Università degli Studi di Firenze
Scuola di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Informatica
Anno Accademico 2014/2015 - Tesi di Laurea

Teoria dei Giochi e Multi-Party Computation

Laureando: *Mucci Francesco* (francesco.mucci@stud.unifi.it)
Relatore: *Boreale Michele* (michele.boreale@unifi.it)

L'obbiettivo di questo lavoro di tesi è fornire un'introduzione semplice e chiara della *Teoria dei Giochi*, illustrare il problema della *Multi-Party Computation (MPC)* e mostrare come sia possibile modellare i partecipanti ad un *protocollo MPC* in modo razionale sfruttando le nozioni della *Teoria dei Giochi*.

Il primo capitolo introduce i concetti fondamentali della *Teoria dei Giochi*: tale campo studia i modelli matematici (*giochi*) che descrivono l'interazione strategica, conflittuale e/o cooperativa, tra più soggetti intelligenti, razionali e tra loro indipendenti (*giocatori*). La struttura del capitolo è la seguente: inizialmente vengono definiti formalmente i *giochi in forma normale* e la nozione di *strategia* in tali giochi; vengono poi enunciati alcuni *concetti di soluzione* ed il capitolo si conclude analizzando tramite esempi alcuni classi di giochi.

Il secondo capitolo si pone l'obbiettivo di introdurre ed analizzare la *Multi-Party Computation (MPC, computazione a parti multiple)* sicura: essa può essere definita come il problema in cui un insieme di soggetti, ognuno avente un input segreto, desidera calcolare una certa funzione dei loro input in modo sicuro, dove per sicuro si intende, come minimo, che: (a) l'output della funzione deve essere corretto (*correttezza della computazione*) e (b) la segretezza degli input deve essere preservata (*input privacy*) anche in uno scenario in cui una parte dei giocatori è corrotta. Nel capitolo illustriamo le nozioni di sicurezza che i *protocolli MPC*, protocolli che risolvono il problema crittografico della MPC sicura, dovrebbero rispettare e mostriamo la struttura di un protocollo MPC per un caso semplice.

Nella trattazione classica del problema MPC, i partecipanti alla computazione sono identificati come onesti oppure disonesti; tuttavia, nella realtà la distinzione non è così netta: sarebbe meglio analizzare i partecipanti vedendoli come individui egoisti, razionali ed intelligenti che cercano unicamente di massimizzare i propri "guadagni". Dunque, il terzo ed ultimo capitolo, seguendo le più recenti ricerche ed introducendo concetti avanzati della Teoria dei Giochi, si occupa della costruzione un appropriato *gioco di Multi-Party Computation* in cui le parti eseguono un protocollo MPC per il calcolo di una funzione non solo da un punto di vista crittografico, ma anche dal punto di vista razionale della *Teoria dei Giochi*.