

Big Data Analytics 2013



Invited talk

Streaming Verification of Outsourced Computation

Graham Cormode, *University of Warwick*

When handling large quantities of data, it is desirable to outsource the computational effort to a third party: this captures current efforts in cloud computing, but also scenarios within trusted computing systems and inter-organizational data sharing. When the third party is not fully trusted, it is desirable to give assurance that the computation has been performed correctly. This talk presents some recent results in designing new protocols for verifying computations which are streaming in nature: the verifier (data owner) needs only a single pass over the input, storing a sublinear amount of information, and follows a simple protocol with a prover (service provider) that takes a small number of rounds. A dishonest prover fools the verifier with only polynomially small probability, while an honest prover's answer is always accepted. Starting from basic aggregations, interactive proof techniques allow a quite general class of computations to be verified, leading to practical implementations.