

DPM 2025

20th International Workshop on Data Privacy Management

Thursday 25 September 2025

09:15-09:30	Opening Welcome & Report
09:30-10:30	Keynote talk Speaker: Bart Preneel Session Chair: TBA
10:30-10:50	Coffee/Tea Break
10:50-12:25	DPM Session 1: Privacy & AI Session Chair: Ken Barker (University of Calgary)
10:50-11:10	How Worrying Are Privacy Attacks Against Machine Learning? (Josep Domingo-Ferrer)
11:10-11:30	Lost in the Averages: Reassessing Record-Specific Privacy Risk Evaluation (Yves-Alexandre de Montjoye, Natasa Krco, Matthieu Meeus, Bogdan Kulynych)
11:30-11:50	Membership Inference Attacks Beyond Overfitting (Mona Khalil, Alberto Blanco-Justicia, Najeeb Jebreel, Josep Domingo-Ferrer)
11:50-12:10	"Why is the sky blue?" – On the feasibility of privacy-friendly conversational LLM smart toys (Isabel Wagner, Valentyna Pavliv, Luigi Lazri, Jan Buechele)
12:10-12:25	Win-k: Improved Membership Inference Attacks on Small Language Models (M. Emre Gursoy, Roya Arkhammadova, Hosein Madadi Tamar)
12:25-13:50	Lunch Break
13:50-15:20	DPM Session 2: Applied Cryptography & statistics Session Chair: Guillermo Navarro-Arribas (Universitat Autònoma de Barcelona)
13:50-14:10	Advanced Electronic Signatures and GDPR: Reconciling the Concepts (Miroslaw Kutylowski, Paweł Kostkiewicz, Gabriel Wechta)
14:10-14:30	Invisible Encryption (Shahzad Ahmad, Stefan Rass, Zahra Seyedi)
14:30-14:45	Eliminating Exponential Key Growth in PRG-Based Distributed Point Functions (Marc Damie, Florian Hahn, Andreas Peter, Jan Ramon)

14:45-15:00	<i>A Pseudo-Inverse Matrix-Based LDP for High-Dimensional Data</i> (<i>Hiroaki Kikuchi</i>)
15:00-15:20	Using Prior Knowledge to Improve GANs for Tabular Data Without Compromising Privacy (Sonakshi Garg, Marcel Neunhoeffer, Jörg Drechsler, Vicenc Torra)
15:20-15:40	Coffee/Tea Break
15:40-16:55	DPM Session 3: Applications <i>Session Chair: Joaquin Garcia-Alfaro (Institute Polytechnique de Paris)</i>
15:40-16:00	Lessons from a Robotaxi: Challenges in Selecting Privacy-Enhancing Technologies (Sebastian Pape, Ala'A Al-Momani, David Balenson, Christoph Bösch, Zoltán Ádám Mann, Jonathan Petit)
16:00-16:20	Performance Analysis of Lightweight Transformer Models for Healthcare Application Privacy Threat Detection (Jude Ameh, Abayomi Otebolaku, Alex Shenfield, Augustine Ikpehai, Dauda Sule)
16:20-16:40	The Bitter Pill: Tracking and Remarketing on EU Pharmacy Websites (Zahra Moti, Kimberley Frings, Christine Utz, Frederik Zuiderveen Borgesius, Gunes Acar)
16:40-16:55	PADOME: Adaptive Privacy Assistant for the Internet of Things (Edward Rochester, Ken Barker)