New Directions in Croptography

Adi Shamir

Applied Math Department, The Weizmann Institute of Science
Rehovot 76100, Israel
shamir@wisdom.weizmann.ac.il

Abstract. Croptography is a relatively new area of research which uses optical techniques to solve cryptographic problems. Optical computations are characterized by extremely high speed and truly massive parallelism, but they can not be used as general purpose computers. In this talk I'll survey the field, and show that many natural problems in cryptography and cryptanalysis can be efficiently solved by simple optical techniques. In particular, I'll describe a new way to break LFSR-based stream ciphers by using commercially available optical devices.

Ç.K. Koç, D. Naccache, and C. Paar (Eds.): CHES 2001, LNCS 2162, p. 159, 2001.