DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF SOUTHERN DENMARK, ODENSE

COMPUTER SCIENCE COLLOQUIUM

Information Theoretically Secure MPC Against Dynamic Adversaries

Ivan Bjerre Damgård
Department of Computer Science
Aarhus University, Denmark

Monday, 28 June, 2021 at 14:15

IMADA's Seminar Room

Abstract:

In Multiparty computation (MPC) a set of parties want to compute on privately held inputs in such a way that only the intended result is revealed. This should hold even in presence of an adversary who corrupts some of the parties, in an attempt to manipulate the result or learn more information than is allowed. The adversary may make some parties crash (fail corruption), or spy on their internal state (passive corruption) or take complete control over a party (active corruption). Assuming we restrict the adversary to f fail, p passive and a active corruptions, it has been known for a long time that (statistically secure) MPC is possible for n parties if and only if $2a + 2p + f < n$. In this work, we ask: what if the adversary is given the protocol first, and can then choose f, p and a? This stronger type of adversary is called dynamic. We show that the feasibility bound for MPC is $2a+2p+f < n$ even for a dynamic adversary. However, any dynamically secure protocol must use at least n rounds of interaction.

Joint work with Daniel Escudero and Divya Ravi.

Host: Joan Boyar