

1106-VJ-2092

**Carl Edward Looney\*** (clooney@uta.edu), 1509 Harwell dr #1215, Arlington, TX 76011.

*Non-Associative Algebraic Structures and Cryptology.*

Associative algebraic structures have been used for constructions of almost all known enciphering systems. However, as shown by Keedwell in 1960's, there exists the possibility of using algebraic structures such as quasigroups, which are not associative, in coding theory, especially in cryptology. In particular m-inverse quasigroups with long inverse cycles have been proven beneficial in coding theory. M-inverse quasigroups  $(Q,*)$  have the following property: there exists a permutation  $J$  such that for all  $a, b \in Q$ ,  $J^m(a*b)*J^{m+1}(a) = J^m(b)$ . Keedwell and Scherbacov have shown the existence of m-inverse loops and quasigroups of some specific small orders. In this talk we discuss the construction of m-inverse quasigroups of orders not shown by Keedwell and Scherbacov. We also show how the method used to construct such algebraic structures can be used to show the nonexistence of such structures for particular orders. (Received September 16, 2014)