Private Heavy-Hitters through Multi-Dealer Secret Sharing

Gabrielle Becke*[1]

[1]Exact Computing (LIRMM — ECO) – Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier – LIRMM, 161 rue Ada, 34000 Montpellier, France

Résumé

We propose a new private telemetry system for computing k-heavy hitters in the STAR and POPSTAR model. In this setting, each client generates a report with the assistance of a lightweight Randomness Server and submits it to a central Aggregation Server, which can then locally compute only the heavy hitters. As compared to STAR and POPSTAR—which reveal either the full (pseudonymized) frequency histogram or a complex function of it—our protocol reduces leakage: the Aggregation Server learns non-heavy-hitter values only if their frequency exceeds a well-defined threshold. Additionally, while STAR and POPSTAR are weak to an Aggregation Server that colludes with clients, our protocol provides optimal security against such a colluding server. To achieve these privacy guarantees, our protocol efficiently adapts multi-dealer secret sharing to the STAR/POPSTAR model and introduces a novel oblivious secret-share sampling protocol to ensure security against a colluding Aggregation Server. We implement and benchmark the performance of our protocol and find that it is practical for a number of use cases. Moreover, we show that it supports a tunable three-way tradeoff between correctness, efficiency and privacy.

*Intervenant