Crypto 2014
Program Co-Chairs Report

Juan Garay (Yahoo Labs)
Rosario Gennaro (City College, CUNY)

Program Committee

Yevgeniy Dodis
Orr Dunkelman
Serge Fehr
Pierre-Alain Fouque
Craig Gentry
Vipul Goyal
Nadia Heninger
Thomas Holenstein
Yuval Ishai
Dimitar Jetchev
Aggelos Kiayias
Kaoru Kurosawa
Alexander May
Ilya Mironov
Payman Mohassel
Jörn Müller-Quade
Maria Naya-Plasencia
Claudio Orlandi
Rafael Pass
Chris Peikert
KrzysztofPietrzak
Leonid Reyzin
Ron Rivest
Amit Sahai
Gil Segev
Elaine Shi
Tom Shrimpton
Alice Silverberg
Marc Stevens
Katsuyuki Takashima
Stefano Tessaro
Vinod Vaikuntanathan
Gilles Van Assche
Muthu Venkitasubramaniam
Ivan Visconti
Bogdan Warinschi
Brent Waters
Vassilis Zikas

YAHOO!

Numbers

- Accepted papers: **60** (/227 = .264)
- Previous years:
  - 2013: **61**
  - 2012: **48**
  - 2011: **42**
  - 2010: **39**

YAHOO!

Accepted Papers by Category

- Secure Computation & Friends (theory & impl.): **14**
- Foundations of Computational Hardness: **9**
  - *Obfuscation*
- Asymm. Encryption and Signatures: **8**
- Cryptanalysis: **7**
- Number Theory & Lattices: **5**
- Symm. Encryption and Authentication: **4**
- Side Channels and Leakage: **4**
- Information-Theoretic Security: **3**
- Key Exchange and Secure Comm.: **2**
- Quantum: **2**
- Formal Methods: **1**

YAHOO!

Review Process

- Initial reviews
  - 3 reviews per paper
  - 4 for PC member papers
- Rebuttal phase
  - Authors received the reviews and could comment
  - Allows authors to comment on reviews
  - Helps clarify issues and discount erroneous reviews
- Extensive discussions & additional reviews
- Physical PC meeting

YAHOO!

The Conference

- No BPA, no BYPA
- Stuck to single sessions
  - Dense program, shorter talks, no free afternoon(s)
  - Alternative: *partially* parallel sessions
  - Community would benefit from attending all talks (?)
- “Topical” program structure

YAHOO!

Academic Credit, Precedence & Other Issues

- PC members and external reviewers had ongoing: Hard to not be influenced
  - Posting on ePrint helps
- Had to reject some papers even when contents overlap with accepted papers
- PC members submissions

YAHOO!

Thanks!