Université de Montréal — Faculté des arts et des sciences

Colloque du
Département d'informatique et de recherche opérationnelle

Mohammad Mahmoody

Cornell University

Time-Lock Puzzles, Proofs of Work, and Timestamping Documents

Résumé :

We construct a publicly verifiable protocol for proving computational work in the random oracle model resisting parallel attacks. Our protocol is based on a novel construction of time-lock puzzles. Given a sampled puzzle $P \leftarrow D_n$, where n is the security parameter and D_n is the distribution of the puzzles, a corresponding "solution" can be generated using N evaluations of the oracle, where $N > n$ is another parameter, while any feasible adversarial strategy for generating valid solutions must take at least as much time as $\Omega(N)$ sequential evaluations of the oracle after receiving P. Thus, valid solutions constitute a "proof" that $\Omega(N)$ parallel time elapsed since P was received. Solutions can be publicly and efficiently verified in time $\text{poly}(n)\,\text{polylog}(N)$. Applications of these "time-lock puzzles" include non-interactive time-stamping of documents and universally verifiable CPU benchmarks. Our construction makes a novel use of "depth-robust" directed acyclic graphs—ones whose depth remains large even after removing a constant fraction of vertices—which were previously studied for the purpose of complexity lower bounds.

Based on joint work with Tal Moran and Salil Vadhan.

Le jeudi 11 avril 2013, 15h30, pavillon André-Aisenstadt, salle 3195
Information : Gilles Brassard, brassard@iro.umontreal.ca