From Rubik's to cryptography: a tour of computational challenges in the field

Christophe Petit (UCL)

November 23, 2012

While cryptography used to be a secret military art, it is now surrounding lambda citizens in their private communications, secure e-banking or public transport RFID cards. In this talk, I will review some highlights of the cryptology science, with an emphasis on computational aspects. Challenges for the "good guy" (the cryptographer) and the "bad guy" (the cryptanalist) require various mathematical tools from number theory to statistics, arithmetic optimization, graph theory or machine learning, and various computing tools from "paper and pencil" to laptops, supercomputers or FPGA and Playstation clusters.