end, the message V is deciphered by using an inverse isotopism(i.e inverse key of $\{\alpha, \beta, \psi\} \equiv \{\delta, \gamma\}$) to get U and then deciphere again(as described earlier on in the introduction) to get the messages. The secret key can be changed over time. The method described above is a double encryption and its a double protection. It protects each piece of information(element of the quasigroup) and protects the combined information(the quasigroup as a whole). Its like putting on a pair of socks and shoes or putting on under wears and clothes, the body gets better protection. An added advantage of the use of Smarandache Keedwell CIPQ over Keedwell CIPQ in double encryption is that the since the S-CIP-subquasigroups of the Smarandache Keedwell CIPQ in use could be more than one, then, the S-CIP-subquasigroups can be replaced overtime.

References

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

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

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

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

[5] V. D. Belousov , Crossed inverse quasigroups(CI-quasigroups), *Izv. Vyss. Ucebn; Zaved. Matematika* 82(1969), 21-27.

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

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

[8] T. G. Jaíyéọlá, An holomorphic study of the Smarandache concept in loops, *Scientia Magna Journal*, 2, 1(2006), 1-8.

[9] T. G. Jaíyéọlá, Parastrophic invariance of Smarandache quasigroups, *Scientia Magna Journal*, 2, 3(2006), 48-53.

[10] T. G. Jaíyéọlá , A Pair Of Smarandachely Isotopic Quasigroups And Loops Of The Same Variety, *International J.Math. Combina.*, Vol.2,2008, 36-44.

[11] T. G. Jaíyéọlá, 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*, Vol. 4, No. 1(2008), 102-108.

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

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

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

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

[16] A. S. Muktibodh, Smarandache Quasigroups, *Scientia Magna Journal*, 2, 1(2006), 13-19.

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

[18] Y. T. Oyebo and O. J. Adeniran, On the holomorph of central loops, Pre-print.

[19] W. B. Vasantha Kandasamy , *Smarandache Loops*, Department of Mathematics, Indian Institute of Technology, Madras, India, 2002, 128pp.

[20] W. B. Vasantha Kandasamy, Smarandache Loops, *Smarandache notions journal*, 13(2002), 252-258.