Twisted Hermitian codes in the McEliece cryptosystem

Gretchen L. Matthews

Virginia Tech

gmatthews@vt.edu

Abstract. We define twisted Hermitian codes based on one-point Hermitian codes and strongly inspired by the twisted Reed-Solomon codes described by Beelen, Puchinger, and Nielsen. We demonstrate that these new codes can have high-dimensional Schur squares, and we identify a subfamily of multi-twisted Hermitian codes that achieves a Schur square dimension close to that of a random linear code. Codes of this subfamily are resistant to Schur square distinguishing when implemented within the McEliece cryptosystem where as one-point Hermitian codes are not, as recently demonstrated by Couvreur, Márquez-Corbella, and Pellikaan.

Many variants of the McEliece cryptosystem have been introduced which use different families of linear codes than the original Goppa codes. Additional structure can lead to a reduction in key size but often at the cost of introducing vulnerabilities that allow an attacker to extract identifying characteristics of the underlying code from the public-key matrix; see, for instance, the recent work by Couvreur, Márquez-Corbella, and Pellikaan on algebraic geometry codes. Schur square distinguishing is effective against one-point Hermitian codes by exploiting the low Schur square dimension of one-point Hermitian codes. To retain many desirable qualities of one-point Hermitian codes while fortifying a Hermitian-based McEliece variant, we introduce a new family of codes called twisted Hermitian codes. These codes are based on one-point Hermitian codes and strongly inspired by the twisted Reed-Solomon code described by Beelen, Puchinger, and Nielson. Hermitian codes have an advantage over Reed-Solomon codes in that longer codes can be obtained over smaller alphabets; for instance, to obtain a Reed-Solomon code of length 4096, one must use an alphabet of size 4096 whereas a Hermitian code of the same length only requires an alphabet size of 256. Twisted Hermitian codes can have a large Schur square, which safeguards against the efficacy of Schur square distinguishing attack. We construct a subfamily of multi-twisted Hermitian codes that achieves a Schur square dimension approaching that of a random linear code. The security of the new code against Schur square distinguishing may be interesting for code-based cryptography.

Joint work with Austin Allen (Carnegie Mellon University), Keller Blackwell (University of South Florida), Olivia Fiol (Vassar College), Rutuja Kshirsagar (Virginia Tech), Bethany Matsick (Liberty University), and Zoe Nelson (Oglethorpe University).
Partially funded by NSF DMS-1403062, -1547399, and -1855136.