Algorithmic Aspects of Secure Computation and Communication

Matt Franklin (U.C. Davis)

Abstract. We survey some recent progress in the design of efficient protocols for secure computation and communication, in a variety of cryptographic settings. The common thread is the usefulness of interesting algorithmic methods originally developed for non-cryptographic applications. We also present some intriguing open problems for which new algorithmic ideas may be needed.

O. Cheong, K.-Y. Chwa, and K. Park (Eds.): ISAAC 2010, Part I, LNCS 6506, p. 2, 2010.