How Low Can We Go?

Invited PKC 2020 Talk

Yuval Ishai*

Computer Science Department, Technion

Abstract. We will discuss the question of minimizing different complexity measures of cryptographic primitives, some known results and remaining challenges, and how the study of this question can have impact beyond cryptography.

Given a cryptographic task, such as encrypting a message or securely computing a given function, a natural question is to find the "minimal cost" of carrying out this task. The question can take a variety of forms, depending on the cost measure. For instance, one can try to minimize computation, communication, rounds, or randomness. In the case of computational cost, one can consider different computation models, such as circuits or branching programs, and different cost metrics, such as size or depth. The answer to the question may further depend on the type of computational assumptions one is willing to make.

The study of this question, for different cryptographic tasks and clean asymptotic cost measures, has led to a rich body of work with useful and often unexpected results. The talk will survey some results along this line, highlighting connections between different research areas in cryptography and relevance beyond cryptography.

In addition to the direct interest in minimizing well-motivated complexity measures, there are cases in which "high-end" cryptographic tasks, such as secure multiparty computation or program obfuscation, call for minimizing different cost measures of lower-end primitives that would otherwise seem poorly motivated. I will give some examples of this kind.

Finally, I will make the case that despite the progress already made, there is much more to be explored. Research in this area can greatly benefit from more cooperation between theoretical and applied cryptographers, as well as between cryptographers and researchers from other fields, including computational complexity, algorithms, computational learning theory, coding theory, and information theory.

* yuvali@cs.technion.il. Supported by ERC Project NTSC (742754), NSF-BSF grant 2015782, BSF grant 2018393, and a grant from the Ministry of Science and Technology, Israel and Department of Science and Technology, Government of India.