Lattice Signatures

Johannes Buchmann, Technische Universität Darmstadt

Digital signatures are extremely important for making open computer networks such that the Internet secure. However, there are only a few practical digital signature schemes. Their security is based on the hardness of the integer factoring problem or on the problem of computing discrete logarithms in the multiplicative group of a finite field or in the point group of an elliptic or hyperelliptic curve over a finite field. Those problems may not be hard at all. For example, they can be solved in polynomial time by quantum computers. A potential alternative are lattice based signatures, in particular lattice based one-time signatures in combination with the Merkle hash tree based signature scheme.

In this talk we explain the importance of digital signatures. We discuss lattice based signature schemes and their security. We describe the Merkle hash tree based signature scheme and we show how it can be made very practical in combination with a new lattice based one-time signature scheme.