Speaker: Binyamin Applebaum, Tel Aviv University

Title: Arithmetic Cryptography

We study the possibility of computing cryptographic primitives in a fully-black-box arithmetic model over a finite field F. In this model, the input to a cryptographic primitive (e.g., encryption scheme) is given as a sequence of field elements, the honest parties are implemented by arithmetic circuits which make only a black-box use of the underlying field, and the adversary has a full (non-black-box) access to the field. A similar model was previously considered in the context of information-theoretic secure multiparty computation.

We prove several positive and negative results in this model for various cryptographic tasks. Our results reveal a qualitative difference between the standard model and the arithmetic model, and explain, in retrospect, some of the limitations of previous constructions.

Joint work with Jonathan Avron and Christina Brzuska.