Resum

L'àrea d'anàlisi formal de protocols criptogràfics ha experimentat una gran activitat des de mitjan 80. L'objectiu és verificar protocols que utilitzen un mecanisme de xifrat per a garantir la confidencialitat i l'autenticació de les dades. Els mètodes formals han sigut utilitzats en l'anàlisi de protocols per a proporcionar proves formals de seguretat i per a descobrir errors i fluxos de seguretat que en alguns casos han romàs ocults durant molt temps després de la publicació del protocol original, com és el cas del conegut protocol Needham-Schroeder Public Key (NSPK). En aquesta tesi abordem problemes relacionats amb els tres pilars principals de la verificació de protocols: capacitats de modelatge, propietats verificables i eficiència.

Aquesta tesi està dedicada a investigar característiques avançades de l'anàlisi de protocols criptogràfics, centrant-se en l'eina Maude-NPA. Aquesta eina és un comprobador de models (model-checker) per a l'anàlisi de protocols criptogràfics que permet la incorporació de diferents teories equationals i que opera en el model de nombre il·limitat de sessions sense realitzar cap tipus d'abstracció de dades o de control.

Una contribució important d'aquesta tesi està relacionada amb aspectes teòrics de verificació de protocols en Maude-NPA. En primer lloc, definim una semàntica operacional cap a avant, usant la lògica de reescriptura com a marc teòric i el llenguatge de programació Maude com a eina de suport. Aquesta és la primera vegada que es defineix una semàntica operacional cap a avant basada en reescriptura per a Maude-NPA. En segon lloc, estudiem el problema que sorgeix en l'anàlisi de protocols criptogràfics quan és necessari garantir que determinats termes generats durant l'exploració d'estats estan en forma normal respecte a la teoria equacional del protocol.

També estudiem tècniques per a estendre les capacitats de Maude-

NPA perquè es puga verificar un ventall més ampli de protocols i de propietats de seguretat. En primer lloc, presentem un marc per a especificar i verificar composicions seqüencials de protocols en les quals un o més protocols "fill" fan ús d'informació obtinguda després d'executar un protocol "pare". En segon lloc, presentem un marc teòric per a especificar i verificar indistinguibilitat de protocols en Maude-NPA. L'objectiu d'aquest tipus de propietats és verificar que un atacant no pot distingir dues versions diferents d'un protocol: per exemple, una en la qual s'utilitza un secret i una altra en la qual s'utilitza un secret diferent, com ocorre en els protocols de vot electrònic.

Finalment, aquesta tesi contribueix a millorar l'eficiència de la verificació de protocols en Maude-NPA. Definim diverses tècniques que redueixen dràsticament l'espai de cerca generat en l'anàlisi d'un protocol, i que, sovint, permet obtenir un espai de cerca finit de tal manera que es pot decidir automàticament si la propietat de seguretat desitjada es satisfà o no, a pesar que tals problemes siguen generalment indecidibles.