**Ph.D. in Information Technology: Thesis Defense**

**February 5th, 2021**

**online by Teams – at 11.00**

**Nicholas MAINARDI – XXXII Cycle**

From Theoretical To Real World Cryptography: Towards Practical Privacy-Preserving Outsourced Computation and Accurate Parsing of Digital Certificates

Supervisor: Prof. **Gerardo Pelosi**

**Abstract:**

The adoption of cryptographic primitives in real-world applications often poses several challenges, which involve both the security and the performance overhead of the cryptographic components. In this research, we consider two significant challenges that hinder the secure and effective adoption of two relevant cryptographic primitives: the unpractical performance overhead of privacy-preserving outsourced computation techniques; the accuracy of parsers for digital certificates. In particular, we investigate how to reduce the performance overhead of Fully Homomorphic Encryption (FHE) schemes, which are a perfect solution for privacy-preserving outsourced computation as they enable computation directly over encrypted data. We focus on two efficient FHE schemes that represented appealing solutions to reduce such performance overhead, unfortunately showing the existence of two attack techniques that completely break them. Conversely, we show that privacy-preserving outsourced computation can be made practical for some applications, designing two privacy-preserving substring search solutions with high security guarantees and low communication cost based on Partial HE schemes and Intel SGX technology, respectively. To improve the parsing accuracy for digital certificates, we propose a novel regular format for X.509 digital certificates, which enables the automatic generation of a parser with sound correctness guarantees and optimal complexities, and we thoroughly analyze the OpenPGP format, proving that it can be described by a Deterministic Context-Free grammar; nonetheless, we also show that the automatically generated parser obtained from this grammar requires a prohibitive amount of memory, which hinders the adoption of such accurate parser in OpenPGP implementations.

**PhD Committee**

Prof. **Luca O. Breveglieri**, DEIB
Prof. **Stefano Paraboschi**, Universita' di Bergamo
Prof. **Pierangela Samarati**, Universita' degli Studi di Milano