## Abstract

Code-based public key cryptography can resist against attacks from quantum computer and has become one of the important types of post-quantum public key cryptography. The security of most code-based public key schemes is based on the hardness of the syndrome decoding problem. The concrete hardness of the problem accurately estimates the specific security strength of the corresponding public key cryptographic schemes by using the best solver of the problem--information set decoding (ISD) algorithms. Therefore, in this talk we survey the ISD algorithms, and present some our results about this aspect.