Cryptography for Computer Scientists 2018/19 Jan, 2019

Exercises 13, 14, and 15

Stefan Dziembowski MIM UW

Exercise 1: Commitment schemes from OT

Construct a commitment scheme from an oblivious transfer protocol.

Exercise 2: OT from correlated randomness

Suppose Alice and Bob have access to a source that samples random values according to some distribution $P_{(R_A,R_B)}$, and passes a freshly sampled R_A to Alice and R_B to Bob. Show how to construct an oblivious transfer protocol from such "correlated randomness"

Exercise 3: Impossibility of IT-secure single-sever PIR

Show that an IT-secure single-sever Private Information Retrieval protocol does not exist.

Exercise 4: IT-secure PIR

Construct and IT-secure Private Information Retrieval protocol with more than 1 server.

Exercise 5: Secret sharing as a matrix operation

Present Shamir's secret sharing as a matrix operation. Show how this observation can be used to generalize Shamir's secret sharing to non-threshold adversary structures.

Exercise 6: Multiplication in IT-secure MPC

Consider a passively-secure MPC protocol based on Shamir's secret sharing. On the lecture we have shown an addition protocol for it. Construct a multiplication protocol for it.

Exercise 7: Adaptive vs non-adaptive security

Show an example of an n-party protocol that is secure *non*-adaptively, but it *not* secure adaptively.

Exercise 8: Authenticated broadcast

Construct an "authenticated broadcast" protocol for $n = 3$ parties and think of such a protocol for $n > 3$ (see, e.g, [1], Sect. 2.5).

References

[1] Ranjit Kumaresan. "Broadcast and Verifiable Secret Sharing: New Security Models and Round Optimal Constructions". PhD thesis. University of Maryland, College Park, MD, USA, 2012.