International Association for Cryptologic Research

Christian Cachin
President, IACR

May 2014

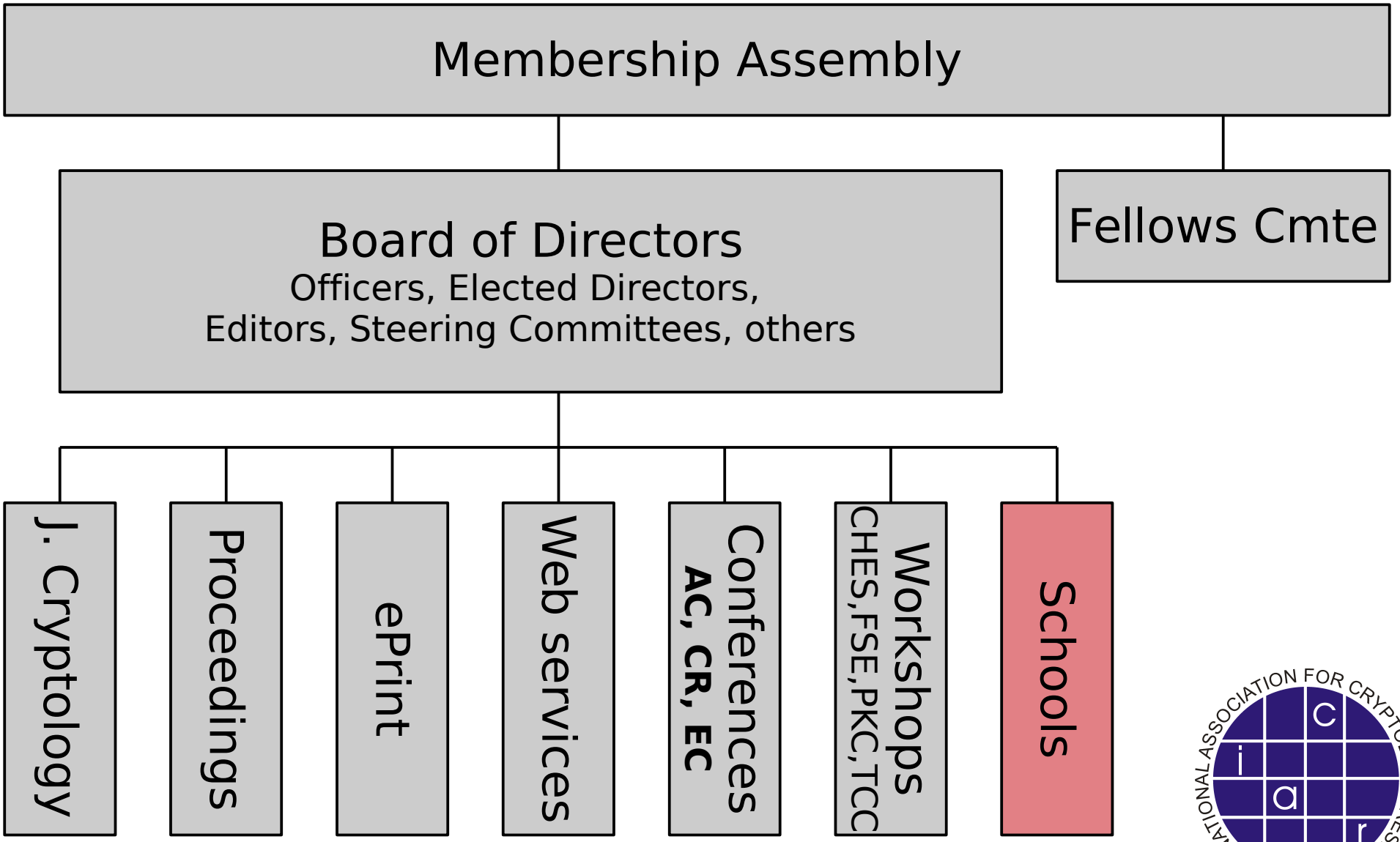
Membership meeting

- About IACR
  - Publications
  - Conferences
  - Services
- Communications Secretary
- Cryptology Schools
- Revision of IACR publications
- Financial report
- Membership report
- Future events

