Winter 2026

Reading Group on Advanced PKEs

Winter 2026			
16/01/2026	MC	**Roman Langrehr**	Towards a Separation of Semantic and CCA Security for Public Key Encryption
23/01/2026	MC	**Sam Jaques**	Impossibility Results for Post-Compromise Security in Real-World Communication Systems
30/01/2026	MC	**Mojtaba Fadavi**	A New Lattice-Based Threshold Signature Scheme with Identifiable Aborts (IA)
06/02/2026	**Cancelled**		
13/02/2026	MC	**Youcef Mokrani**	Adaptive Attacks Against FESTA Without Input Validation or Constant-Time Implementation
20/02/2026	**Reading Week**		
27/02/2026	MC	**Jack Zhao**	Post-Quantum PKE from Unstructured Noisy Linear Algebraic Assumptions: Beyond LWE and Alekhnovich’s LPN
06/03/2026	MC	**Leonardo Colò**	IS-CUBE: An isogeny-based compact KEM using a boxed SIDH diagram
13/03/2026	MC	**Huanhuan Chen**	CCA-1 Secure Updatable Encryption with Adaptive Security
20/03/2026	MC	**Pranshu Kumar**	Generic Transformations for Updatable PKEs
27/03/2026	MC	**Mohammad Hajiabadi**	Challenges in Realizing CCA in Advanced Encryption Schemes
03/04/2026	**Good Friday**		
10/04/2026	MC	**Elnaz Hessami Pilehrood**	TBD
17/04/2026	MC	**Maggie Simmons**	Enabling FrodoKEM on Embedded Devices
17/04/2026	**End of the term lunch**		

Organizers

Leonardo Colò	University of Waterloo
Seunghoon Lee	University of Waterloo
Bruno Sterner	University of Waterloo