Encrypted search and weighted hashing

Brice Minaud*[1]

[1]ENS Paris – Ecole Normale Supérieure de Paris - ENS Paris, L'Institut National de Recherche en Informatique et e n Automatique (INRIA) – France

Résumé

Much of our private or professional data is stored in the cloud. To protect it, encryption is necessary. However, naive encryption precludes searching over, or interacting with the data. Several tools to address this issue have been developed within cryptography. In this talk, I will focus on a simple but fundamental algorithmic problem that occurs when wanting to store and efficiently fetch files on a distant server, while fulfilling a minimalist privacy requirement. (No prior knowledge of cryptogaphy is necessary.) The problem occurs especially in the area of Searchable Encryption. The main obstacle comes from a tension between security and efficiency, that was captured in a seminal impossibility result by Cash and Tessaro (Eurocrypt 2014). Since then, a long line of work has studied how to reconcile security and efficiency in this minimalist setting, by proposing new constructions, definitions, and lower bounds, both theoretical and practical. I will try to give an overview of this area and some recent advances in it: what is known so far, and what questions remain open.

*Intervenant