TITOLO: Tra la Logica e la Crittografia

PROGETTO DI RICERCA

Il progetto prevede lo studio dell'indistinguibilità computazionale, concetto chiave in ambito crittografico, dal punto di vista della logica e in particolare della logica equazionale. In particolare, si studierà la natura dell'indistinguibilità computazionale, da un lato da un punto di vista equazionale e dall'altro anche da un punto di vista metrico, definendo un sistema di prova che permetta di derivare giudizi corretti per essa.

PIANO ATTIVITA

Il laureato recrutato nel progetto si occuperà di studiare lo stato nell'arte rispetto all'indistinguibilità computazionale e ai metodi formali per essa. Si occuperà poi di definire un sistema di prova, dimostrando un teorema di correttezza per esso.