UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DOTTORATO DI RICERCA / PHD PROGRAM IN
INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Seminar announcement

Friday, April 12th, 2024; Time: 11:45 -13:15
Seminar Room, Floor I, Building 3, DIETI - Via Claudio, 21 - NAPOLI

Prof. Antonis Michalas

Tampere University, Tampere, Finland,
Department of Computing Sciences
E-mail: antonios.michalas@tuni.fi

Exploring the Frontiers of Modern Cryptography

Abstract: In the realm of modern cryptography, innovative techniques have emerged to safeguard information in diverse applications. This presentation delves into a spectrum of cutting-edge cryptographic paradigms poised to redefine the landscape of secure computation and data utilization. First, we embark on a journey through Symmetric Searchable Encryption, a paradigmatic shift enabling efficient search over encrypted data while preserving confidentiality. We unravel the intricacies of Functional Encryption, a powerful framework facilitating fine-grained access control over encrypted data, empowering selective disclosure of information to authorized entities. Continuing our exploration, we delve into the realm of Hybrid Homomorphic Encryption, a synthesis of symmetric and asymmetric encryption paradigms, enabling secure computation on encrypted data, heralding a new era of privacy-preserving computations. Subsequently, we illuminate the innovative domain of Anamorphic Encryption, where data is transformed into encrypted forms with differing dimensions, amplifying security without compromising utility. Finally, we delve into the convergence of cryptography and machine learning, exploring Privacy-Preserving Machine Learning techniques.

Lecturer short bio: Antonis Michalas is an Associate Professor at the Department of Computing Sciences at Tampere University, where he leads the Network and Information Security group (NISEC). Group members conduct research in areas spanning from the theoretical foundations of cryptography to the design and implementation of efficient and secure communication protocols. His research interests include applied cryptography, privacy-preserving protocols in widely deployed communication networks, analysis of encrypted data, privacy-preserving machine learning, cloud security and trusted computing.

For information: Prof. **Simon Pietro Romano** – spromano@unina.it *(organizer)*