DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
ODENSE UNIVERSITY

COMPUTER SCIENCE COLLOQUIUM

Some Problems in Monotone Span Program Complexity with Applications to Multiparty Computations

Ivan Damgård
Department of Computer Science
University of Aarhus

Tuesday, March 31, 1998, at 2:15 PM
The Seminar Room

Abstract: In recent work, Cramer, Damgaard and Maurer have shown that monotone span programs can be used to implement fault tolerant multiparty computations, protecting privacy without intractability assumptions. The possible faulty subsets of the n players can be described in a natural way by a monotone Boolean function on n inputs bits. The protocols by CDM are efficient in scenarios where the function describing the possible faulty subsets has a poly-size monotone span program.

The performance of earlier protocols was connected in a similar way to the monotone formula complexity of these functions. We show that the well known separation between monotone span programs and monotone formulae carries over to the types of functions occurring here, which implies that monotone span programs give rise to strictly more efficient verifiable secret sharing protocols that what was known earlier.

If the separation we show could be proved to hold, also if the span program is required to have a special "multiplication property", this would imply that span programs can make general multiparty computations more efficient. This is open at the time of writing.

Joan Boyar