JINTAI DING, University of Cincinnati

Post-Quantum Key Exchange from the LWE

In this lecture, we present practical and provably secure (authenticated) key exchange protocol and password authenticated key exchange protocol, which are based on the learning with errors problems. These protocols areconceptually simple and have strong provable security properties. This type of new constructions were started in 2011-2012. These protocols are shown indeed practical. We will explain that all the existing LWE based key exchanges are variants of this fundamental design. In addition, we will explain some issues with key reuse and how to use the signal function invented for KE for authentication schemes.