Private Set Intersection

Benny Pinkas, Bar-Ilan University

Abstract

Private set intersection (PSI) allows two parties to compute the intersection of their sets without revealing any information about items that are not in the intersection. PSI is relevant in many scenarios of secure computation, such as data sharing or contact discovery. PSI is one of the best studied applications of secure computation and many different PSI protocols have been proposed, using a wide and interesting variety of cryptographic tools. However, existing PSI protocols do not scale up well, and therefore some applications use insecure solutions instead.

This talk will survey what we believe to be the most interesting PSI protocols, describe new approaches for designing PSI protocols, and present a performance comparison.

Joint work with Thomas Sander, Gel Segev, and Michael Zohner.