An overview of (some) post quantum threshold schemes

Giacomo Borin

Abstract: Threshold schemes allow a group of parties to jointly perform cryptographic operations in a distributed matter, providing enhanced security and reliability. Being in the middle of a transition from classical public key cryptography to quantum resistant alternatives, the design of post-quantum threshold protocols is an active and timely area of research, boosted by the recent NIST call for distributed schemes. In this talk, we give an overview of several recently proposed threshold schemes, from a variety of post-quantum assumptions. We will focus on open questions, key differences between protocols and mathematical techniques involved, design challenges and gaps in security arguments.