abstract

Video of this lecture

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In this talk, I shall describe an ongoing project to develop a complexity theory for cryptographic (multi-party computations. Different kinds of cryptographic computations involve different constraints on how information is accessed. Our goal is to qualitatively -- and if possible, quantitatively -- characterize the "cryptographic complexity" (defined using appropriate notions of reductions) of these different modes of accessing information. Also, we explore the relationship between such cryptographic complexity and computational intractability.

Our first set of results considers cryptographic complexity with no reference to computational complexity aspects. We identify several cryptographic complexity classes, with the help of new reductions (protocols) as well as new separations (impossibility results), revealing a rich structure in the universe of cryptographic tasks. We also develop an information-theoretic measure to quantify the cryptographic content of correlated random variables distributed between two parties.

Our second set of results explores the connection between computational intractability and cryptographic complexity. Our results suggest that there are only a few distinct intractability assumptions that are necessary and sufficient for all the infinitely many reductions among cryptographic tasks. In deriving these results, again, we provide new protocols as well as separation results.

Significantly, this approach of defining the universe of intractability requirements in terms of cryptographic tasks (rather than using specific assumptions formulated for proving the security of specific contructions) gives a possibly finite set of computational complexity

assumptions to study, corresponding to a finite set of worlds between "Minicrypt" and "Cryptomania." The main open problem we pose is to identify the set of all intractability assumptions that appear in this way.

These results are mostly based on joint work with Hemanta Maji and Mike Rosulek; if time permits I will mention on going works that also involve Mohammad Mahmoody-Ghidary, Pichayoot Ouppaphan, Vinod Prabhakaran and Amit Sahai.