Panel: Crypto for Security and Privacy

Daniel J. Bernstein
University of Illinois at Chicago
Technische Universiteit Eindhoven

Matthew Green
Johns Hopkins University

Tanja Lange (moderator)
Technische Universiteit Eindhoven

Nick Mathewson
Tor Project

Zooko Wilcox-O'Hearn
Tahoe LAFS

Panel motivation

Right now real-world communication security and privacy are a mess, not only (but also) because of crypto. Most web pages serve http instead of https; CAs have been compromised; and users store their data unencrypted in Dropbox.

- Can this be improved within the existing framework?
- Do we need completely new approaches at the expense of breaking compatibility?
- What are the most urgent problems?
- What are the most urgent problems where cryptographers can take action?