DOCTORATS INDUSTRIALS

EL PLA DE DOCTORATS INDUSTRIALS

PROJECTE DE DOCTORAT INDUSTRIAL EXPEDIENT 2014 DI 049

DADES DE L'EMPRESA I DE L'ENTORN ACADÈMIC

Títol del projecte
Proves de coneixement nul per a sistemes de votació electrònica
Empresa
Scytl Secure Electronic Voting, SA
Responsable de l'empresa
Jordi Puiggalí Allepuz
Universitat
Universitat de Lleida
Director/a de tesi
Magda Valls Marsal
Treballador/a de l'empresa i doctorand/a
Víctor Mateu Meseguer

BREU DESCRIPCIÓ DEL PROJECTE DE RECERCA

Actualment, en votació electrònica la privadesa del votant s'ha de garantir tant en el moment de la emissió del vot com en el moment de fer el recompte dels resultats. Pel que fa a garantir la privades en el moment de votar, els sistemes de vot electrònic utilitzen el xifrat del vot en el mateix dispositiu que utilitza el votant, ja sigui el seu ordinador o mòbil intel•ligent personal com un terminal del vot específic que facilitin les entitats electorals en el mateixos col•legis electorals (quiosc de vot). Per al xifrat del vot s'utilitza un algoritme criptogràfic de clau asimètrica. D'aquesta manera, la clau de xifrat és pública i coneguda per tothom mentre que la clau de desxifrat es privada i està custodiada per una entitat de confiança assignada a vetllar per a la privadesa de l'elecció (p.e., mesa electoral).

Per garantir que, un cop finalitzat el període de vot, l'entitat responsable del desxifrat i recompte no pugui comprometre la privadesa dels votants (i.e., correlacionar els vots desxifrats amb l'ordre en el que van ser emesos), s'utilitza normalment un dels següents dos paradigmes: recompte homomòrfic o mix-nets (xarxes de mescla).

Quan s'utilitza el paradigma de recompte homomòrfic, els votants xifren el seu vot utilitzant un criptosistema homomòrfic i l'envien al servidor que guarda els vots. Els votants també han d'enviar una prova que demostra que el seu vot s'ha generat correctament (p.e., que el contingut xifrat sigui vàlid i no s'hagin seleccionat més opcions de les permeses). Un cop el servidor ha verificat tots els vots xifrats, quan es fa el procés de recompte s'agreguen els vots xifrats (operen matemàticament sense desxifrar) i demana a l'entitat de confiança (p.e., mesa electoral), que té la clau privada de l'elecció, que desxifri el resultat de la agregació dels vots.

Aquest haurien de ser els resultats finals (nombre de seleccions totals per opció).

En el paradigma de mix-net, els votants envien el seu vot al servidor que guarda els vots. Al finalitzar la elecció i començar el procés de desxifrat i recompte, el servidor demana a diferents "mixers" que barregin (permutin posicions i rexifrin o desxifrin parcialment) els vots rebuts i generin la prova de coneixement nul que demostri la correctesa de la barreja. Un cop verificat que tot el procés s'ha realitzat correctament, l'entitat de confiança amb la clau privada de l'elecció desxifrarà tots i cadascun dels vots sortits de la barreja dels mixers.

L'eficiència dels dos paradigmes està directament lligada amb el cost de les proves de coneixement nul utilitzades i aquesta eficiència es sumament important a l'hora de donar els resultats quan abans millor. A més, les proves de coneixement nul són un component essencial per poder facilitar la auditoria del procés electoral i per tant dels resultats de la elecció. Sense ells, l'auditoria de les eleccions electròniques no es podrien equiparar a les de les eleccions tradicionals (les proves de coneixement nul es poden auditar de forma universal i són independents del software que els executa), i per tant es perdria la transparència que es té en aquestes.

En aquesta proposta de tesi es pretén estudiar i dissenyar noves proves de coneixement nul que millorin l'eficiència de les existents. Això redundaria en un increment de les possibilitats de les tecnologies de votació electrònica per a entorns amb un nombre de votants més elevat.

La propietat intel•lectual que s'obtingui del projecte es patentarà i es farà servir en productes de la companyia.