Research Week Proposal

Title – Twisted Hermitian Codes in the McEliece Cryptosystem

Program of Study – Mathematics/Computer Science

Presentation Type –PowerPoint

Mentor(s) and Mentor Email – N/A

Student name(s) and email(s) – Bethany Matsick (blmatsick@liberty.edu)

Category –Applied

Abstract: In 1978, Robert McEliece introduced a public key cryptosystem based on the difficult problem of decoding a random linear code. Due to its large key size, the McEliece cryptosystem has yet to see widespread use. However, since the McEliece cryptosystem does not appear to be susceptible to Shor's (quantum) algorithm as is the case with the widely used RSA and elliptic curve cryptosystems, it is now being considered as a candidate for post-quantum cryptography. To ensure that a code appears random in this system, we desire a code with a Schur square that behaves like that of a random linear code, meaning the dimension of its Schur square is equal to that of a random linear code of the same dimension. Because most classical families of codes fall far short of this ideal, we develop a family of "twisted" Hermitian codes with a Schur square dimension comparable to that of random linear code. We show that, when constructed properly, these "twisted" Hermitian codes not only achieve a high dimensional Schur square but also maintain a reasonable data transfer rate. The twisted construction is a variant of that considered by Peter Beelen, Martin Bossert, Sven Puchinger, and Johan Rosenkilde. This is joint work with Austin Allen, Keller Blackwell, Olivia Fiol, Rutuja Kshirsagar, and Zoe Nelson, supervised by Gretchen Matthews.