General information

Università degli Studi dell'Aquila (ITALY)

- **Center of Excellence DEWS**
  Design Methodologies for Embedded controllers, Wireless interconnect and System-on-chip
  http://dews.univaq.it/

Dr. Luigi Pomante (Assistant Professor)

- **luigi.pomante@univaq.it**

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	Y
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	Y
○ Authenticated encrypted token research for mobile payment solution	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- ***Design Methodologies for Networked Embedded Systems***
  - **W**ireless **S**ensor **N**etworks & **M**obile **A**d-hoc **NET**works

- *Relevant European Projects*
  - **SAFECOP (ECSEL-JU RIA-2015)**
    Safe Cooperating Cyber-Physical Systems using Wireless Communication
  - EMC2 (Artemis-JU 2013 AIPP)
    Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable RT environments
  - CRAFTERS (Artemis-JU 2011 ASP)
    ConstRaint and Application-driven Framework for Tailoring Embedded RT Systems
  - PRESTO project (Artemis-JU 2010 ASP)
    ImProvements of industrial Real Time Embedded SysTems develOpment process
  - **VISION (FP7 "Ideas" 2009 – ERC SGA)**
    Video-oriented UWB-based Intelligent Ubiquitous Sensing

- *Relevant skills*
  - **Lightweight Cryptography, Topology-based Key Management and Certification, and Intrusion Detection Systems for WSN and resource-constrained MANET**