IACR Membership Meeting
Eurocrypt 2013, Athens, Greece

Bart Preneel

presidentHEREATiacr.org

http://www.iacr.org

Agenda

- About IACR & Your Board
- Membership & Elections
- Financial Report
- Conferences & Workshops
- IACR Fellows
- Publications
- Current Board Activities
- Open Discussion

About IACR

- Non-profit organisation registered in the USA

- The Association's purposes are "to advance the theory and practice of cryptology and related fields, and to promote the interests of its members with respect thereto, and to serve the public welfare"

Delivering

- Eurocrypt, Crypto, Asiacrypt
- FSE, PKC, CHES, TCC
- Journal of Cryptology and newsletter
- IACR archive of past proceedings
  - http://www.iacr.org/archive
- ePrint server
  - http://eprint.iacr.org/

About IACR

- Run by a Board of Directors
  - 4 elected Officers
  - 9 elected Directors
  - 6 General Chairs
- Supported by
  - JoC editor in Chief, Membership Secretary, Archivist, Database Administrator
  - representatives of Asiacrypt, PKC, FSE, CHES & TCC Steering Committees

Your Board ('13)

OFFICERS

- Bart Preneel
- Christian Cachin
- Martijn Stam
- Greg Rose

DIRECTORS

- Michel Abdalla
- Josh Benaloh
- Tom Berson
- Shai Halevi
- Anna Lysyanskaya
- Matsuru Matsui
- Christof Paar
- David Pointcheval
- Nigel Smart

Your Board ('13)

APPOINTEES

- Matt Franklin
- abhi shelat
- Kevin McCurley
- Hilarie Orman
- Christopher Wolf

GENERAL CHAIRS

- Aggelos Kiayias
- Helena Handschuh
- Satyanarayana V. Lokam
- Gregor Leander
- Alexandra Boldyreva
- D.J. Guan

STEERING COMMITTEE REPRESENTATIVES

- San Ling
- Jean-Jacques Quisquater
- (Bart Preneel)
- (David Pointcheval)

Membership

- By attending this conference, you will become a member of IACR for 2014
- If you attended one of our conferences or workshops last year, you are already a member for 2013

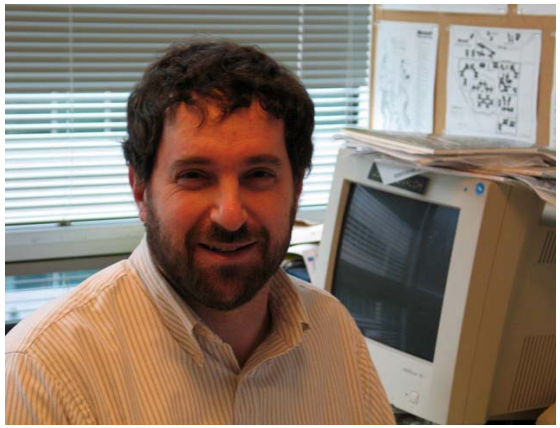
IACR Election

- There is an election for Board members every year in the Fall
  - At the end of 2013 the terms of the 4 officers and 3 elected Directors expire
  - we are actively seeking interested members to join the Board
  - please contact any Board member (or a member of the 2013 Election Committee) if you would like to know more, or are interested in standing for election

