Fall 2025

Reading Group on Digital Signatures

Fall 2025			
24/09/2025	MC	**Sam Jaques**	Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions
01/10/2025	MC	**Seunghoon Lee**	Compact Lattice Signatures via Iterative Rejection Sampling
08/10/2025	MC	**Leonardo Colò**	CSI-Otter: Isogeny-based (Partially) Blind Signatures from the Class Group Action with a Twist
15/10/2025	**Reading Week**		
22/10/2025	MC	**Youcef Mokrani**	TBD
29/10/2025	MC	**Mojtaba Fadavi**	ROAST: Robust Asynchronous Schnorr Threshold Signatures
05/11/2025	MC	**Camryn Steckel**	A Note on Hybrid Signature Schemes & Bird of Prey: Practical Signature Combiners Preserving Strong Existential Unforgeability
12/11/2025	MC	**Yuheng Wen**	Seems Legit: Automated Analysis of Subtle Attacks on Protocols that Use Signatures
22/11/2025	MC	**Douglas Stebila**	Verifiable Verification in Cryptographic Protocols
26/11/2025	MC	**Maher Mamah**	The Supersingular Isogeny Path & Endomorphism ring problems with Applications to SQISign
03/12/2025	MC	**Nic Swanson**	PRISM: Simple And Compact Identification and Signatures From Large Prime Degree Isogenies
10/12/2025	MC	**Bruno Sterner**	Loquat: post-quantum Signature from, tthe legendre symbol

Organizers

Leonardo Colò University of Waterloo
Seunghoon Lee University of Waterloo