April 2010

Crypto & MADALGO seminar
by Ivan Damgård and Jonas Kölker, Aarhus University

Multiparty Computation with Storage Servers, or: Combining Secure Computation and IO-Efficient Algorithms

Abstract:

We introduce a new connection between IO-efficient algorithms and secure computation. We use this to design protocols for a setting where a set of *n* players use a set of *m* servers to store a large data set. Later the players want to compute on the data without the servers needing to know which computation is done, while the computation should be secure against an adversary corrupting a constant fraction of the players and servers. Using packed secret sharing the data can be stored in a compact way but will only be accessible in a block-wise fashion. We explore the possibility of using IO-efficient algorithms to nevertheless compute on the data as efficiently as if random access was possible.

We show for sorting, this is indeed the case, by showing how to evaluate the odd-even merge sort network I/O-efficiently, and by giving efficient protocols for reading and writing blocks of data to the servers.