Elliptic Curve Cryptography and Applications

Kristin Lauter from Microsoft Research and University of Washington

In the last 25 years, Elliptic Curve Cryptography has become a mainstream primitive for cryptographic protocols and applications. This talk will give a survey of elliptic curve cryptography and its applications, including applications of pairing-based cryptography which are built with elliptic curves. No prior knowledge about elliptic curves is required for this talk. One of the information-theoretic applications I will cover is a solution to prevent pollution attacks in content distribution networks which use network coding to achieve optimal throughput. One solution is based on a pairing-based signature scheme using elliptic curves. I will also discuss some applications to privacy of electronic medical records, and implications for secure and private cloud storage and cloud computing.

Related Links:
Pacific Institute for the Mathematical Sciences
Event Type:
- Colloquia

Event Subcalendar:
- UW-PIMS Colloquium

Department of Mathematics
University of Washington

Administrative Office
C-138 Padelford
Box 354350
Seattle, WA 98195-4350
Phone: (206) 543-1150
Fax: (206) 543-0397

For all academic inquiries, please contact:

Math Student Services
C-36 Padelford
Phone: (206) 543-6830
Fax: (206) 616-6974
advising@math.washington.edu

Privacy
Terms
Site Map
Alumni Update
Contact Us

Source URL: https://math.washington.edu/events/2012-01-13/video-kristin-lauter-microsoft-research-and-university-washington