北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
青 年 讲 座

Oblivious zero-knowledge and the ROS problem

Dr. Michele Orrù

Assistant Professor
CNRS

Host：刘天任 助理教授
2026年3月11日 星期三 15:00
静园五院204室

Abstract

Schnorr’s blind signatures, introduced over 30 years ago, lie at the core of many modern cryptographic protocols. In concurrent settings, the security of many such constructions rely on a computational assumption known as ROS (Random Inhomogeneities in an Overdetermined Solvable system of linear equations), whose hardness was already questioned by Schnorr himself (Schnorr ’01).

In this talk, we present an efficient algorithm that solves the ROS problem, thereby breaking the security of Schnorr blind signatures in polynomial time whenever more than $\ell > \log p$ parallel sessions are allowed.

Our attack translates into practical breaks of several constructions proposed in the literature, including multisignatures, threshold signatures, zero-knowledge protocols, e-cash systems, and electronic voting schemes.

Finally, we introduce a fix that extends blind issuance to Σ-protocols for discrete-logarithm representations with AND-composition, resolving an open problem left by the seminal work of Camenisch and Stadler (1997).

Biography

Michele Orrù is a chargé de recherche (assistant professor) at CNRS in Paris, France. His research seeks to build authentication mechanisms that preserve user anonymity and confidentiality. Prior to that, he was a research scholar at UC Berkeley, and he got his PhD from École Normale Supérieure. In the past, he has contributed to several open-source projects including Python and Debian.