IACR

- International Association for Cryptologic Research
  - Purpose is to further research in cryptology and related fields
  - 1983
  - Incorporated as non-profit organization in Nevada (US)

One picture


Membership Assembly
Board of Directors
Officers, Elected Directors,
Editors, Steering Committees, others
Fellows Cmte
J. Cryptology
Proceedings
ePrint
Web services
Conferences
AC, CR, EC
Workshops
CHES,FSE,PKC,TCC
Schools

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
c
i
a
r

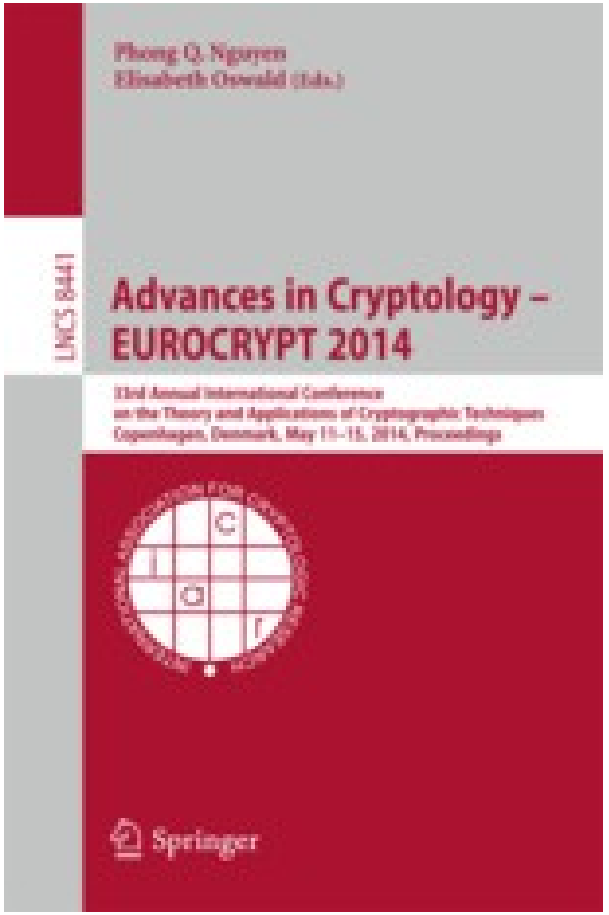
Membership

- Everyone attending an IACR event becomes a member in next calendar year
- Become a member online
- Membership fee of $50 ($25 students)

Journal of Cryptology

- Editor in Chief
  - Matt Franklin (-2014)
  - Ivan Damgård (2014-)
- New from 2014: Paper delivery is opt-in
  - Contact membership secretary to continue receiving paper issues

Proceedings



- ASIACRYPT
- CRYPTO
- EUROCRYPT
- CHES
- FSE
- PKC
- TCC

- Online for members
  www.iacr.org
- Online for all (> 4yr)
  link.springer.com

Cryptology Schools

- New initiative, starting now
- IACR reviews proposals and supports some schools each year
  - Educational, typically 1-week, learning required (Summer/Winter/Spring/Fall/...)
  - Financial support for speakers etc.
  - Publicity
- Proposals due June 30
  - Committee chaired by Michel Abdalla
- http://www.iacr.org/schools/

Online services

- IACR announcements
- Cryptology ePrint Archive
  - Tal Rabin & Nigel Smart
- Calendar of events
- Open positions
- Book reviews
  - Edoardo Persichetti
- PhD genealogy database
- Bibliography (CryptoDB)
- IACR Archive

