

- ▶ ARMANDO MATOS, ANDRE SOUTO, ANDREIA TEIXEIRA, *Distinguishing probability ensembles.*

LIACC, Portugal.

*E-mail:* `acm@dcc.fc.up.pt`.

University of Porto - Instituto de Telecomunicaes, Portugal.

*E-mail:* `andresouto@dcc.fc.up.pt`.

Instituto de Telecomunicaes/Faculdade de Cincias Universidade Porto, Portugal.

*E-mail:* `andreiasofiat@hotmail.com`.

We generalize the concept of distinguishability, based on the input or the output of the randomized, polynomial-time distinguishing algorithms. First we consider algorithms with an arbitrary integer output (instead of just 0 or 1) and prove that, when the output is bounded by a polynomial, these distinguishers are no more powerful than a variant of the classical (computational) one in which the algorithms may have a short advice (order  $O(\log n)$ ). Then, we characterize a distinguishing method in which two samples, one from each ensemble, may be given as input to the algorithm (the case of two or more samples of the *same* ensemble as input has already been studied in [?, ?]) and we study the properties of this new distinguishing method. Finally, we use, as distinguishers, algorithms that are lossless compressors and output the *length* of the compressed string; somewhat surprisingly, any pair of classically distinguishable ensembles, is also distinguishable by the length of the output of some compressor.