Perfect Secrecy Based on Kolmogorov Complexity

Luis Antunes* Sophie Laplante+ Liliana Salvador*

*Departamento de Ciência de Computadores, FCUP & LIACC
+Laboratoire de Recherche en Informatique, Université Paris-Sud

There exist several notions of security for cryptographic systems. Most of them are based on assumptions from complexity theory, for example P $\neq$ NP or the factorization of large integers cannot be performed in polynomial time. Nevertheless there are some systems (symmetric) that we can prove to be unconditional secure against an opponent with unconditionally computational power. The proof of unconditional security is based on the notion of entropy, introduced by Shannon, measuring the amount of information in situations where unlimited computational power is available. However this measure does not provide a satisfactory framework to the analysis of public key cryptosystems, always based on cryptographic assumptions (imposing limited computational power to an adversary).

In this work we use Kolmogorov Complexity, a rigorous measure of the amount of information in an individual string. We replaced entropy by Kolmogorov complexity and still were able to prove the perfect secrecy of some symmetric systems, such as One-time-Pad and secret sharing. We are now working on authentication.