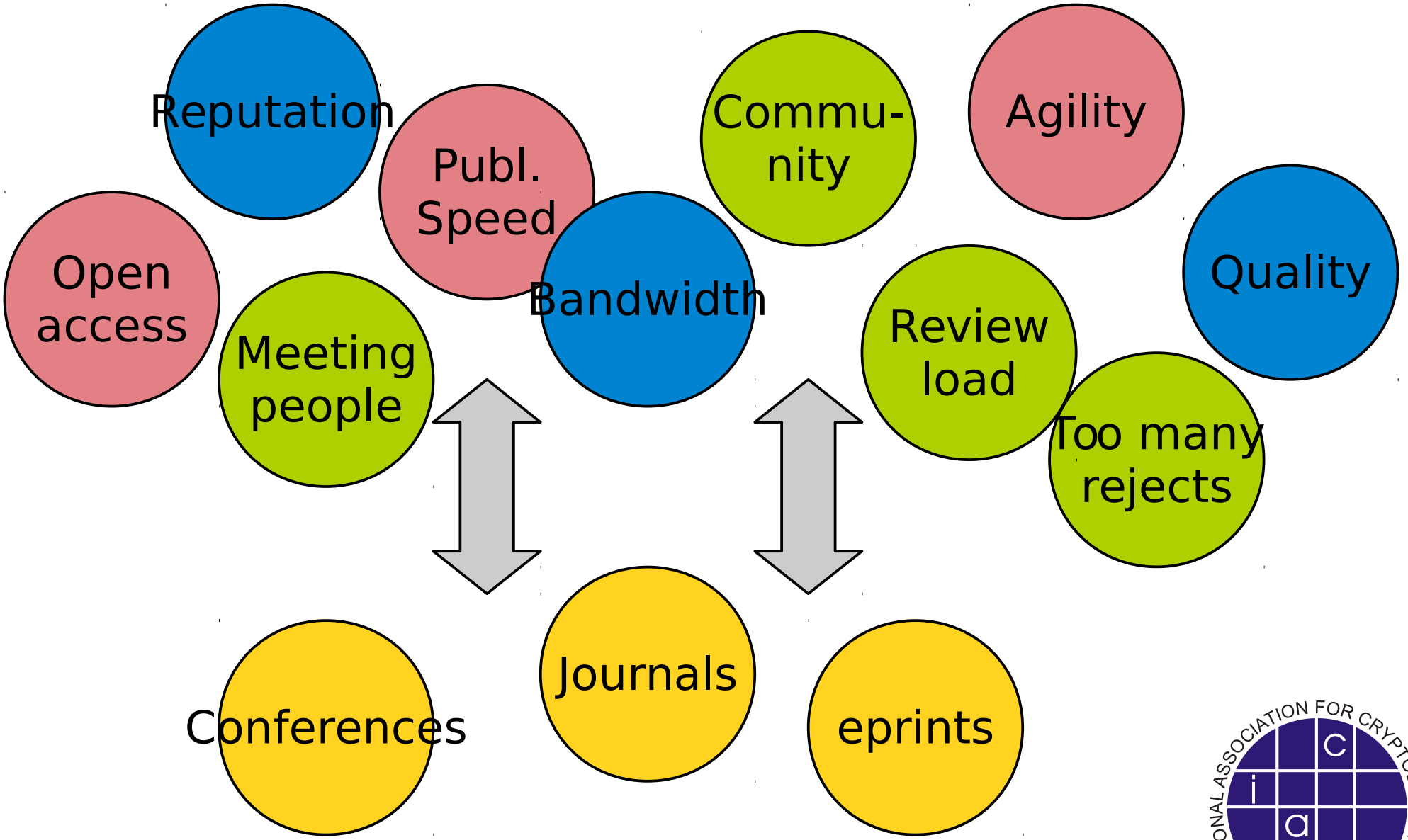
- News channels

Communications Secretary

- Chief Communication Officer
- PR-Manager of the IACR
- Webmaster and database hacker
  - 1998-2004: Christian Cachin
  - Currently: Christopher Wolf - will resign
- Volunteer(s) needed to replace him
- Please contact president@iacr.org

Future of IACR publications

Publications and conferences



Some history

- Conference attendance is down w.r.t. 10 yrs. ago (CR/EC now: 300..350 / it was 450..500)
- Acceptance rates are down w.r.t. 10-20 yrs. ago
- But the community has grown
- The number of competing events has grown

Future of IACR publications

- Three questions
  - Each of them can be answered independently
  - The consequences imply a course of action
- 1 - Should IACR move to Gold Open Access?
- 2 - Should IACR publish exactly what is submitted?
- 3 - Should reviews stick to papers in the sense of multi-round reviewing?

