

# Hash<sup>3</sup>: Proofs, Analysis, and Implementation

ECRYPT II Event on Hash Functions



November 16-20, Tenerife, Spain

## Event Announcement

<http://www.ecrypt.eu.org/workshops.html>

The ECRYPT II event “Hash<sup>3</sup>: Proofs, Analysis, and Implementation” is a meeting that aims at bringing together people from various fields of hash functions research.

### Outline

- 3.5 days of lectures on state of the art in cryptographic hash functions
- 1.5 days of discussions and brainstorming in smaller groups (limited number of attendees)

### Tentative list of topics

- Definitions, Implications, Separations, Preservation
- Possibilities (based on ideal blockciphers and permutations)
- Impossibilities (in above model)
- Indifferentiability
- Analysis of stream-based hashes
- Rebound cryptanalysis
- Analysis techniques for AXR and MD4-like designs
- Dedicated preimage attacks
- Software efficiency
- Hardware efficiency
- Implementation techniques for software
- Implementation techniques for hardware

### List of speakers

- to be announced soon

### Organizers

- Tanja Lange
- Bart Preneel
- Christian Rechberger
- Martijn Stam

**ECRYPT II**  
↑ ↓ ↻ ↺ ↻ ↻ ↻ ↻ ↻

---