$$H(x) = \sum_x p(x)\log\left(\frac{1}{p(x)}\right)$$

CALL FOR PAPERS

Protect-IT’25 as a part of ACM AsiaCCS 2025

2nd Workshop on Security, Privacy and Information Theory
August 26, 2025 Hanoi, Vietnam

Scope and topics of interest

Protect-IT focuses on the security and privacy of machine learning (ML) from an information-theoretic standpoint. ML systems rely on extensive datasets, often containing sensitive personal information, posing a threat to user privacy and security. Protect-IT aims to bring together experts in machine learning, (algorithmic) fairness and information theory to explore, develop, and evaluate privacy, security, and fairness attacks against ML algorithms along with defense strategies to counter them.

- Information leakage, data correlation
- Defining and quantifying privacy
- Differential privacy and private data analysis
- Machine learning and privacy
- Transparency, robustness and abuse in privacy systems
- Information theoretic foundations of security and privacy

- Cryptographic tools for privacy
- Algorithmic fairness
- Adversarial learning
- Intrusion detection
- Privacy and security attacks and defenses

Submission Instructions

We welcome two types of submissions: full papers of maximum 12 pages or extended abstracts up to 4 pages. Full papers of work that is new to the community of data privacy, security and information theory must be unpublished elsewhere and will appear in **ACM digital library as workshop proceedings**. Extended abstracts can be previously published or currently under review elsewhere and will **not** be included in proceedings. All submissions must adhere the latest ACM Sigconf style conference template. We also welcome recently published studies as well as unpublished recent results in privacy and security venues **only** as poster submissions.

Poster Instructions

To encourage one to one exchanges, we welcome poster submissions of recent results and all accepted full paper submissions will have a slot at the poster session (poster size A0 (841 × 1189 mm).

Important Dates

Submission deadline: February 21, 2025, 23:59 (Anywhere on Earth)
Notification of acceptance: April 8, 2025

Technical Program Committee

- Josep Domingo-Ferrer, Universitat Rovira i Virgili
- Aurélien Bellet, Inria
- Emre Gürsoy, Koç University
- Weizhi Meng, Lancaster University
- Parastoo Sadeghi, UNSW Canberra
- Tobias Oechtering, KTH Royal Institute of Technology
- Thorsten Strufe, Karlsruhe Institute of Technology
- Vicenç Torra, Umea University

Organizers

Workshop Chairs

- Ayşe Ünsal, EURECOM, France
- Javier Parra-Arnau, Universitat Politècnica de Catalunya, Spain
- Natasha Fernandes, Macquarie University, Australia

Protect-IT’25
webpage

LaTeX TikZposter