Randomness Delegation and its Connections with Secure Computation

Mahshid Riahinia*[1]

[1]Ecole Normale Supérieure (ENS) – École normale supérieure [ENS] - Paris – 45 Rue d'Ulm, 75005 Paris, France

Résumé

Pseudorandom functions (PRFs), introduced in 1986, enable efficient generation of randomness and serve as essential tools in cryptography. Constrained pseudorandom functions (CPRFs), introduced in 2013, extend traditional pseudorandom functions (PRFs) by additionally allowing the delegation of constrained keys that enable the evaluation of the function only on specific subsets of inputs. Interestingly, this additional functionality significantly enhances the power of constrained PRFs in building advanced cryptographic protocols and, at the same time, makes CPRFs more challenging to realize. The goal of this talk is to introduce and motivate recent efforts in drawing connections between CPRFs and secure computation protocols.

The content of this talk is based on the results published in my thesis as well as ongoing research

*Intervenant