# CRISES: security and privacy

## DEIM (URV)

RED2018-102384-T

Red RISC-V members: C. Aliagas, M. Bamiloshin, A. Blanco, **O. Farràs**, J. Manjón, P. Millán J. Ribes.

CRISES faculty: J. Domingo-Ferrer, J. Castellà, J. M. Bras-Amorós, D. Sánchez, A. Viejo

***Contact: oriol.farras@urv.cat***

## Mission

The group mission is centered in the creation of technologies that make compatible three objectives:

- **Security** for companies, governments and individuals in the information society
- **Privacy** of the individuals who are users or passive subjects of the information society
- **Utility** of the underlying informatics systems.

## Vision

***Design cryptographic schemes and privacy-preserving mechanisms*** from different technologies in order to protect communications, perform secure computations, and preserve individuals' privacy.

## Group Profile

### Research

- **Data privacy**
- **Information-theoretic cryptography**
- **Post-quantum cryptography**
- **Vehicle security**
- **Artificial intelligence**

## Recent / Ongoing Results

- **Designing RISC-V-based Accelerators for next generation Computers (RIS3CAT-FEDER):** design, verify and create an out-of-order general purpose processor with RISC-V accelerators
- **Red-RISCV (RED2018-102384-T):** Investigación, Formación e Innovación en Sistemas RISC-V.
- **SoBigData++ ((H2020):** European Integrated Infrastructure for Social Mining and Big Data Analytics
- **CONSENT: GDPR-compliant CONSumer oriENTed IOT (RTI2018-095094-B-C21):** Privacy in IOT Technologies
- **BAnDIT: Advanced Blockchain Attacks and Defense Techniques (H2020-MSCA-ITN-2018-814284)**: Platform to test real persistent threats to BCT and assess the weaknesses of blockchain systems

### Teaching

- **Fundamentals of Computing**
- **Computer Architecture**
- **Cryptograpy and Privacy**
- **Parallel Computing**
- **Informatics, Telecomunication & Electronics** engineering degrees
- **Security and Artificial Intelligence /Computational Mathematics Masters**

- **Master courses with mixed classes : on-line (MOOC) & Classroom**
- **URV** Engineering School:
  - Computer Architecture subjects updated. Future introduction of **RISC-V design**.
  - Introduction of **hardware security** to master students

### Innovation

- **Privacy preserving mechanisms**
- **Secure implementation of cryptographic protocols and schemes**
- **Cloud computing**

- **Security & Privacy Technical Analysis in Federated Learning** (Huawei Technologies Oy Finland)
- **Secure vehicular environments** (SEAT, LEAR)
- **Hardware design for efficient implementation of Post-Quantum cryptographic schemes** (LEAR)

## Group positioning & Perspectives in front of Open-Hw & RISC-V

### R+D+i+T

- **Design secure accelerators for current cryptographic standards**
- **Design secure accelerators for post-quantum cryptographic schemes.**
- **Protection against side-channel attacks in RISC-V**

### Global Remarks

*"The new RISC-V architectures offer a valuable opportunity to enhance security protection in computers in a transparent and verifiable process. The final goal is to protect society against malicious attacks and to create a trustable computation environment.*