Innovative solutions to ensure data security in the cloud using cryptographic mechanisms

The recent technological advance together with the variety of services provided by third parties have produced both a paradigm shift around security, as well as new opportunities for data monetization. The different stages in which the information resides have their own challenges, some which are addressed and others still being an open issue, such as protection of data in use. Incomplete addressing of the problem allows a growth of cyber-attacks at the border between the phases.

The goal of this thesis is to present the emerging technologies and the necessary solutions to ensure security during execution, no matter where it takes place. Firstly, homomorphic encryption schemes are addressed together with a series of contributions at the theoretical and practical level, covering topics of circuit optimization, new encryption schemes, accelerations using hardware platforms as well as concrete applications. Subsequently, secure multi-party computation is addressed where is proposed a fully decentralized authentication system using a related technology called blockchain and SMPC protocols for the distributed digital signature. Another area of contributions is the trusted execution environments where a software security module is designed, capable of emulating an HSM, based on the Intel SGX instructions set. At the end of the thesis there are mentioned several similar technologies, able to provide protection during processing.

Based on the results of this research, it can be concluded that the tools needed to protect the information through their life cycle do exist, and the emerging segment addressed leaves a great room for innovation and improvement of current solutions.