



DIPARTIMENTO  
DI INFORMATICA  
**SAPIENZA**  
UNIVERSITÀ DI ROMA

## **DISTINGUISHED LECTURE**



**Lecturer:** Prof. Alessandro Chiesa  
(University of California, Berkeley)

**Title:** From Zero Knowledge to  
Private Transactions

**Location:** [Zoom meeting](#)

**Date:** February 24, 2021

**Time:** 17.00-18.00 (CET)

**Abstract:** The integrity of digital currencies such as Bitcoin rests on the fact that every payment is broadcast in plaintext. This fails to provide any meaningful privacy guarantees for users. In this talk I will explain how a beautiful cryptographic tool, zero knowledge proofs, can be used to design digital currencies that provide strong privacy guarantees for users. These ideas have been deployed in the wild, as part of the cryptocurrency Zcash and in several other settings.