Journal of mathematics and computer science 10 (2014), 113-118

Contents list available at JMCS

Journal of Mathematics and Computer Science

Journal Homepage: www.tjmcs.com

An Application of Co-Medial Algebras with Quasigroup Operations on Cryptology

Amir Ehsani

Department of Mathematics, College of Polymer,

Mahshahr Branch, Islamic Azad University, Mahshahr, Iran.

a.ehsani@mhriau.ac.ir

Article history:
Received February 2014
Accepted March 2014
Available online March 2014

Abstract

A modification of Markovski quasigroup based crypto-algorytm has been presented. This modification is based on the pair of co-medial quasigroup operations, which we show that they are orthogonal quasigroup operations.

Keywords: co-medial pair of operations, quasigroup operation, orthogonal operations, cryptology, cipher-text, enciphering.

1. Introduction

Two main elementary methods of ciphering the information are known.

(i). Symbols in a plaintext (or in its piece (its bit)) are permuted by some law. One of the first known ciphers of such kind is cipher ”Scital” (Sparta, 2500 years ago).

(ii). All symbols in a fixed alphabet are changed by a law on other letters of this alphabet. One of the first ciphers of such kind was Cezar’s cipher ($x \to x + 3$ for any letter of Latin alphabet, forexample $a \to d$, $b \to e$ and so on).

In many contemporary ciphers (DES, old Russian GOST, Blowfish [13, 2]) the methods (i) and(ii) are used with some modifications. Therefore, permutations and substitutions are main elementarycryptographical procedures (see for example [8]).

What does the use of quasigroups in cryptography give us? It gives the same permutations andsubstitutions but easy generated, requiring not very big volume of a device memory, acting ”locally”on only one block of a plain-text.

Stream-ciphers based on quasigroups and their parastrophes were discovered in the end of theXX-th century [10, 11].

2. Preliminaries

2.1 Definition

A binary algebra $\boldsymbol{A}$ is an ordered pair *(A, F)*, where A is a nonempty set and F is a family of binary operations$f: A^2 \to A$. The set A is called the universe (or underlying set) of the algebra $\boldsymbol{A}$= *(A, F)*.

If F is finite, say$F = \{f_1, \dots, f_k\}$, we often write $(A, f_1, \dots, f_k)$ for *(A,F)*. The algebra $\boldsymbol{A}$ is a groupoid if it has only one binary operation.

2.2 Definition

A binary quasigroup is a groupoid *(A,f)* such that for any $a, b \in A$ there are unique solutions *x,y* to the following equations:

$$f(a,x)=b,\ f(y,a)=b.$$

If *(A,f)* be a quasigroup then we say that *f* is a quasigroup operation.A loop is a quasigroup with unit (*e*) such that $f(e,x)=f(x,e)=x$. Groups are associative quasigroups, i.e. they satisfy: $f(f(x,y),z)=f(x,f(y,z))$ and they necessarily contain a unit.

From the above definition of a quasigroup follows that any binary quasigroup *(A, f)* defines else 5 binary quasigroups namely$(A, {}^{(13)}f)$, $(A, {}^{(23)}f)$, $(A, {}^{(12)}f)$, $(A, {}^{(123)}f)$, $(A, {}^{(132)}f)$, so-called parastrophes of quasigroup *(A, f)*. For the binary quasigroup *(A, f)* the following identities are fulfilled:

$$f\left({}^{(13)}f(x,y), y\right) = x,\ {}^{(13)}f(f(x,y), y) = x,$$
$$f\left(x, {}^{(23)}f(x,y)\right) = y,\ {}^{(23)}f\left(x, f(x,y)\right) = y\ .$$

It was propose usingthe above quasigroup property to construct the following stream cipher [9].

2.3 Algorithm

Let A be a non-empty finite alphabet, k be a natural number, $u_i, v_i \in Q$, $i \in \{1,...,k\}$. Define a quasigroup *(A, f)*. It is clear that the quasigroup $(A, {}^{(23)}f)$ is defined in a unique way.

Take a fixed element l $(l \in A)$, which is called a leader.

Let $u_1u_2...u_k$ be a k-tuple of letters from A.

It is proposed the following ciphering procedure

$v_1 = f(l,u_1)$,

$v_i = f(v_{i-1}, u_i)$, $i = 2, ..., k$.

Therefore we obtain the following cipher-text $v_1v_2 \dots v_k$.

The deciphering algorithm is constructed in the following way:

$u_1 = {}^{(23)}f(l, v_1)$, $u_i = {}^{(23)}f(v_{i-1}, v_i)$,$i = 2, ..., k$.

Indeed ${}^{(23)}f(v_{i-1}, v_i) = {}^{(23)}f(v_{i-1}, f(v_{i-1}, u_i)) = u_i$.

Notice, the equality $f = {}^{(23)}f$ is fulfilled if and only if $f(x, f(x, y)) = y$ for all $x, y \in A$.