IACR Election Committee 2013

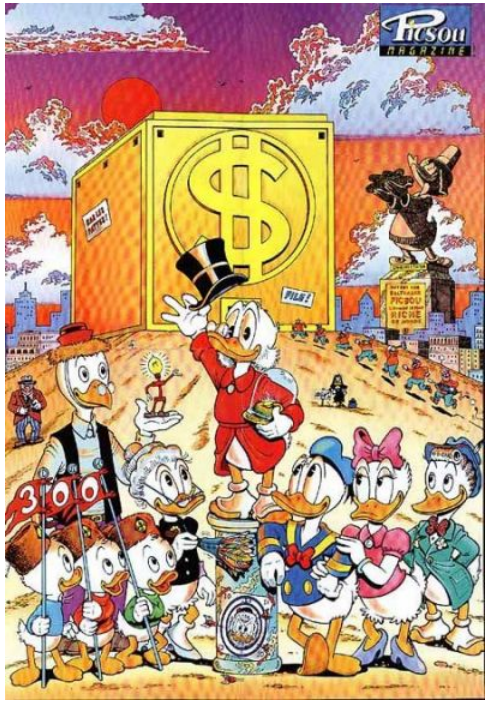
Michel Abdalla

Josh Benaloh



Tom Berson

IACR Preliminary Financial Report 2013



Greg Rose

treasurer@iacr.org

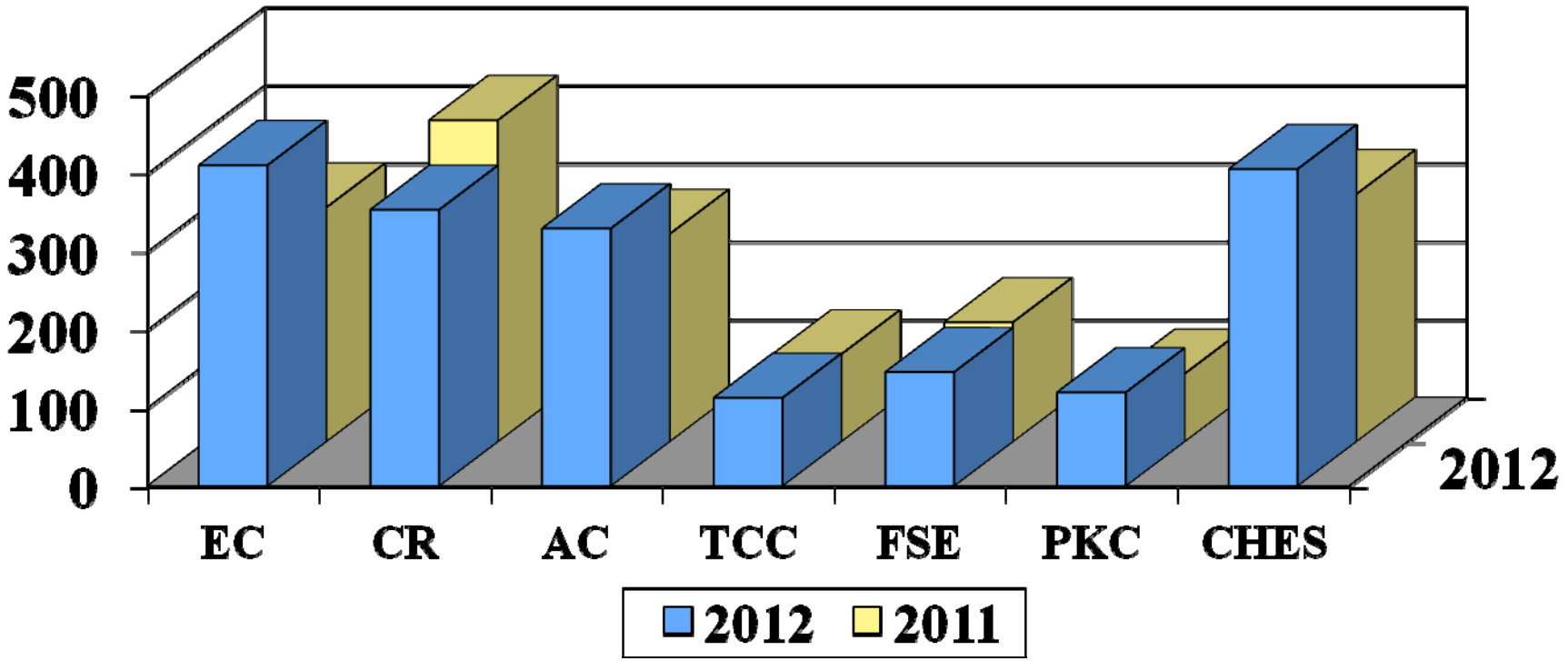
Financial Summary - 2012

- US economy recovering, European? Asian?
- Financial support from sponsoring organisations increasing greatly, maybe due to recruiting?

