Bocconi

Università Commerciale
Luigi Bocconi

Department of Decision Sciences
Occasional Seminar

Total Search Problems and Cryptography

Alon Rosen

Herzliya Interdisciplinary Center

Friday, 13th December 2019
12:30 pm Room 3-E4-SR03 Via Roentgen 1 Milano

Abstract

Total search problems are ones where every instance has a solution. Yet, a growing body of evidence suggests that finding this solution is sometimes intractable. This phenomenon has fascinated complexity theorists since the 1980's. Over the last few decades, it has also been tied to an increasingly diverse list of applications from areas such as Combinatorial Optimization, Graph Theory, Economics and Social Choice.

In this talk I will survey connections between cryptographically hard problems and total search problems in NP (TFNP), and in particular between incrementally verifiable proofs and the problems of finding a Nash equilibrium in a bimatrix game. Such connections provide new, extrinsic, evidence supporting the conjecture that some prominent TFNP problems are indeed hard.

Bio:

Alon Rosen is a full professor at the School of Computer Science at the Herzliya Interdisciplinary Center.

His areas of expertise are in theoretical computer science and cryptography. He has made contributions to the foundational and practical study of zero-knowledge protocols, as well as fast lattice-based cryptography, most notably in the context of collision resistant hashing and pseudo-random functions. He co-introduced the ring-SIS problem and related SWIFFT hash function, as well as the Learning with Rounding problem. These works lie at the heart of modern efficient lattice-based cryptography.

Alon is an associate editor of the Journal of Cryptology and served as Program Committee chair of the 2019 Theory of Cryptography Conference (TCC'19). He is a recipient of an ERC starting grant as well as grants from the BSF, ISF, NSF-BSF, Horizon 2020, and the MIT-Israel fund. He was awarded the TCC 2017 test of time award, for his TCC 2006 work on fast collision-resistant hashing from algebraic lattices.

Alon earned his PhD from the Weizmann Institute of Science (Israel) in 2003, and was a Postdoctoral Fellow at MIT (USA) in the years 2003-2005 and at Harvard University (USA) in the years 2005-2007. He is a faculty member at IDC since 2007.