2.4 Definition

Binary pair of groupoids *(A, f)* and *(A, g)* are called orthogonal, if for any fixed $a, b \in A$ the following equations have unique solution:

$$f(x, y) = a, \quad g(x, y) = b.$$

2.5 Definition

A binary algebra $\boldsymbol{A}= (A, F)$ is called medial (entropic or abelian) if it satisfies the following identity of mediality for every binary $, g \in F$:

$$g\big(f(x,y), f(u,v)\big) = f\big(g(x,u), g(y,v)\big) \qquad (1)$$

The binary operation f is called idempotent if $f(x, x)=x$, for every $x \in A$. The algebra $\boldsymbol{A}=(A,F)$ is called idempotent, if everyoperation $f \in F$ is idempotent. An idempotent medial algebra isa mode [16]. Notethat a groupoid is medial if and only if it satisfies the identity ofmediality:$xy.uv = xu.yv$.

Let g and f be binary operations on the set A. We say that the pair ofoperations (f,g) is medial (or entropic), if the identity (1) holds in the algebra $\boldsymbol{A}=(A,f,g)$ [3, 5].

2.6 Definition

The pair of operations (f, g) is called co-medial, if the following identity holds in the algebra $\boldsymbol{A}= (A, f, g)$:

$$g\big(f(x,y), f(u,v)\big) = g\big(f(x,u), f(y,v)\big) \qquad (2)$$

An algebra $\boldsymbol{A}= (A, F)$ is called co-medial if every pair of operations $f, g \in F$ is co-medial [4].

3. Main Results

3.1 Definition

A binary quasigroup (A,f) is linear over a group if $f(x, y) = \varphi\, x + a + \omega\, y$, where $(A,+)$ is a group, φ and ω are automorphisms of the group $(A,+)$ and $a \in A$ is a fixed element.

A quasigroup linear over an Abelian group is also called a T-quasigroup.

3.2 Theorem

Let (A, F) be binaryco-medial algebra with quasigroup operations; then there exists a binary operation "+" under which Aforms an abelian group, and for every operation $f_i \in F$ and elements $x,y \in A$ wehave:

$$f_i(x,y)=\varphi_i(x)+\omega_i(y)+c_i,$$

where c_i is a fixed element of A, φ_i and ω_i are automorphisms of the group $(A,+)$,such that: $\varphi_i\omega_j = \omega_j\varphi_i$.

Proof. See [6].

3.3 Theorem

A T-quasigroup $(A, \cdot)$ of the form $x \cdot y = \alpha x + \beta y + c$ and a T-quasigroup $(A, \circ)$ of the form $x \circ y = \gamma x + \delta y + d$, both defined over a group $(A,+)$, are orthogonal if and only if the map $\alpha^{-1}\beta - \gamma^{-1}\delta$ is an automorphism of the group $(A,+)$.

Proof. See [14].

3.4 Corollary

Every pair of operations in the binary co-medial algebra with quasigroup operations is an orthogonal pair of operations.

Proof. By using Theorem 3.2 and Theorem 3.3 the proof is straightforward.

If the set A is finite, then any pair of orthogonal binary operations (A, f), (A, g), defines a permutation of the set A^2 and vice versa. Therefore if $|A|=k$, then there exist $(k^2)!$pairs of orthogonal groupoids defined on the set A.

Here we propose to use a system of orthogonal binary groupoids as additional procedure in order to construct almost-stream cipher. Such systems have more uniform distribution of elements of base set and therefore such systems may be more preferable in protection against statistical cryptanalytic attacks.

3.5 Algorithm

Let A be a non-empty finite alphabet and$x_1, x_2,\dots,x_t$ be a plain-text. Take the binary co-medial algebra (A, F) with quasigroup operations, and a pair operation f, $g\in F$. This orthogonal pair of operations defines apermutation E of the set A^2. We propose the following enciphering procedure.

• **Step 1:**$(y_1,y_2)=F^l(x_1,x_2)$, where $l \geq 1$, l is a natural number;l is vary from one enciphering roundtoother. If $t<2$, then we can add to plaintext some"neutral" symbols.

• **Steps ≥ 2:**It is possible to use Feistel schema [7, 12]. For example, we can dothe following enciphering procedure $(z_1,z_2)= F^s(y_2, y_3)$, and so on.

The deciphering algorithm is based on the fact that orthogonal system of binary operations (f, g) hasa unique solution for any tuple of elements a_1,a_2.

The above algorithm is sufficiently safe relative to chosen ciphertext and plaintext attack since the key is a non-periodic sequence of applications of permutation E, i.e. sequence of powers of permutation E. Therefore any permutation of the group $\langle E\rangle$can be used by ciphering information using the above algorithm.

We propose to use Algorithm 2.3 and Algorithm 3.5 simultaneously.

3.6 Algorithm

Suppose that we have a plaintext $x_1,\dots,x_t$, $t \geq 2$.

