dimarts, 07 d’abril de 2026

La criptografia basada en lattices, protagonista d’una xerrada a l’EPS

El passat 26 de març, Nicolas Thériault, de la Universitat de Santiago de Chile, va visitar l’EPS i va oferir la xerrada “Votació electrònica basada en lattices, una primera parametrització”

En aquesta xerrada es van presentar les idees utilitzades en criptografia basada en reticles per assolir comunicacions segures mitjançant el problema LWE. Aquest enfocament permet l’encapsulació de claus (KEM), signatures digitals (DSS) i el xifratge homomòrfic (FHE). Nicolas Thériault va explicar com aquestes tècniques es podrien adaptar a situacions com la votació electrònica i obtenim paràmetres que puguin oferir la seguretat desitjada amb més eficiència en les operacions criptogràfiques. La xerrada va acabar amb un debat d’alguns temes emergents en criptografia.