

Crypto 2013: Program Committee Report

co-Chairs:

Ran Canetti(Chair)

Juan Garay(co-Chair)

Numbers

- **61 accepted papers:**
 - **MPC/2PC: (theory & practice) 16**
 - **Fancy asymmetric encryption & friends: 14**
 - **Cryptanalysis: 8**
 - **Symmetric encryption: 7**
 - **Foundations (complex. & NT): 4**
 - **Quantum: 4**
 - **Other protocols: 3**
 - **Signatures: 3**
 - **New primitives: 2**

Review process

- **Initial reviews**
 - 3 reviews per paper
 - 4 for PC member papers
- **Rebuttal phase**
 - Authors received the reviews and could comment
- **Extensive discussions & extra reviews**
- **Physical PC meeting**

New this year

- **More accepted papers**
(61, compare with: 48 in 2012,
42 in 2011,
39 in 2010,
38 in 2009)
- **Rebuttal phase**
 - Allow authors to comment on reviews
 - Help clarify issues and discount erroneous reviews
- **Best Young Author Paper Award**
 - More awards are good: helps researchers in the community
 - Give awards to authors in early stages of career
 - Promote independent research by young authors

Not new this year

Kept with single sessions

- **Cons:**

- Away with free afternoons (tue/thu)
- Dense program, 20 minute talks

- **Pros:**

- Everyone together, no hopping
- Choose your own subset of talks to attend
- All talks equal

Preserving credit of submissions

Had several issues:

- **PC members and external reviewers had ongoing work related to submitted papers: Hard to not be influenced**
- **Had to reject some papers even when some of the contents overlaps with accepted papers.**

Preserving credit of submissions

Had several issues:

- **PC members and external reviewers had ongoing work related to submitted papers: Hard to not be influenced**
- **Had to reject some papers even when some of the contents overlaps with accepted papers.**

Personal advice: Post your work on eprint before submitting!