Fine-Grained Cryptography: A New Frontier?

Invited Talk

Alon Rosen*

IDC Herzliya

Abstract. Fine-grained cryptography is concerned with adversaries that are only moderately more powerful than the honest parties. We will survey recent results in this relatively underdeveloped area of study and examine whether the time is ripe for further advances in it.

One approach for weakening the assumptions underlying cryptographic constructions is to require less from them. For instance, rather than requiring a super-polynomial gap between the running time of the honest parties and that of the adversary, one could settle for some fixed polynomial gap. This *fine-grained* approach to cryptography was considered as early as 1974 by Merkle, who relied on a random oracle to construct a key-exchange protocol in which the honest parties run in time $O(n)$, while security holds against $O(n^2)$-time adversaries.

Merkle's scheme demonstrates how in a fine-grained setting, public-key encryption can be obtained from a primitive as unstructured as a random oracle. While this lack of structure renders the scheme less susceptible to cryptanalysis than its traditional counterparts, it does have its limitations. As proved by Barak and Mahmoody in 2009, the quadratic gap in Merkle's construction is optimal. If one were to increase the gap between honest and malicious parties, it will be necessary to rely on structured computational problems.

It has already been shown how structure could be used to attain larger than quadratic gaps between honest and malicious parties. For instance, recent advances in fine-grained complexity have increased our confidence in the concrete polynomial hardness of a host of problems in P, along with a web of interconnectedness between them. Based on such problems, we now have new candidate proofs of work with any arbitrary fixed polynomial gap between parties.

Could such results be extended to constructing fine-grained one-way functions? This is a necessary step we need to take if we were to bypass the optimality of the gap in Merkle's key-exchange protocol. Looking even further, suppose we do succeed in our quest. Should we stop there? And what about the foundations? Shouldn't they also be revisited and adapted to the fine-grained setting?

One could rightfully argue that structured problems tend to be computationally easy, and hence are less desirable from a cryptographic standpoint. Still, aren't the most structured problems within P the ones that admit the only known lower bounds in complexity theory? Could it actually be a structured problem that will eventually give rise to unconditionally secure cryptography?

* Supported by ISF grant No. 1399/17 and by Project PROMETHEUS (780701).