1. Divide plaintext on pairs.

2. We apply to any pair of plaintext binary permutation $F^l(x_1, x_2)=(y_1,y_2)$.

3. To a pair(y_1, y_2) we apply Algorithm 2.3$g(y_1, y_2) =(z_1, z_2)$.

4. We apply to the pair(z_1, z_2)binary permutation $F^s(z_1, z_2) = (t_1, t_2)$.

Deciphering algorithm is clear.

3.7 Definition

Let $(A, \cdot)$ be a groupoid and let a be a fixed element in A. Translation maps L_a(left) and R_a (right) are defined by the following equalities $L_a x = a \cdot x$, $(R_a x = x \cdot a)$ for all $x \in A$. For quasigroups it is possible to define a third kind of translation, namely, middle translations. If P_a isa middle translation of a quasigroup $(A, \cdot)$, then $x \cdot P_a x = a$, for all $x \in A$ [1].

It is well known that in a quasigroup $(A, \cdot)$ any left and right translation is a bijective map of theset A [11, 15].

Below we denote the action of the left (right, middle) translation in the power a of a binaryquasigroup (A, g) on the element u_1 by the symbol ${}_gT_{l_1}^{a}(u_1)$. And so on.

3.8Algorithm

Enciphering.

Initially we have the plaintext u_1,u_2.

${}_gT_{l_1}^{a}(u_1)=v_1$

${}_fT_{l_2}^{b}(u_2)=v_2$

$E_l^c(v_1, v_2)=(v_1', v_2')$

And so on. We obtain ciphertext (v_1', v_2').

Deciphering.

Initially we have ciphertext (v_1', v_2').

$$E_l^{-c}(v_1', v_2') = (v_1, v_2)$$

$${}_gT_{l_1}^{-a}(v_1) = u_1$$

$${}_fT_{l_2}^{-b}(v_2) = u_2$$

We obtain plaintext u_1, u_2.

In the Algorithm 3.8 the elements a, b, c should be vary in order to protectthis algorithm against chosen plain-text and chosen cipher-text attack.Algorithm 3.8 allows obtainingalmost "natural" stream cipher, i.e. stream cipher that encodes apair of elements of a plaintext on any step.

ACKNOWLEDGEMENTS

Thisarticleis a part of theachievements of theresearch projectentitled"On Applications of Quasigroups in Cryptology". Theauthorthanks Mahshahr Branch ofIslamic Azad University, forfinancial supportofthis research project.

References

[1] V.D. Belousov, The group associated with a quasigroup, Mat. Issled. 4(3) (1969) 21 – 39.

[6] V. Domashev, V. Popov, D. Pravikov, I. Prokof'ev, and A. Shcherbakov, Programming of algorithms of defense of information, Nolidge, Moscow, 2000.

[2] A. Ehsani, The Generalized entropic property for the pair of operations, Journal of ContemporaryMathematical Analysis 46(1) (2011) 29-34.

[3] A. Ehsani, On Regular Co-medial Algebras, J. Mathematics Research 4(2) (2012) 101-109.

[4] A. Ehsani, On Medial-like Functional Equations, Mathematical Problems of ComputerScience 38 (2012) 53-55.

[5] A. Ehsani, Yu. M. Movsisyan, Linear Representation of Medial-like Algebras, Communications in Algebra 41(9) (2013) 3429-3444.

[7] H.Feistel, Cryptography and computer privacy, Scientific American 228(5) (1973) 15–23.

[8] S. H. Kamali, M. Hedayati, R. Shakerian and S. Ghasempour, Using Identity-Based Secret Public Keys Cryptography for Heuristic Security Analyses in Grid Computing, The Journal of Mathematics and Computer Science 3(4) (2011) 357-375.

[9] S. Markovski, D. Gligoroski, and S. Andova, Using quasigroups for one-one secure encoding, In *Proc.* VIII Conf. Logic and Computer Science "LIRA97", Novi Sad (1997) 157–167.

[10] S. Markovski, D. Gligoroski, and V. Bakeva, Quasigroup string processing: Part 1, Contributions, Sec. Math. Tech. Sci., MANU, XX(1-2) (1999) 13–28.

[11] S. Markovski and V. Kusakatov, Quasigroup string processing:Part 2, Contributions, Sec. Math.Tech. Sci., MANU, XXI(1-2) (2000) 15–32.

[12] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, 1997.

[13] N.A. Moldovyan, Problems and methods of cryptology,S.Petersburg University Press, S.Petersburg, 1998.
[14]G. L. Mullen, V. A. Shcherbacov, Onorthogonality of binary operations and squares, BULETINUL ACADEMIEI DE STIINTE A REPUBLICII MOLDOVA. MATEMATICA 2(48) (2005) 3–42.
[15] H.O. Pflugfelder, Quasigroups and Loops: Introduction,HeldermannVerlag, Berlin, 1990.
[16] A. Romanowska, J. D. H. Smith, Modes, World Scientific, River Edge, New Jersey, 2002.