

Matemàtiques i seguretat de continguts digitals

Desenvolupaments recents suggereixen que la majoria de protocols de clau pública usats actualment en el comerç electrònic poden oferir noves oportunitats en el futur. Al mateix temps, noves tècniques matemàtiques, com la teoria de la complexitat genèrica o la teoria de grups algorítmica i combinatorial, prometen aplicacions útils per a la creació i l'avaluació de criptosistemes de seguretat. En aquest programa s'aprofundeix en aquestes noves tècniques i s'utilitza la potència d'aquestes modernes branques de les matemàtiques per a l'obtenció de criptosistemes més segurs i més robustos.