انجمن رمز ایران
Iranian Society of Cryptology

Code based Cryptography as a Post Quantum Cryptography candidate

Code based cryptography is one of the prominent replacements of Number Theory based cryptosystems which will be broken by large scale Quantum computers. The main challenge of code based cryptography as one of the candidates for post quantum cryptography is its standardization in two aspects of efficiency and security to prepare it to use in these ages and also in the Quantum Computer age. Designing secure and efficient algorithms to reduce key length is one of the main needs of code based cryptosystems. In addition, cryptanalysis of several proposed schemes is another hot topic in this field, since the efforts to overcome some weak points of code based cryptosystems make them vulnerable to structural or decoding attacks.

In this talk, I will discuss the basic coding hard problems, Primary schemes and main attacks in the code based cryptography. Also, I will give an overview of code based cryptosystems which prepared for post quantum cryptography in the recent years and discuss their efficiency and security. Moreover, I will highlight some hot topics and the situation of code based cryptography among other post quantum cryptography candidates.