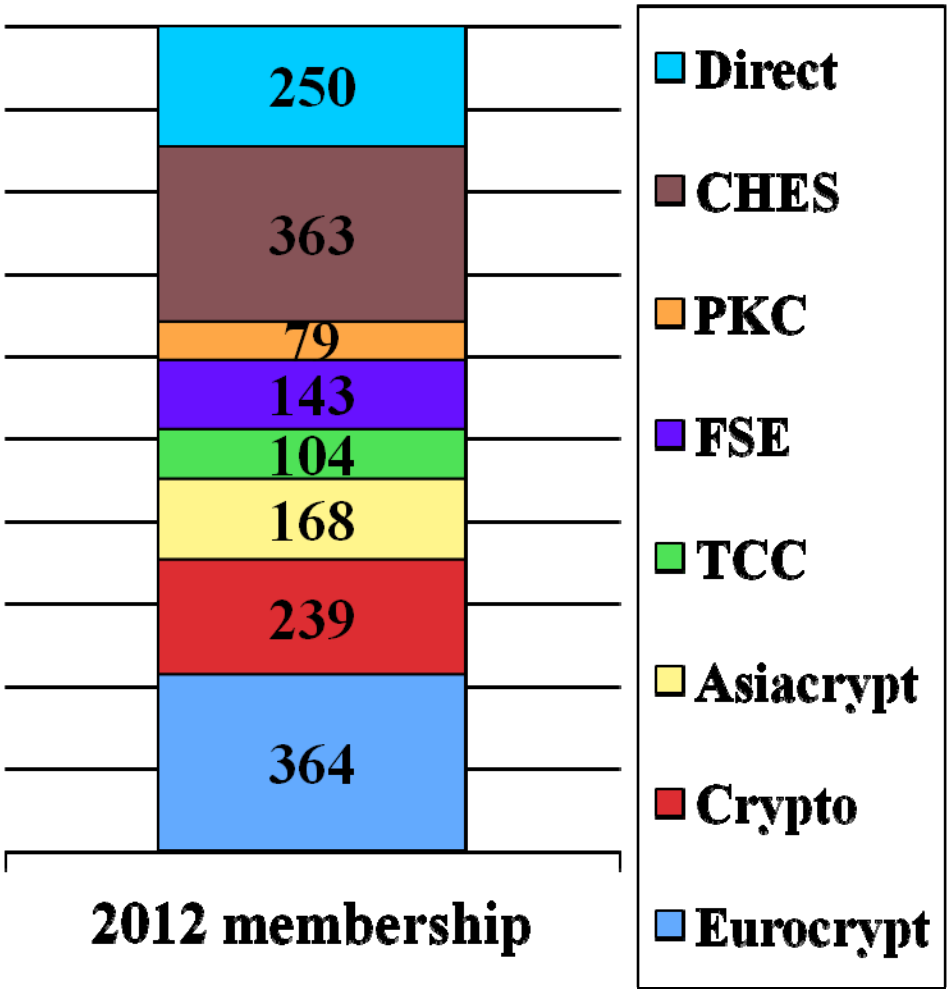
- Attendance at our events stable or up, except Crypto
  - PKC(87->120)
  - TCC(112->113),
  - FSE(153->146)
  - CHES(317->406)
  - Crypto (412->354),
  - Eurocrypt, (300->411)
  - Asiacrypt (266->330)

- Extremely low administration overhead : < 2%

2010-12 Conferences and Workshops



2012 Membership

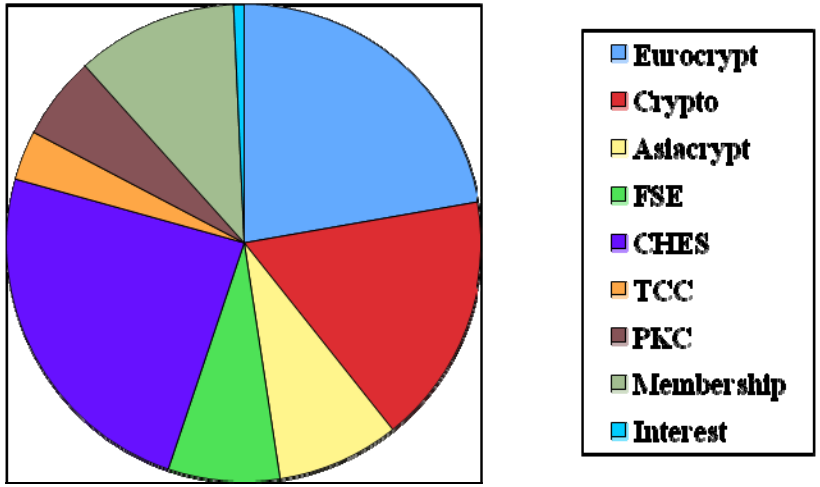


2013 Membership fees collected in 2012:

- Conferences and Workshops
- Directly through IACR
- Now US$70/35 -- Maybe decrease?
- 1710 up 12%

