Classification of Quasigroup-structures with respect to their Cryptographic Properties

Quratul-ain Mahesar* and Volker Sorge†
*School of Computer Science, University of Birmingham
Edgbaston, Birmingham
B15 2TT, United Kingdom
{Q.Mahesar|V.Sorge}@cs.bham.ac.uk

1 Introduction

Computationally simple but cryptographically strong ciphers play an important role for efficient Computer Security tasks. It is suggested in (Knapskog, 2008) that there is a need for simple cryptographic primitives to implement security in an environment with end users connected with terminals having limited storage and processing power. Constructing ciphers using the algebraic structures of Quasigroup leads to particular simple yet efficient ciphers. Quasigroups are structures very similar to groups with the primary difference that they are in general not associative. Stream ciphers can be constructed from quasigroups using a permutation based scrambling technique (Maruti, 2006). For security considerations the main goal of the scrambler is to maximize the entropy of the produced output. Depending on the quasigroup used the cryptographic strength of the cipher can vary significantly. In order to find strong ciphers quasigroups have to be generated and the resulting ciphers are tested with respect to standard statistical methods. Quasigroups are then categorised as cryptographically strong or weak according to the outcome of these tests.

In our research we aim to tackle the problem from a different angle. We consider quasigroups that have already been categorised with respect to their cryptographic properties. We then automatically classify these quasigroups with respect to their algebraic properties, with the goal to identify properties common to cryptographically strong quasigroups in order to use them for a goal directed construction of quasigroups for strong ciphers. Our work builds on previous work (Sorge et al., 2008) that was concerned with the generation of classification theorems in quasigroup theory. A bootstrapping algorithm was designed to successively refine a classification of quasigroups of a given finite order by constructing algebraic invariants using machine learning techniques, until a full classification into non-equivalent classes was achieved. The procedure incorporated a set of diverse reasoning techniques, including first order resolution theorem proving, model generation, satisfiability solving and computer algebra methods, and was successfully applied to produce a number of novel classification theorems for loops and quasigroups with respect to isomorphism and isotopism.

2 Quasigroup Ciphers

Following (Pflugfelder, 1990), a quasigroup Q can be defined as a group of elements $(1, 2, 3...n)$ along with a multiplication operator '$*$', such that for every element $x, y \in Q$, there exists a unique solution $z \in Q$ such that the following two conditions hold (1) $x * a = z$, and (2) $y * b = z$, where the elements a, b and z belong to the Quasigroup Q. These conditions ensure that a quasigroup can also be viewed as a Latin square; that is, each element of Q occurs exactly once in each row and each column of the multiplication table defining '$*$'. Conditions (1) and (2) essentially postulate the existence of unique left and right divisors for each element in Q. This gives rise to an explicit definition of left and right division operations:

Let $(Q, \circ)$ be a Quasigroup, then two operations $\backslash$ and $/$ on Q can be defined as:

(3) $x * (x\backslash y) = y$ and $x\backslash(x * y) = y$ (4) $(y/x) * x = y$ and $(y * x)/x = y$

The following is an example of a Quasigroup Q of order 4 given in terms of multiplication tables for all three operations:

*	1	2	3	4
1	2	3	1	4
2	4	1	3	2
3	3	4	2	1
4	1	2	4	3

\	1	2	3	4
1	3	1	2	4
2	2	4	3	1
3	4	3	1	2
4	1	2	4	3

/	1	2	3	4
1	4	2	1	3
2	1	4	3	2
3	3	1	2	4
4	2	3	4	3

Quasigroup Encryption

We can now define a quasigroup cipher in terms of encryption and decryption function following (Dimitrova and Markovski, 2004). Let $(Q, *, \backslash, /)$ be a Quasigroup and $a_1, a_2, a_3, ..., a_n \in Q$. We define the encryption function E with respect to the key $a \in Q$ as

$$E_a(a_1, a_2, a_3, ..., a_n) = b_1, b_2, b_3, ...b_n$$

where $b_1, b_2, b_3, ..., b_n \in Q$ are computed by (i) $b_1 = a * a_1$, and (ii) $b_i = b_{i-1} * a_i$, for $i = 2, \ldots, n$.

Quasigroup Decryption

The decryption process is similar to the encryption but the left division operation '$\backslash$' is used as operation. The decryption function D is then define as:

$$D_a(a_1, a_2, a_3, ...a_n) = e_1, e_2, e_3...e_n$$

where the original plaintext is computed by (i) $e_1 = a\backslash a_1$, and (ii) $e_i = a_{i-1}\backslash a_i$, for $i = 2, \ldots, n$.

3 Examining Cryptographic Properties

The cryptographic properties of quasigroup ciphers are primarily determined by subjecting the resulting pseudo-random sequences to statistical tests for randomness. In (Markovski et al., 2004) eight bespoke statistical tests are performed by random walk on torus examining the properties of strings obtained from specific quasigroup transformations. This can provide an empirical classification of Quasigroups with respect to their cryptographic hardness. However, exhaustive classification of quasigroups is prohibitive even for small sizes of quasigroups due to the sheer number of different structures to consider. For example, there are over $2 \cdot 10^{30}$ different isomorphism classes of quasigroups of order 10 (McKay et al., 2004). Moreover, (Markovski et al., 2004) shows that quasigroups belonging to the same isomorphism class can behave differently with respect to their cryptopgraphic properties and therefore considering quasigroups up to isomorphism would not be enough. In (Koscielny, 2002) a system for generating quasigroups for cryptographic applications is presented giving a set of procedures implemented in Maple 7. It is also stated that practical ciphers should be constructed using quasigroups of order between 32 and 256. Since the generation of structures of this size is non-trivial, the construction of larger quasigroups is done via composition of smaller ones and cryptographic properties are lifted from the smaller to larger structures. Nevertheless the final cryptographic hardness can only be ensured using randomness test.

The goal of our work is to use these results as a bases on which to start an algebraic classification process, establishing properties that discriminate small quasigroups with good cryptographic properties from those with poor cryptographic behaviour using the automated bootstrapping approach from (Sorge et al., 2008). Once invariants of this nature have been established they have to be examined with respect to their behaviour under compositions of quasigroups. After appropriate relationships between algebraic and cryptographic properties can be established they can subsequently be exploited to aid the modular construction of larger quasigroups for more effective ciphers.

References

V. Dimitrova and J. Markovski. On quasigroup sequence random generator. *Proceedings of the 1st Balkan Conference in Informatics*, pages 393–401, 2004.

S. J. Knapskog. New cryptographic primitives (plenary lecture). *7th Computer Information Systems and Industrial Management applications*, 2008.

C. Koscielny. Generating quasigroups for cryptographic applications. *Int. J. Appl. Math. Comput. Sci.*, 12(4):559–569, 2002.

S. Markovski, D. Gligoroski, and J. Markovski. Classification of quasigroups by random walk on torus. *IJCAR workshop on Computer Supported mathematical Theory Development*, 2004.

Satti Maruti. A quasigroup based cryptographic system. *CoRR*, 2006.

Brendan D. McKay, Alison Meynert, and Wendy Myrvold. Small Latin Squares, Quasigroups and Loops. Preprint, 2004.

Hala O. Pflugfelder. *Quasigroups and Loops: Introduction*, volume 7 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, Germany, 1990.

V. Sorge, S. Colton, R. McCasland, and A. Meier. Classification results in quasigroup and loop theory via a combination of automated reasoning tools. *Comment.Math.Univ.Carolinae*, 49(2):319–339, 2008.