A Light-weight Bit Commitment Protocol Based on Unpredictable Channel Noise

官振傑
National Sun Yet-sen University

Bit commitment is an important tool in the design of many secure cryptographic protocols, such as coin flipping, zero-knowledge proof, and secure computation. In this talk, we present a computationally light-weight bit commitment protocol over a noisy channel. For the security of the proposed protocol, we show that the receiver has almost no information about the committer's secret due to unpredictability of the noises in the communication channel. Hence, the security of our bit commitment protocol does not depend on hard problems; it is information-theoretically secure. Furthermore, the protocol needs only exclusive-or operations. Thus, it is computationally light-weight, and it can be used in the devices whose computing resources are limited.