Secure Multi Party Computing

Proposta de Projeto

Orientador: Paul Crocker (DI/UBI)

1 Objetivos

(Secure)Multi-party computation (MPC) is the computation of a specified function among a set of possibly mutually distrusting parties. The goal other than correctly computing a specific function on the (possibly encrypted) data is to prevent any participant from learning with non-negligible probability any information about the inputs provided by other parties.

This project will be a study of this particular area and the various protocols that may be used. In particular the project aims to explore these protocols for fraud analysis and detection amongst a set of distributed databases that contain financial and other tax data, this is done by calculating disproportionalities and other statistical data. The exact specification of these disproportionalities will be defined by the projects partners (Unidade de Ação Fiscal da Guarda Nacional Republicana) however in this phase only synthetic data and models will be used.

There are many (open source) software's that implement MPC protocols and also semi) commercial offerings such as the Sharemind SDK. The final phase of the project will be to build a demonstrator/ proof of concept using the ShareMind API (or other) and analyse its performance.

2 Tarefas a Realizar

T1 Study of MPC protocols (0.5M
T2 Implementation of Simple MPC Protocols. (0.5M)
T3 The ShareMind API (1M)
T4 Construction of a Demonstrator/Proof of Concept. (1M)
T4 Project Report write up. (0.5M)

4 Requisitos Técnicos/Académicos

Programming Skills. Computer and Data Security. Concepts in Number Theory and Statistics.

5 Contactos

Paul Crocker (crocker@di.ubi.pt