Cryptography from Lossy Reductions: Towards OWFs from ETH, and Beyond

Pouria Fallahpour*[1]

[1]LIP6 – Sorbonne Universite, Centre National de la Recherche Scientifique – 4 Place JUSSIEU 75252 PARIS CEDEX 05, France

Résumé

One-way functions (OWFs) are essential cryptographic tools and can be viewed as the minimal assumption required for cryptography. Informally, a function is called one-way if it is easy to compute but hard to invert. The existence of one-way functions implies that of many cryptographic primitives such as pseudorandom generators, commitments schemes, and zero-knowledge proofs. Although it is unknown whether they unconditionally exist, several candidate constructions have been proposed assuming the hardness of concrete computational problems such as discrete logarithm, lattice-based problems, and more. Instead of depending on the hardness of specific problems, the pinnacle result in this direction would be to construct OWF from minimal computational complexity assumptions such as P not equal NP.

In this talk, we study this question by exploring its relation to lossy reductions, i.e., reductions R for which it holds that the mutual information between X and R(X) is much smaller than n for all distributions X over inputs of size n. Notable examples are worst-case to average-case Karp reductions and compression reductions. The main part of the talk is dedicated to show the following: either OWFs exist or any lossy reduction for any decision problem Q runs in time exp(c log t(n) / log log n) for some constant c, where t(n) is the infimum of the runtime of all (worst-case) solvers of Q on instances of size n. In other words, this shows that if OWFs do not exist, then randomizing or compressing the worst-case instances of any problem has at best polynomially-better runtime as solving these instances. We also see various aspects and stronger variants of this result. We finally discuss the consequences of these results for the NP-complete problem SAT.

The results are based on a collaboration with Alex Grilo, Garazi Muguruza, and Mahshid Riahinia.

*Intervenant