Abstract:

With the possibility of quantum computing threatening the security of RSA and ECC cryptosystems, the McEliece Cryptosystem and its variants have been considered as a possibly suitable replacement. While the major drawback of the originally proposed McEliece cryptosystem was its large key size, one variant of the cryptosystem uses quasi-cyclic MDPC (QC-MDPC) codes to generate the keys. By using quasi-cyclic codes, the key size can be dramatically reduced while still retaining the same security (public keys have only 4801 bits for 80-bits of security, as opposed to 50-100 kByte for the same amount of security using the original design). This talk will present an implementation of a critical component of the QC-MDPC McEliece Cryptosystem, the key generator, in software. The key generator has three main components, random number generation, matrix inversion, and matrix multiplication, all over GF(2). In addition, we will discuss optimizations and considerations for implementing the key generator in hardware.