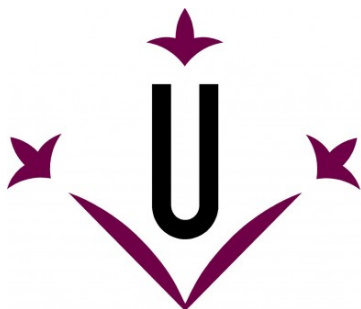


dimarts, 16 de juliol de 2013

Grup de recerca en Criptografia i Grafs de l'EPS de la UdL. Garantir la seguretat i la privacitat



Universitat de Lleida
Grup de Recerca
Criptografia i Grafs

El grup de recerca en [Criptografia i Grafs](http://www.cig.udl.cat/) [<http://www.cig.udl.cat/>] de l'Escola Politècnica Superior de la Universitat de Lleida treballa en el desenvolupament de protocols criptogràfics per garantir la seguretat en les votacions electròniques.



Membres del grup d'investigació en Criptografia i Grafs de l'Escola Politècnica de la UdL.

Josep M. Miret, coordinador del grup, destaca la presència i la importància actual de la criptografia en diversos aspectes de la nostra vida quotidiana com per exemple en el DNI, les targetes i transferències bancàries, el comerç electrònic, així com els treballs de recerca en altres camps en expansió com la privacitat en les xarxes socials o les etiquetes intel·ligents.

En els darrers anys s'ha experimentat un creixent interès pel desenvolupament de tecnologies basades en l'ús de targetes intel·ligents, així com de sistemes d'identificació RFID (Radio Frequency Identification). Les targetes intel·ligents s'utilitzen com a mecanismes d'autenticació d'usuaris com, per exemple, targetes de crèdit, de comunicació mòbil, d'autorització de mecanismes de pay-per-view, etc. D'altra banda, els sistemes RFID proporcionen una tecnologia que permet automatitzar el procés d'identificació a distància d'objectes o persones; aquests objectes van etiquetats mitjançant una RFID tag, que consisteix en un microxip dissenyat per transmetre dades via un canal wireless. L'ús de corbes el·líptiques facilita ajustar-se a les restriccions computacionals de memòria o d'amplada de banda (en el cas de RFID) que presenten aquests entorns.

Els grafs serveixen, en particular, per modelitzar i estudiar diferents tipus de xarxes (de comunicació, transport, d'activitats, socials, ...) sobre les quals pot interessar resoldre determinats problemes d'optimització (cerca

d'itinerari menys costós, determinació de la millor localització) o d'anàlisi (càlcul de mesures de connectivitat, identificació dels elements crítics). L'assessorament sobre el plantejament i la resolució d'aquest tipus de problemes, que apareixen, per exemple, en l'àmbit de la investigació operativa, és un dels serveis que ofereix el grup de recerca en Criptografia i Grafs.



14 de juliol de 2013



[http://www.eps.udl.cat/docs/noticies/Juliol13_14_Segre.pdf]



[http://www.eps.udl.cat/docs/noticies/Juliol13_14_Segre2.pdf]



[http://www.eps.udl.cat/docs/noticies/Juliol13_14_Segre3.pdf]



[http://www.eps.udl.cat/docs/noticies/Juliol13_14_Segre4.pdf]