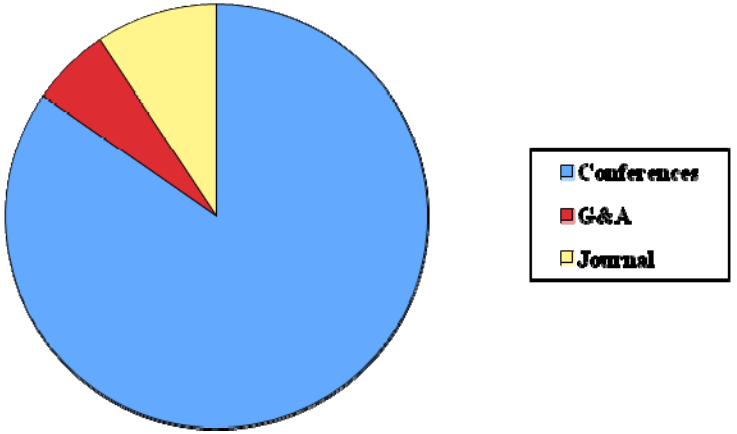
Profit & Loss Y2012 (not final)

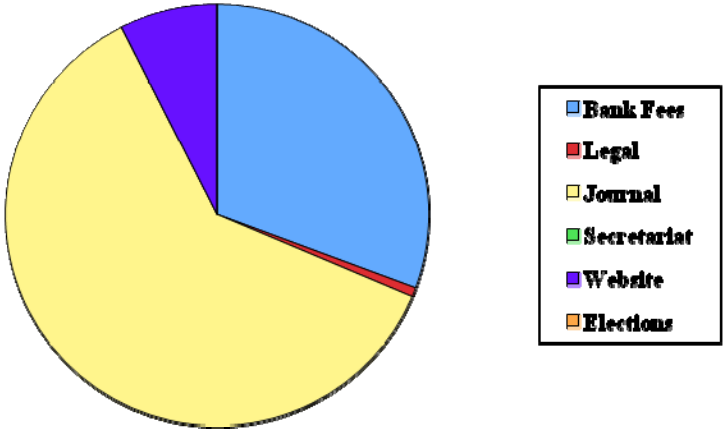
Income (936k$)



Expenses (764k$)

G&A (16k$)





2012 Highlights + Fee

- Marconi grant has run out but sponsorships increasing
  - Thanks Ron Rivest!
  - Board agrees to subsidize students in budget process
- Target break-even (or slight loss) budgets
- Keep minimal overhead - less than 2%

- Three proposals for membership fee:
  - A. keep US$ 70/35 and charge US$ 20 extra for paper copies of Journal of Cryptology
  - B. reduce to US$ 50/25 and charge US$ 20 extra for paper copies of Journal of Cryptology
  - C. keep $70/35 US dollars

