# Some Perspectives on Complexity-Based Cryptography

Andrew Chi-Chih Yao

Tsinghua University, Beijing, China
andrewcyao@tsinghua.edu.cn

**Abstract.** In the 1940's, Shannon applied his information theory to build a mathematical foundation for classical cryptography which studies how information can be securely encrypted and communicated. In the internet age, Turing's theory of computation has been summoned to augment Shannon's model and create new frameworks, under which numerous cryptographic applications have blossomed. Fundamental concepts, such as "information" and "knowledge transfer", often need to be re-examined and reformulated. The amalgamation process is still ongoing in view of the many unsolved security issues. In this talk we give a brief overview of the background, and discuss some of the recent developments in complexity-based cryptography. We also raise some open questions and explore directions for future work.