## Criptologia contemporània

Els principals temes tractats foren:

1. Seguretat dels criptosistemes basats en RSA.
2. Sobre la necessitat del model de L'Oracle Aleatori en el disseny de criptosistemes de xifrat segurs i eficients.
3. Aplicacions del xifrat homomòrfic multiplicatiu al disseny de sistemes de computació multipart.
4. Criptosistemes segurs basats en grups no abelians i en accions de grups.
5. Relacions entre la teoria de codis, la teoria de matroides i els problemes de la multiplicació en esquemes per a compartir secrets.