Título: **DiPCoDing: A Differentially Private Approach for Correlated Data with Clustering**

Data: **24/10/2017** Horário: **16h** Local: **Sala de seminários – MDCC**

Resumo:

Differential privacy is a model which gives strong privacy guarantees. It was designed to make difficult to distinguish individuals' records on statistical databases while maximizing data utility. Differential privacy approaches usually assume that database records are sampled independently, i.e., each record of this database is independent of the rest. However, this assumption is not always true in the context of real-world applications. In this paper we propose DiPCoDing, a novel approach to calculate the correlation between records in statistical databases using clusterization. For this matter, we have considered Density-Based Spatial Clustering of Applications with Noise (DBSCAN) and Gaussian Mixture Model (GMM). Our method aims to group similar records, which are more likely to be correlated, to reduce the sensitivity of differential privacy and consequently the amount of noise added to the query answer, increasing data utility while providing privacy for correlated data. The experimental results of our approach showed that relative errors and noisy answers are significantly lower than those from existing works.

Banca:

- Prof. Dr. Javam de Castro Machado (MDCC/UFC - Orientador)
- Prof. Dr. José Maria Monteiro da Silva Filho (MDCC/UFC)

- Prof. Dr. José Antônio Fernandes de Macedo (MDCC/UFC)