

DPM 2025

20th International Workshop on Data Privacy Management

Thursday, 25 September 2025

Opening

09:15 – 09:30 “Opening & Welcome”

Keynote

Chair: TBA

09:30 – 10:30 “Privacy: Technology and Policy” *Speaker: Bart Preneel*

Coffee Break

10:30 – 10:50 Coffee/Tea Break

Session 1: Privacy & AI

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

Lunch Break

12:25 – 13:50 Lunch Break

Session 2: Applied Cryptography & Statistics

Chair: Guillermo Navarro-Arribas (Universitat Autònoma de Barcelona)

13:50 – 14:10 “Advanced Electronic Signatures and GDPR: Reconciling the Concepts”

Mirosław Kutylowski, Paweł Kostkiewicz, Gabriel Wechta

14:10 – 14:30 “Invisible Encryption”

Shahzad Ahmad, Stefan Rass, Zahra Seyed

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 “A Pseudo-Inverse Matrix-Based LDP for High-Dimensional Data”

Hiroaki Kikuchi

15:00 – 15:20 “Using Prior Knowledge to Improve GANs for Tabular Data Without Compromising Privacy”

Sonakshi Garg, Marcel Neunhoeffler, Jörg Drechsler, Vicenç Torra

Coffee Break

15:20 – 15:40 Coffee/Tea Break

Session 3: Applications

Chair: Joaquin Garcia-Alfaro (Institut Polytechnique de Paris)

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