Secure computation and correlated randomness, from theory to practice

Geoffroy Couteau*[1]

[1]IRIF – CNRS, Université Paris Cité – France

Résumé

In this talk, we provide an in-depth introduction to secure multiparty computation, shedding light on how researchers approach it through the lens of correlated randomness. We give an overview of core historical protocols and some key milestones, with the aim to convey an intuition about their concrete efficiency and the core obstacles we must overcome to make them usable in the real world. Towards the end of the talk, we will also cover some recent developments in methods to generate correlated randomness using a minimal amount of communication.

*Intervenant