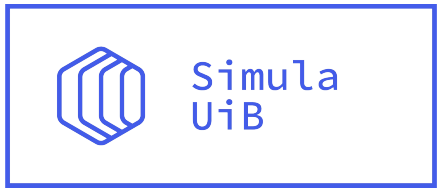
Cryptologic Research at Simula UiB

Presented at NKS'24



Who we are…

A **research institute** owned by Simula Research Lab (Oslo) and University of Bergen

Mission:

Lead in **research** and **education** in **cyber security**, especially related to disruptive technologies for secure and reliable communication and computation

Two departments: **Cryptography** and **Information Theory**

Future focus

Quantum Technologies

- quantum error correcting codes
- quantum algorithms
- quantum cryptography
- **post-quantum cryptography**

Privacy-Enhancing Technologies

- private and distributed ML / AI
- secure computation and data sharing
- fully-homomorphic encryption
- zero-knowledge proofs

Senior researchers

Eirik Rosnes

Hsuan-Yin Lin

Øyvind Ytrehus

Carlos Cid

Håvard Raddum

Martijn Stam

Information theory

Cryptography

Postdocs	1	5
PhDs	2	4

Leaving our footprints…

- **Research:** Selected publications

	Eurocrypt	PKC	Crypto	CHES	FSE	ISIT	IEEE T IT
2023	✅🪑	✅	✅	✅	✅	✅	✅
2024	✅	✅	✅			✅	✅

- **Education:** PhD graduates working at NSM, NTNU, Equinor and… Simula UiB!

- **Outreach:** Bi-annual networking event at Simula UiB:
  Tuesday 12 March 2024: Quantum Cybersecurity
  Monday 4 Nov 2024: Privacy Preserving Technology (free registration!)

ArcticCrypt 2025

ArcticCrypt 2025 will take place in Longyearbyen, Svalbard on July 6th-11th 2025

Registration opens 1 November!