Cryptography after the time of Shannon and in the presence of a quantum computer

Joachim Rosenthal
University of Zürich
Mathematics Institute
8057 Zürich, Switzerland

Assymmetric cryptographic protocols such as the RSA system, the Diffie-Hellman key exchange and the ElGamal protocol rely on the hardness of factoring or on the hardness of the discrete logarithm problem in a finite group. These protocols will become obsolete in the presence of a capable quantum computer.

In this talk we will describe two sets of public key systems which so far seem to be quantum computer resistant.

The first system is a generalization of the usual Diffie-Hellman key exchange and ElGamal protocol. Crucial for this generalization will be semi-group actions on finite sets. Our main focus point will be semi-group actions built from semi-rings and several examples will be provided.

In a second part we review some coding based systems.