

# Colloquium d'Informatique de l'UPMC Sorbonne Universités

## Proof, Secrets and Computation



Silvio Micali

Amphi 25

4, place Jussieu  
75005 Paris  
Metro Jussieu

26 Mai 2015  
à 18h00

We show how Theory of Computation has revolutionized our millenary notion of a proof, revealing its unexpected applications to our new digital world.

In particular, we shall demonstrate how interaction can make proofs much easier to verify, dramatically limit the amount of knowledge released, and yield the most secure identification schemes to date.

Silvio Micali has received his Laurea in Mathematics from the University of Rome, and his PhD in Computer Science from the University of California at Berkeley. Since 1983 he has been a member of the MIT faculty, in Electrical Engineering and Computer Science Department, where is currently is the Associate Department Haeaad.

Silvio's research interests are cryptography, zero knowledge, pseudo-random generation, secure protocols, and mechanism design.

Silvio has received the Turing Award, the Gödel Prize, and the RSA prize. He is a member of the National Academy of Sciences, the National Academy of Engineering, and the American Academy of Arts and Sciences.

contact : [colloquium@lip6.fr](mailto:colloquium@lip6.fr)

<http://colloquium.lip6.fr>

Vidéo disponible sur le site

