White-box vs. black-box search problems: a cryptographic perspective

Abstract:

Ramsey theory assures us that in any graph there is a clique or independent set of a certain size, roughly logarithmic in the graph size. But how difficult is it to find the clique or independent set? If the graph is given explicitly, then it is possible to do so while examining a linear number of edges. If the graph is given by a black-box, where to figure out whether a certain edge exists the box should be queried, then a large number of queries must be issued. But what if one is given a program or circuit for computing the existence of an edge? What if we are assured that the program is small without being given explicitly?

In this talk I will explore recent work on the complexity of search problems with guaranteed solution (the class TFNP) and the tight relationship with cryptographic assumptions and techniques.

Based on joint works with Pavel Hubacek, Ilan Komargodski and Eylon Yogev