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

CALL FOR PAPERS

Protect-IT'24 as a part of IEEE CSF 2024

1st Workshop on Security, Privacy and Information Theory
July 8, 2024 Enschede-The Netherlands

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 cryptography, (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
- Cryptographic tools for privacy
- Machine learning and privacy
- Transparency, robustness and abuse in privacy systems
- Information theoretic foundations of security and privacy
- Algorithmic fairness
- Adversarial learning
- Intrusion detection
- Abstract attacks on privacy
- Security attacks and defenses

Submission Instructions

We welcome two types of submissions: extended abstracts and posters. Extended abstracts must be at most 4 pages long excluding references and adhere to the CSF format. We encourage submissions of work that is new to the community of data privacy, security and information theory in addition to submissions which are currently under review elsewhere or recently published in privacy and security venues. The workshop ***will not*** have formal proceedings, but authors of accepted abstracts can choose to publish their work on the workshop's webpage or to provide a link to arXiv.

Poster Instructions

All accepted papers have a slot at the poster session for posters with size no bigger than A0 (841 × 1189 mm).

Important Dates

Submission deadline: May 4, 2024, 23:59 (Anywhere on Earth)
Notification of acceptance: June 4, 2024

Organizers

Workshop Chairs

- Ayşe Ünsal, EURECOM
- Javier Parra-Arnau, Universitat Politècnica de Catalunya

Publications Chair

- Melek Önen, EURECOM

Technical Program Committee

- Josep Domingo-Ferrer, University of Rovira i Virgili
- Aurélien Bellet, INRIA
- Sébastien Gambs, Université du Québec à Montréal
- Cédric Gouy-Pailler, CEA
- Emre Gürsoy, Koç University
- Arun Padakandla, EURECOM
- Vicenç Torra, Umeå University
- Weihzi Meng, Technical University of Denmark
- Jan Ramon, INRIA

Protect-IT'24 webpage