Definite clauses applied to security

Prof. G.Filè[1]

[1] *University of Padova*
Department of Mathematics
Email: gilberto@math.unipd.it

Timetable: 12 hrs. Lectures on May 2014, Torre Archimede, Room 2BC/30.

Course requirements: some logic

Examination and grading: oral examination

SSD: MAT and INF/01

Aim: Show that definite clauses are a powerful tool for modelling communication protocols at different levels of complexity (with and without a notion of state)

Course contents: Preliminaries: definite clauses, unification and resolution, clauses for modelling communication protocols. Proverif study and use in laboratory. Limits of Proverif and a way to overcome them. Definite clauses used for modelling state sensitive protocols.