Geoffroy Couteau (GT C2) – CNRS, IRIF, Université Paris cité.

Title: Secure computation: protecting the privacy of sensitive data used in distributed computations

Abstract: The importance of privacy over networks is well-acknowledged: more than 85% of our Internet communications are encrypted, and end-to-end encryption is becoming a standard in messaging apps. Yet, with the explosive growth of social networks and machine learning applications, our private data is also routinely revealed to third parties when it is used in distributed computations (in Cloud storage, social networks, apps, recommendation systems, ads, and more). Secure computation addresses this issue by providing a means to execute distributed computations without compromising private data. This talk will cover the old and recent developments in this area and discuss the remaining barriers to be lifted before deploying secure computation on the large scale.