Metodi geometrici per la crittografia

dr. Luca Giuzzi

Università degli Studi di Brescia

Lo sviluppo di sistemi di comunicazione e di commercio tramite internet e' strettamente legato alla disponibilita' di metodi efficienti per garantire l'integrita' e la confidenzialita' dei dati.
I metodi correntemente impiegati, come pure alcuni di quelli in fase di sviluppo, sono basati sull'utilizzo di strutture algebriche discrete. Fra le varie possibilita', le strutture che si sono rivelate piu' promettenti dal punto di vista pratico sono quelle legate agli automorfismi di enti geometrici (curve algebriche, disegni).
In questa conferenza si presenteranno alcuni elementi fondamentali dei protocolli di comunicazione a chiave pubblica basati sul logaritmo discreto, nonche' l'importanza a questo proposito dello studio delle curve ellittiche, considerate come "gruppi in cui e' facile calcolare".
Inoltre si mostrera' come le strutture di incidenza (e i relativi gruppi di automorfismi) possano essere sfruttate per costruire sistemi di codifica con proprieta' prescritte a priori.