Data Privacy: The Land Where Average Cases Don’t Exist and Assumptions Quickly Perish

Olga Ohrimenko ✉ 🏠

The University of Melbourne, Australia

Abstract

Machine learning on personal and sensitive data raises serious privacy concerns and creates potential for inadvertent information leakage (e.g., extraction of private messages or images from generative models). However, incorporating analysis of such data in decision making can benefit individuals and society at large (e.g., in healthcare). To strike a balance between these two conflicting objectives, one must ensure that data analysis with strong confidentiality guarantees is deployed and securely implemented.

Differential privacy (DP) is emerging as a leading framework for analyzing data while maintaining mathematical privacy guarantees. Although it has seen some real-world deployment (e.g., by Apple, Microsoft, and Google), such instances remain limited and are often constrained to specific scenarios. Why?

In this talk, I argue that part of the challenge lies in the assumptions DP makes about its deployment environment. By examining several DP systems and their assumptions, I demonstrate how private information can be extracted using, for example, side-channel information or the ability to rewind system’s state. I then give an overview of efficient algorithms and protocols to realize these assumptions and ensure secure deployment of differential privacy.

2012 ACM Subject Classification Security and privacy → Systems security; Security and privacy → Privacy-preserving protocols; Security and privacy → Hardware attacks and countermeasures

Keywords and phrases Differential privacy, side-channel attacks, trusted execution environment, privacy budget, state continuity

Digital Object Identifier 10.4230/LIPIcs.ISAAC.2024.2

Category Invited Talk

35th International Symposium on Algorithms and Computation (ISAAC 2024).
Editors: Julián Mestre and Anthony Wirth; Article No. 2; pp. 2:1–2:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany