IEEE BITS | The Information Theory Magazine

Special Issue on Privacy and Security

Call for Papers

Scope and Motivation

The large-scale use of data in many areas, including in machine learning, bring new challenges to security and privacy. This data is increasingly sensitive as it could relate to personal data, but without its use, building modern-scale learning models is difficult. Though security and privacy have a long history, the scale and types of data and its uses give rise to several new theoretical and algorithmic questions. Information theory gives a rigorous framework for powerful security and privacy guarantees without computational assumptions. Ideas from information theory have influenced developments in cryptography and privacy, and many of these ideas are starting to be deployed at wide-scale. Information theory not only can give guarantees, it also suggests secure/private algorithms, as well as gives a framework to understand important tradeoffs, such as in performance versus security/privacy and other constraints (such as communication).

Given the rapid recent developments of ideas in security and privacy, and its importance in modern day information systems, this special issue explores the recent developments in security and privacy from an information theoretic perspective. The goal of this special issue is not only to capture the recent exciting developments but also attempt to frame important research questions in these domains for the coming years. Therefore we invite expository articles on the following topics of interest (not a comprehensive or exclusive list):

- Secure interactive (multi-party) communication and computation
- Information theoretic bounds and analysis for differential privacy
- Privacy and personalization
- Security and privacy for distributed and federated learning
- Auditing: privacy and security
- Security, privacy, safety and alignment in large-language models
- High-dimensional robust statistics and robust learning
- Secure and private online learning
- Security and privacy in sensing and cyber-physical systems
- Theoretical foundations for trusted execution environments
- Decentralized trust and blockchains
- Quantum cryptography
- Post-quantum cryptography

BITS Submission Instructions

We will follow the BITS two-stage submission process outlined below and described in BITS Information for Authors at www.itsoc.org/bits/information-authors

White Paper: Prospective authors should submit a white paper (limited to three pages single column 11-point font size) containing manuscript title, motivation and significance, outline, representative references, and the author list with contact information and short bios. The submission is via Manuscript central per the above link. Full articles will be invited based on the review of white papers.

Full Articles: The full article must be of tutorial/overview/survey nature, accessible to a broad audience, and have significant relevance to the scope of the Special Issue. The full article would have up to 12 double-column pages including references, 11-point font size, at least one figure (to be hosted on the website), up to 30 references, at least 1.25" margin on the left and right sides, and 1" margin from top and bottom. The articles should not have been published or be under review elsewhere.

Revised Relevant Dates

White paper submission:	June 10, 2024
Manuscript invitation:	June 30, 2024
Manuscript submission:	Aug 15, 2024
Manuscript reviews:	September 20, 2024
Manuscript final version:	December 15, 2024
Special Issue publication:	December 2024

Special Issue Editors

Suhas Diggavi, UCLA
Giulia Fanti, Carnegie Mellon University
Peter Kairouz, Google Research
Sewoong Oh, University of Washington
Vinod Prabhakaran, TIFR
Lalitha Sankar, Arizona State University