Ciências ULisboa | Informática

Talks@DI

Wednesday

19

Feb

2025

Private Information Retrieval Protocols for Simple (and Less Simple) Databases

Speaker

Alex Davidson

Affiliation

DI/FCUL

When

February 19th, 14h00

Where

6.3.27

Abstract

In this talk, I will introduce the focus of my investigation within the study of modern cryptography, as seen through the lens of today's methods of communication. In particular, I will highlight the core security properties we expect from cryptographic mechanisms, and how we argue security even in scenarios where adversaries have access to all the computing power in the world. I will then highlight some of my recent work towards building practical mechanisms for being able to privately retrieve data from large, online databases, without revealing the queries being made. Finally, I will highlight existing applications using such tools in the wild, as well as open scientific problems in this area, and avenues for future work.

Short bio

Alex Davidson is an Assistant Professor in the Departments of Informatics of the Faculty of Sciences at the University of Lisbon, and an integrated member of the LASIGE research centre. His research is broadly situated within the field of cryptography, the mathematical study of secure communication. His recent research has focused on the development of frameworks for privacy-preserving retrieval of data from online databases, large-scale comparisons and aggregations of sensitive datapoints, and online mechanisms for evaluating reputation of individuals without revealing personally identifiable traits or characteristics. Since completing his PhD studies (Information Security Group, Royal Holloway, University of London, 2014-2019), he has undertaken subsequent periods of scientific investigation in both industry (Cloudflare 2018-2020, Brave 2021-2022) and academia (post-doc @ LIP 2020-2021, Assistant Professor @ NOVA FCT 2023-2024).