Master thesis topic on a side note: Cryptology

- FFI – security clearance – interested in mathematics
- Examples
  1. **«Quantum-proof» cryptography** is under standardization. New algoriths are more secure but also more resource demanding, while at the same time they will be applied on units with few resources. This requires testing and analysis
  2. **Secure Multi-party Computation (MPC)** handler om hvordan flere parter kan gjøre beregninger eller sammenstille data uten at de nødvendigvis stoler på hverandre. Her er det aktuelt å se på både eksisterende metoder og protokoller samt mulige anvendelser.
  3. Implementation of cryptology in real systems, and how to protect against **covert channels** (time usage, power usage, EM radiation etc.)
  4. **Analysis of crypto-algorithms** is a foundation of trust. E.g. The relation between informataion and ciphertext can can be represented by a system av non-linear equations. How to represent and solve these kinds of equations?
- Contact person: Martin.Strand@ffi.no
- See also: https://www.mn.uio.no/ifi/studier/masteroppgaver/cybersecurity/