Stream Ciphers: Dead or Alive?

Adi Shamir

Weizmann Institute of Science, Israel
adi.shamir@weizmann.ac.il

Secret key cryptography was traditionally divided into block ciphers and stream ciphers, but over the last 30 years the balance had steadily shifted, and today stream ciphers have become an endangered species. In this talk I'll survey the current state of the art in stream ciphers: who needs them, who uses them, how they are attacked, and how they can be protected by new types of constructions.