The Way to Modern Cryptography

Ferucio Laurentiu Tiplea

Department of Computer Science
"Al.I.Cuza" University of Iasi
Iasi, Romania
E-mail: fltiplea@info.uaic.ro

In the late 20th century, cryptography radically changed from the cryptography as an art of writing or solving codes to cryptography as a science. The field of cryptography includes now not only secret communication but also message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, electronic auctions and elections, and digital cash. If before the 1980s the major consumers of cryptography were military and intelligence organizations, today cryptography is everywhere: security mechanisms based on cryptography are used to enforce access control in multi-user operating systems, to protect personal laptops or software applications. The scientific nature of modern cryptography relies mainly on the use of rigorous and precise definitions of security, accompanied with rigorous proofs of security for the cryptographic primitives.

The aim of this talk is to discuss the main achievements in (modern) cryptography since 1980s. The starting point is probabilistic encryption together with the concepts of semantic security and indistinguishability. Identity-based encryption (IBE) became reality since 2001 and commercial software based on it has already been produced. A more general form of IBE, called attribute-based encryption (ABE), offers solutions to cryptographically based access control systems. Both IBE and ABE make use of bilinear maps, one of the most influential discoveries in cryptography. In this context, lattice-based cryptography revolutionized the field of cryptography with fundamental theoretical breakthroughs and potentially transformative application: constructions such as fully homomorphic encryption, functional encryption, hashing, and signature schemes using hard problems on lattices, and cryptanalytic attacks using algorithms on lattices.