Cryptographic Protocols from Lattices

Eike Kiltz

CWI, Amsterdam
kiltz@cwi.nl

Abstract. In this talk, we will introduce abstract tools and techniques for working with lattices from the perspective of a cryptographic protocol designer. We will also show how to apply these tools to yield a number of provably secure public-key primitives ranging from digital signatures and public-key encryption, to more advanced protocols such as (hierarchical) identity-based encryption.

S.-H. Heng and K. Kurosawa (Eds.): ProvSec 2010, LNCS 6402, p. 199, 2010.