1 - Should IACR move to Gold Open Access?

- Gold open access = papers open to anyone
- Cost? Who pays?
  - Note: Eurocrypt '14 attendees do not pay this
- With ACM for conferences: $1100 per paper
- With Springer in current model: $900 per paper (avg. 18 p.)
- With other publishers: perhaps as low as $200 per paper

1a - Proceedings of the IACR

- Idea launched in 2013, "Strawman proposal"
  - http://eprint.iacr.org/forum/list.php?14
- Features
  - Submission at any time
  - Multi-round reviewing => shorter publication latency
  - Higher bandwidth than today
  - Inspired by Proc. VLDB model
- ISI indexing
  - Not done today for LNCS
  - Unclear for "Proceedings of the IACR"
- 1a - Should IACR worry about ISI indexing?

1b - Who should pay for Open Access?

- Cost does arise, in order to guarantee professional publication
  - 280 papers per year
    - 50 papers at AC/EC/CR; 33 papers at CHES/FSE/PKC/TCC
- Answers
  - Authors per paper
    - $500-$1000 per paper
  - Members/IACR through membership fee
    - $90-$180 per member (1500)
  - Conference attendees
    - $70-$140 with 350 attendees at typical CR/EC/CHES
    - $130-$260 with 125 attendees at typical PKC/TCC/FSE

2 - Should we publish what is submitted?

- Due to e-publishing, the cost no longer arises per page
  - However, reviewing of 40-page submissions not feasible during conference time frame
  - Overall quality may suffer
- Reduces proliferation of multiple versions
  - Accepted model outside computer science
  - No more full version or appendix during submission
- Blaise Pascal — I would have written a shorter letter, but I did not have the time.
- Answers: YES / NO

Publish what is submitted?

- CS and cryptography have adopted conferences as most important publ. venue
  - Elsewhere and early on in CS, light-weight publication at conference precedes journal
  - If conference-only, full versions are never reviewed
  - Conference+journal is seen as double-publication elsewhere
  - This may hurt the field in the long run
- FSE already has post-proceedings
  - Not reviewed again
- Many implications
  - Make reviewing time proportional to length?

Page limit for submissions? (Vote)

- What should the page limit be?
- Small adjustment to current practice
- Should submissions to IACR conferences and workshops be limited in length?
  - Assuming the usual single-column format, where the CFP today states max. 12 pages
  - This may enable that reviewing covers what is published
- Limit? YES / NO
  - 12p? / 18p? / 30p? / 40p?

3 - Should reviews stick to papers (multi-round rev.)?

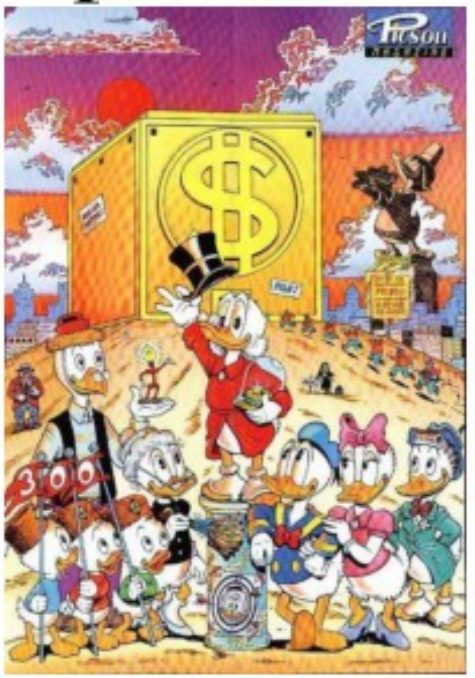
- Primitive version is already done via rebuttals

