1145-94-2120 **Austin P. Allen*** (apallen@andrew.cmu.edu) and **Keller L. Blackwell** (kellerb@mail.usf.edu). *Distinguisher-attack resistance and decoding of twisted Hermitian codes.*

The McEliece public-key cryptosystem is a code-based scheme that is thought to achieve post-quantum security through the NP-hardness of decoding a random linear code; however, its reliance on binary Goppa codes forces impractical key sizes and relatively low data rates. Implementation of the McEliece PKC with more structured codes can improve feasibility, but care must be taken to avoid incurring vulnerabilities under cryptanalysis. For instance, while Reed-Solomon codes are highly structured, they have a small dimensional Schur square that makes them unsuitable for the McEliece PKC. Recently, twisted Reed-Solomon codes were introduced to increase the dimension of the Schur square. In this talk, we introduce a new variant of Hermitian codes, called twisted Hermitian codes. We identify a subfamily of these new codes that achieve large Schur square dimension and show their resistance to distinguisher attacks. Furthermore, we demonstrate a decoding algorithm for twisted Hermitian codes. This is joint work with Olivia Fiol, Rutuja Kshirsagar, Bethany Matsick, and Zoe Nelson, supervised by Gretchen Matthews. (Received September 25, 2018)