

# Cryptography at FFI

- History
  - Minimal activity during 2000-2014
  - Two PhD students for 2014-2018
  - Current research project ongoing from 2018
- Professional environment
  - Four researchers with background in mathematics and cryptology (two PhDs)
  - Part of a cyber security group working with i.e. prevention, detection, event management and information infrastructure
  - Cooperation with government, industry and academia

# Research interests

- Project: *Quantum safe cryptography for unmanned and autonomous devices*
  - First and foremost cryptography
  - Currently little focus on algorithms, quantum safe means symmetric
  - Integration and challenges of cryptography in unmanned and autonomous devices
- Examples of activities
  - Review of academic work
  - Review existing solutions for drones
  - Side channels and fault injections
  - Secure underwater communication (NATO)
  - Formal security modelling