Secure Computation and Its Diverse Applications

Yuval Ishai

Technion and UCLA
yuvali@cs.technion.il

Abstract. Secure multiparty computation (MPC) allows two or more parties to perform a joint distributed computation without revealing their secrets to each other. While MPC has traditionally been viewed as an ends rather than a means, in recent years we have seen a growing number of unexpected applications of MPC and connections with problems from other domains.

In this talk we will survey several of these connections and highlight some research directions which they motivate. In particular, we will discuss the following connections:

- MPC and locally decodable codes. How can the secrecy property of MPC protocols be useful for reliable and efficient access to data?
- MPC and the parallel complexity of cryptography. How can progress on the round complexity of MPC lead to better parallel implementations of one-way functions and other cryptographic primitives?
- MPC and private circuits. How can MPC be used to protect cryptographic hardware against side-channel attacks?
- MPC in the head. How can MPC protocols which assume an honest majority be useful in the context of two-party cryptography?

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-3-642-11799-2_36

D. Micciancio (Ed.): TCC 2010, LNCS 5978, p. 90, 2010.