Abstract:

In 1978, Robert McEliece proposed a public-key encryption scheme based on error-correcting codes. The McEliece scheme (and its variant due to Niederreiter) is a simple, elegant and efficient design, and has its security based on two hardness assumptions: the intractability of decoding a random linear code, and the difficulty of distinguishing some permuted linear binary codes from a random code. McEliece's construction is over 40 years, and despite enormous cumulative efforts by the cryptographic community, it remains unbroken when instantiated with Goppa codes for suitable parameters. Its main drawback is the large public key, and attempts to reduce it to more manageable sizes have often resulted on insecure designs. Code-based cryptography is again attracting considerable attention from the cryptographic community, mainly due to the ongoing NIST PQ competition: over 20 submissions are based on error-correcting codes. In this talk we give an overview of code-based cryptography, main designs and their security, and discuss a selected few submissions to the NIST competition.