

1011-17-168 **Kristen Meyer*** (kristi@iastate.edu), 396 Carver Hall, Ames, IA 50011. *Message Authentication Codes and Quasigroups.*

Message Authentication Codes, or MACs, are commonly used in cryptography to ensure that a message has not been changed in transit. This talk will describe a new MAC (called QMAC) which relies on the nonassociativity of quasigroups. In order to ensure that QMAC is secure, highly nonassociative quasigroups of large order must be used. I will also discuss methods for creating such quasigroups and measuring their nonassociativity. (Received August 25, 2005)