NTNU | Norwegian University of Science and Technology

Crypto @ NTNU

Norwegian Crypto Seminar 2024

NTNU Applied Cryptology Lab (NaCl)

NTNU Applied Cryptology Lab (NaCl)

Collaboration between the Department of Information Security and Communication Technology and the Department of Mathematical Sciences with members in Gjøvik and Trondheim.

We currently have 25 members (ntnu.edu/iik/nacl-lab):

- 12 permanent staff
  - (3 outgoing contracts)
- 4 postdocs
- 9 PhD candidates

We supervise 10-15 master students in cryptography each year.

Main research areas

- Post-quantum cryptography
- Key exchange and signatures
- Electronic voting schemes
- Symmetric cipher design and analysis
- Verifiable and homomorphic computation
- Multi-party/threshold cryptography
- Formal verification and computer-aided proofs
- Privacy-enhancing cryptography and data privacy

Research projects

Ongoing projects:

- Lightweight Cryptography for Future Smart Networks
- OFFPAD - Optimizing balance between high security and usability
- Secure, Usable, and Robust Cryptographic Voting Systems

Current applications:

- Centre for Research-based Innovation
- National Research Schools for Quality and Relevance

Recent graduates

- Yao Jiang (2021)
- Tjerand Silde (2022)
- Mayank Raikwar (2022)
- Shuang Wu (2022)
- Mattia Veroni (2023)
- Bor de Kock (2023)
- Morten R. Solberg (2023)
- Pia Bauspiess (2024)
- Elsie M. Fondevik (2024)
- Jonathan K. Eriksen (2024)
- Runzhi Zeng (2024)

Cryptography courses

- TTM4135 – Applied Cryptography and Network Security (BSc)
- TTM4138 – Wireless Network Security (MSc)
- TTM4205 – Secure Cryptographic Implementations (MSc)
- TTM4195 – Blockchain Technologies and Cryptocurrencies (MSc)
- TTM4536 - Advanced Ethical Hacking (MSc, Online)
- IMT4217 – Introduction to Data Privacy (MSc, Online)
- IMT4124 – Cryptology (MSc, Gjøvik)
- TMA4160 – Cryptography (MSc)
- + 4 PhD level cryptography courses (Trondheim & Gjøvik)

Upcoming event: PKC 2025

Bor de Kock and Tjerand Silde are the general co-chairs of the IACR Public Key Cryptography conference 2025, which will be held in Røros from May 12 to 15. Save the dates!

We are looking for sponsors to support the event

Website: pkc.iacr.org/2025.

THANKS!