Bocconi

24 JANUARY 2024
11:30 PM

Bocconi University
Room 3-E4-SR03
Via Röntgen 1, Milano (3° floor)

On Two-Witness Blind Signatures

Speaker

Julia Kastne
Phd Student working on Cryptography
EHT Zurich

Abstract

Blind signatures are a cryptographic primitive that allow a signer to issue signatures to a user without learning the message it signs. Among their applications are electronic cash, electronic voting and anonymous credentials.

In this talk, I will show a proof technique for proving the security of a subclass of blind signatures that have an "alternative secret key" that can be used in a security reduction. I will also discuss limitations of the proof technique, some alternatives, and open questions in the area.

The talk is based on joint works with Julian Loss, Omar Renawi, and Jiayu Xu.

Università Bocconi
DEPARTMENT OF COMPUTING SCIENCES