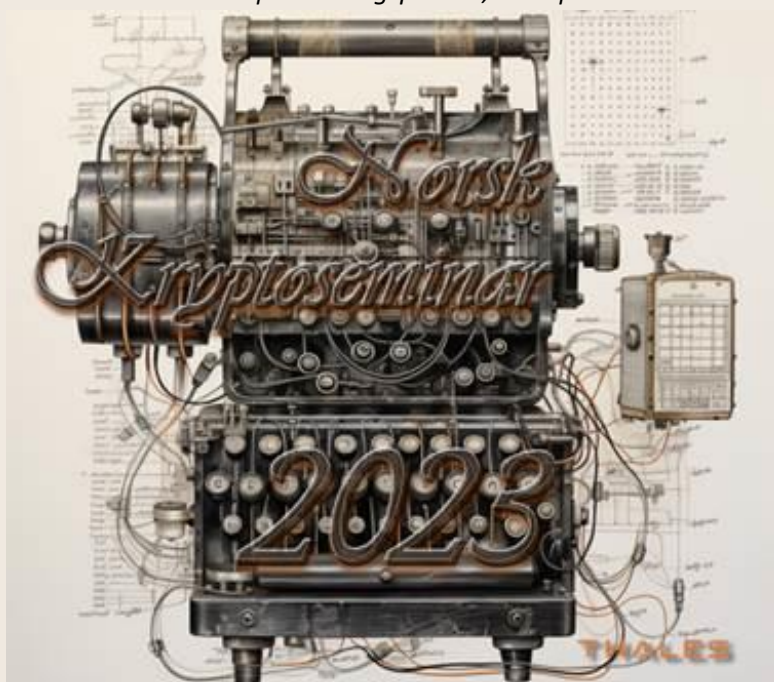


Norsk Kryptoseminar 2023

27. oktober | Forskningsparken, Oslo | kl. 09:00



[Thales Norway AS](#) ønsker velkommen til Norsk Kryptoseminar 2023. Arrangementet avholdes 27. oktober i [Forskningsparken](#) (Gaustadalléen 21, 0349 Oslo) fra kl. 08:30 til ca. 16:30-17:00.

Arrangementet har til hensikt å samle de norske kryptologimiljøene, både academia, brukere og myndigheter/forvaltning, og er åpent for alle. Foredrag holdes på engelsk, norsk eller lignende.

Program:

Tid	Tittel	
Fra 8:30	Oppmøte og registrering	
9:00	Velkommen v/ Thales	
	Hardware managed keys in Azure v/ Lars Olaussen (Bouvet)	
	Obfuscation in Software Protection v/ Anton Tkachenko (Promon)	
	PhD-bolk 1	Hagen (Ny MSc) Jesper (Ny PhD)
10:30	Pause	
11:00	Multi Party Computation i praksis v/ Martin Strand (FFI)	
	Acquiring Data from Encrypted Containers and Devices v/ Kripos-NC3	
12:00	Lunsj (60 min)	
13:00	Real-world crypto mistakes v/Tor Erling Bjørstad (Mnemonic)	
	PhD-bolk 2	Arne (Zero knowledge proofs) Amund (Reset Glitching) Caroline (Lattice-Based Electronic Voting) Anton (C-differential uniformity as a new crypto characteristic)
14:30	Pause	
15:00	PhD-bolk 3	Ole Martin (Testing the security usability of electronic ID schemes)
		Lea (Circuit Privacy in Fully Homomorphic Encryption)
		Emil (Post-Quantum stuff)
		Jonathan (Après-SQL)
	Kjent chiffer-tekst med steinhard integritet v/ Stig Frode Mjølåsnes (NTNU)	
	Avslutning/praktisk info	
Før 17:00	Slutt	