- Conclusion of discussion + vote: Option B

Questions for the Treasurer

IACR Membership

2013

abhi shelat

iacrmemHEREATiacr.org

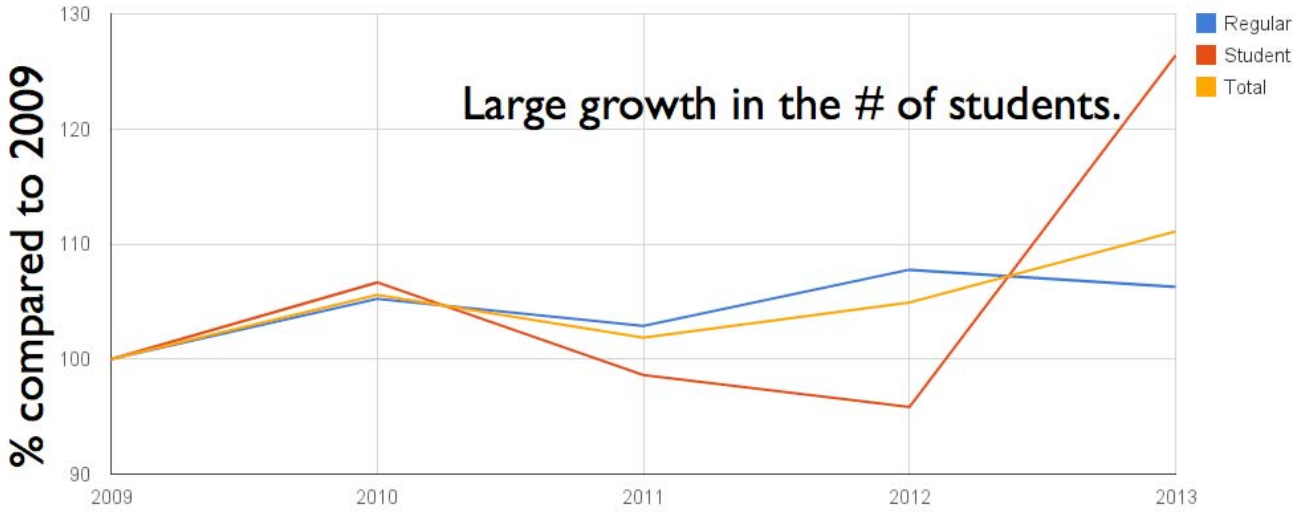
2013

1673 Members

1218 Regular+

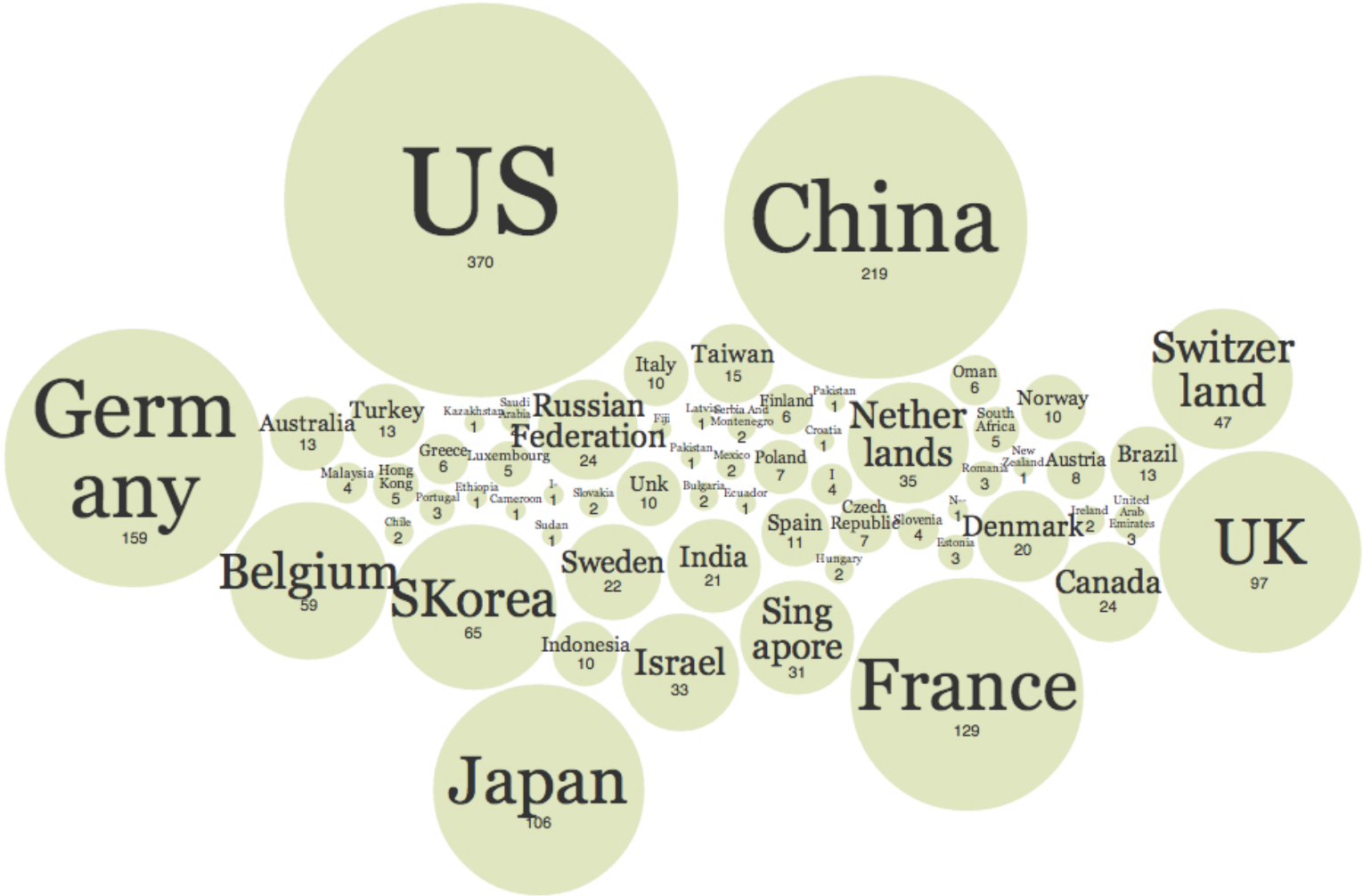
455 Students

Membership Demographics



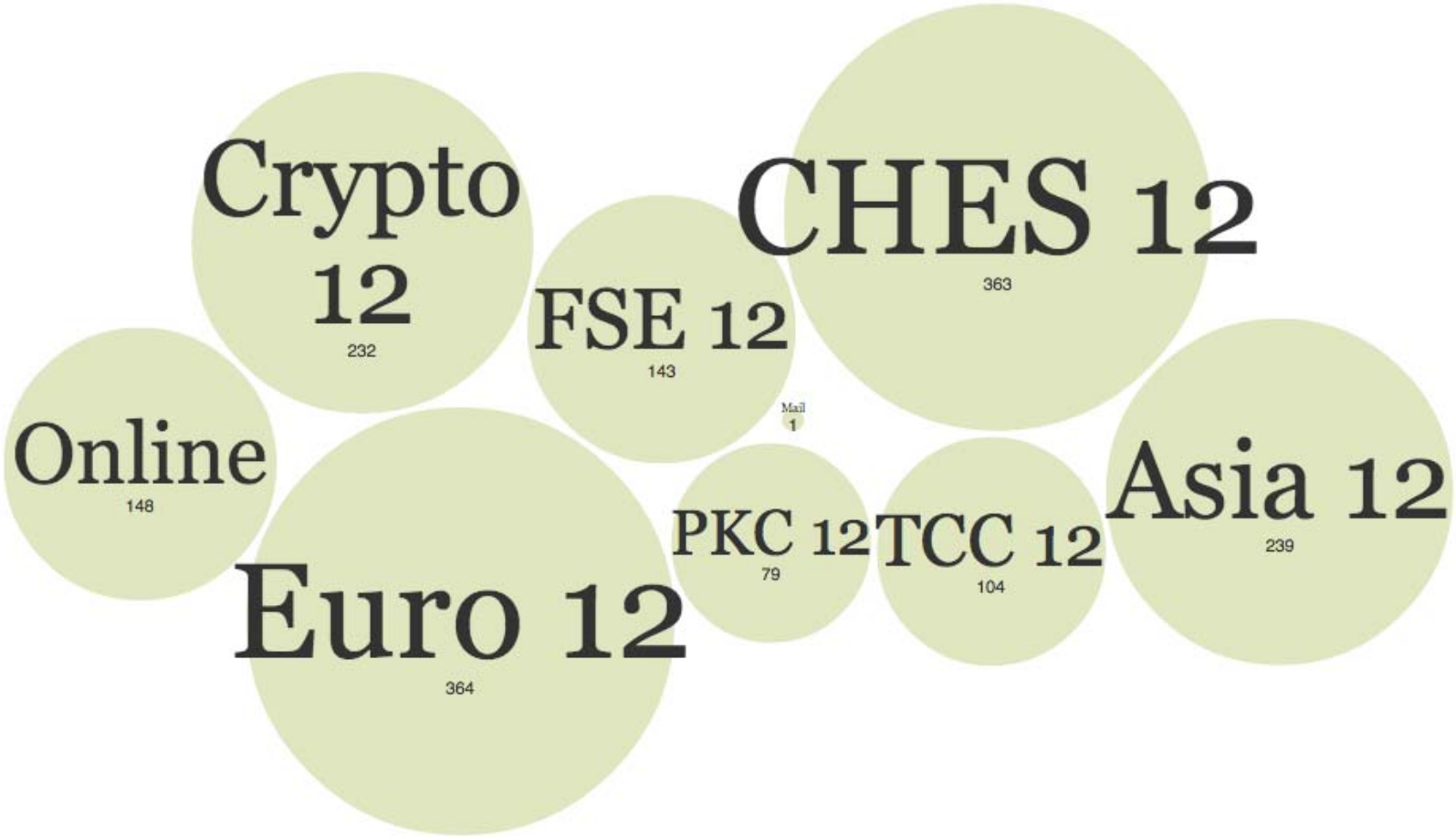
IACR Membership Distribution

By Country



IACR Membership Distribution

By Country



On-Line services

- All on the same server
  - www.iacr.org
  - ePrint
  - newsletter, mailing lists
  - membership/conference registration
  - submission/review for conferences
  - CryptoDB, archive
- Machine upgrade needed

