## Compartició de secrets

**Resum de la línia de recerca.** Els esquemes de compartició de secrets permeten distribuir en fragments un valor secret de manera que només alguns conjunts autoritzats de participants poden recuperar el valor secret. La compartició de secrets és una primitiva molt important en Criptologia, que s'utilitza en la construcció de diferents tipus de protocols criptogràfics. L'estudi d'aquesta primitiva criptogràfica ha conduït al desenvolupament d'una teoria matemàtica molt rica en la que intervenen l'Àlgebra Lineal, la Combinatòria, la Teoria de Codis, la Teoria de la Informació i, darrerament, la Geometria Algebraica.

La nostra recerca en aquest camp s'ha centrat en diferents problemes oberts de la Teoria de Matroides relacionats amb l'optimització dels esquemes de compartició de secrets per a estructures d'accés generals i amb la construcció d'esquemes amb la propietat multiplicativa.