1096-A0-11 **Jill Pipher***, Department of Mathematics, Brown University, Providence, RI. *The mathematics of lattice-based cryptography.*

Lattice-based cryptography has become a major focus of research in the field of public key cryptography: various schemes offer efficiency, provable security, resistance to quantum computing based attacks, or most recently, fully homomorphic functionality. This chapter in cryptography research took off in 1996-97 with Ajtai's breakthrough paper "Generating Hard Instances of Lattice Problems" and a quick succession of three lattice-based public key encryption schemes: NTRU, GGH, and Ajtai-Dwork. Up to then, lattices had been primarily used in the cryptanalysis of a number of public key potential alternatives to RSA, known as knapsack schemes. This lecture introduces the mathematical ideas in this subject from 1996 to the present, ending with a discussion of fully homomorphic encryption. It will be accessible to a wide audience. (Received April 09, 2013)