Conferences & Workshops

2013 Conferences

- Eurocrypt'13: 26-30 May, Athens, Greece
  - Aggelos Kiayias/Thomas Johansson + Phong Nguyen
  - **IACR Distinguished Lecture: Eli Biham**
- Crypto'13: 18-22 Aug., UCSB, Santa Barbara, USA
  - Helena Handschuh/Ran Canetti + Juan Garay
- Asiacrypt'13: 1-5 Dec., Bangalore, India
  - Satyanarayana V. Lokam/Kazue Sako + Palash Sarkar

2014 Conferences

- Eurocrypt'14: 4-8 May, Copenhagen, Denmark
  - Lars R. Knudsen + Gregor Leander/Phong Nguyen + Elisabeth Oswald
- Crypto'14: *17-21 Aug* (tbc), UCSB, Santa Barbara
  - Alexandra Boldyreva/Juan Garay + NN
  - **IACR Distinguished Lecture: Mihir Bellare**
- Asiacrypt'14: 7-11 Dec, Kaohsiung, Taiwan
  - D. J. Guan/Palash Sarkar + Tetsu Iwata

2015 Conferences

- Eurocrypt'15: 4-8 May, Sofia, Bulgaria
  - Dimitar Jetchev + Svetla Nikova/Elisabeth Oswald + NN
- Crypto'15: Aug, UCSB, Santa Barbara
- Asiacrypt'15: 6-10 Dec, Auckland, New Zealand
  - Steven Galbraith/Tetsu Iwata + NN

2013 + 2014 Workshops

- CHES'13: 22-24 Aug, UCSB
  - Thomas Eisenbarth + Çetin Koç/Guido Bertoni + Jean-Sébastien Coron
- TCC'14: 24-26 February, UCSD, San Diego, CA, USA
  - Mihir Bellare + Daniele Micciancio/Yehuda Lindell
- FSE'14: 10-12 March, London, UK
  - Carlos Cid + Christian Rechberger
- PKC'14, 26-28 March, Buenos Aires, Argentina
  - Ariel Waissbein + Juan Garay/Hugo Krawczyk

Conferences and Workshops

- Now hearing proposals for 2016 conferences and 2015 workshops
- Details on how to submit a proposal on www.iacr.org
- Or see a member of the Board/Steering Committee

In particular: candidates for Crypto general chair

Journal of Cryptology

Editor in Chief – Matt Franklin
franklinHEREATcs.ucdavis.edu

Journal of Cryptology

- The premier Journal in cryptology
  - published by Springer-Verlag
  - available in reading room and via postal mail to IACR members (unless you opt-out)
- Overall health very good
- Submission pipeline steady and sustainable
- Send me your ideas for new special issues
  - practical topics especially welcome

IACR Newsletter

Editor – Christopher Wolf
newsletterHEREATiacr.org

IACR Newsletter/Website

- available on http://www.iacr.org/newsletter
- contents
  - calendar of events
  - job opportunities
  - publication announcements
  - book reviews
  - **PhD database (please submit!)**
- via web but also
  - **twitter (http://twitter.com/#!/iacr_news)**
  - **RSS**
  - **email subscription**

- Submit to newsletterHEREATiacr.org

IACR Fellows

New IACR Fellows in 2013

- Dan Boneh
- Ronald Cramer
- Claude Crépeau
- Lars Knudsen
- Hugo Krawczyk
- Victor S. Miller
- Rafail Ostrovsky

Selection committee members:

- Arjen Lenstra (chair), Ueli Maurer, Kevin McCurley, Ron Rivest, Phil Rogaway

Procedures

- Candidates, nominators, and endorsers must be IACR members. Verify membership by corresponding with iacrmemHEREATiacr.org
- Deadline: December 31, 2013
- Instructions: http://www.iacr.org/fellows/
- Submit to fellowsHEREATiacr.org
- Selection committee members:
  - Gilles Brassard, Ueli Maurer, Kevin McCurley (chair), Phil Rogaway

Publications

Springer-Verlag

- Publisher of IACR's conference and workshop proceedings in the LNCS series and the Journal of Cryptology
- LNCS: new contract has been signed for 2013-2016

Multiple versions of a paper

- Springer version (has DOI)
  - NN and NN (Eds.): EUROCRYPT 20xx, LNCS xxxx, pp. xx-xx, 2013. © International Association for Cryptologic Research 2013
- IACR version (minor differences)
  - "© IACR <year>. This article is the final version submitted by the author(s) to the IACR and to Springer-Verlag on <date>. The version published by Springer-Verlag is available at <DOI>."
- Minor revision
  - "© IACR <year>. This article is a minor revision of the version published by Springer-Verlag available at <DOI>."
- Full version (more than 25% difference)
  - “This article is based on an earlier article: <bibliographic data>, © IACR <year>, <DOI>."

