Private Set Intersection with dynamic datasets

Melek Onen*[1]

[1]EURECOM – EURECOM – Campus SophiaTech, 450 Route des Chappes, 06410 Biot FRANCE, France

Résumé

Private Set Intersection (PSI) has been widely studied, deployed, and demonstrated through various real-life use cases such as mobile private contact discovery, privacy-preserving contact tracing, etc. Nevertheless, the majority of existing solutions assume that the underlying datasets are static. In this talk, we will present the problem of and requirements for designing efficient and secure PSIs when datasets are frequently updated. We will review and study existing "updatable PSI" (UPSI) constructions and further construct a generic framework for UPSIs based on the use of circuit-PSIs.

*Intervenant