Availability

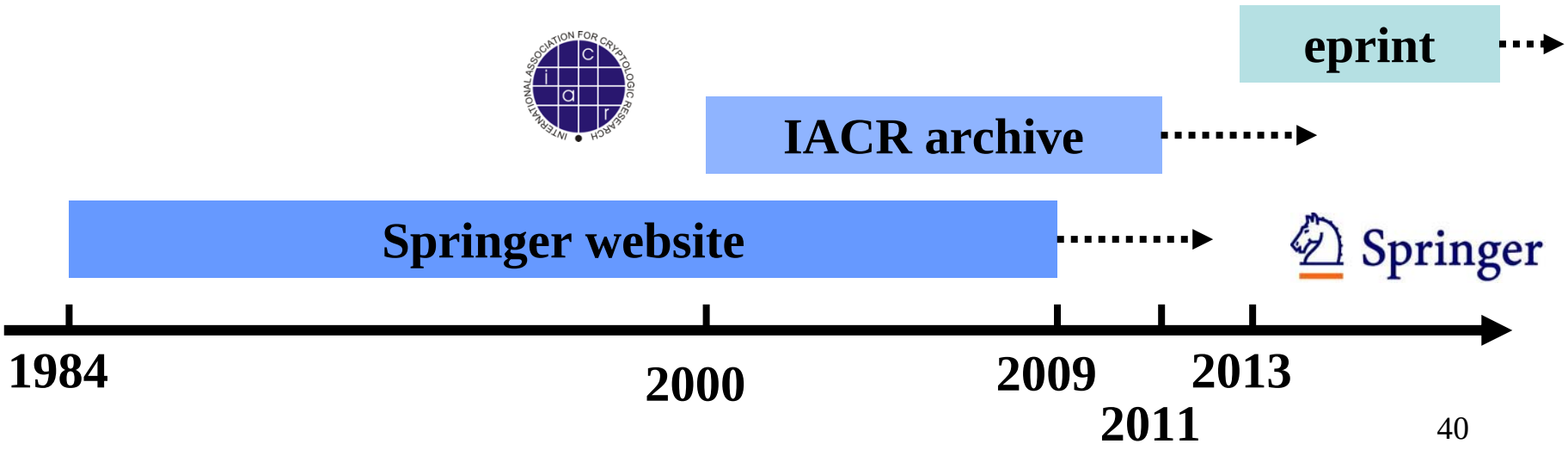
- 1984-2008 (+JoC): open access on link.springer.com
- 2000-2010: IACR archive (IACR version)
- 2013-: IACR eprint service (IACR version)

IACR members only

- 1984-2012 + JoC: IACR reading room www.springer.com.iacr
- 2013- : closed access on link.springer.com
- PrintPDF on USB stick or conference website

Access of broader community

Version	Where	Which papers
IACR	Eprint	2013-...
IACR	IACR archive	IACR papers from 2000 older than 2 years
Springer	Springer website	All IACR papers older than 4 years



Authors

- Copyright form revised
  - submit IACR version to eprint
  - reuse of pictures and parts
  - inclusion in Master/PhD thesis
  - give license for slides/video/extra content

- Eurocrypt authors: please sign again
  https://secure.iacr.org/websubrev/ec2013/submit/copyright.php

Current Board Activities

E-publishing

Opt-In for paper

- Proceedings: since 2011
- Journal of Cryptology: from 2014 onwards?

Towards a journal publication model?

- Multi-dimensional problem
  - Quality
  - Speed
  - Reputation
  - Review load
  - Bandwidth limitation
  - Complexity
- Discussion forum

http://eprint.iacr.org/forum/list.php?14

Current Board Activities

- **Flagship conferences**
  - the Board encourages program co-chairs to take the necessary actions to ensure a balanced program
  - increase number of accepted papers (accommodate this with shorter talks, more half-days, longer days, parallel sessions)

- **Ethical guidelines for authors and reviewers**
  - http://www.iacr.org/docs/

- **Discussion forum will be added to iacr.org**

- **Audit Committee has been installed: 3-yearly audit of finances**