- From conference to conference
  - Authors submit with reviews from previous reject and changes
  - Cuts down review time
  - Contradicts independence of PCs
  - Complicates conflict handling

- In "Proc. IACR" model this is automatic
  - Comes with strict deadlines for review and revision cycles

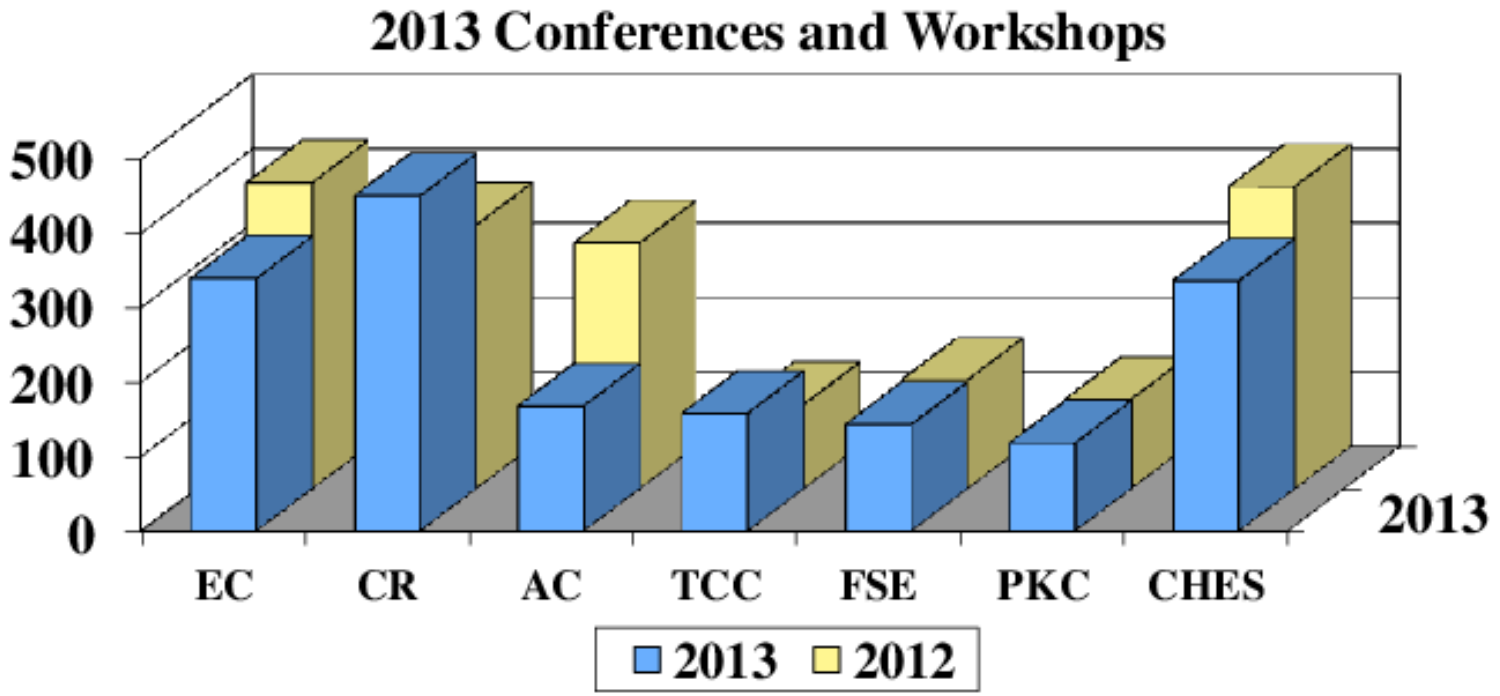
- Answers: YES / NO

IACR Preliminary Financial Report 2013

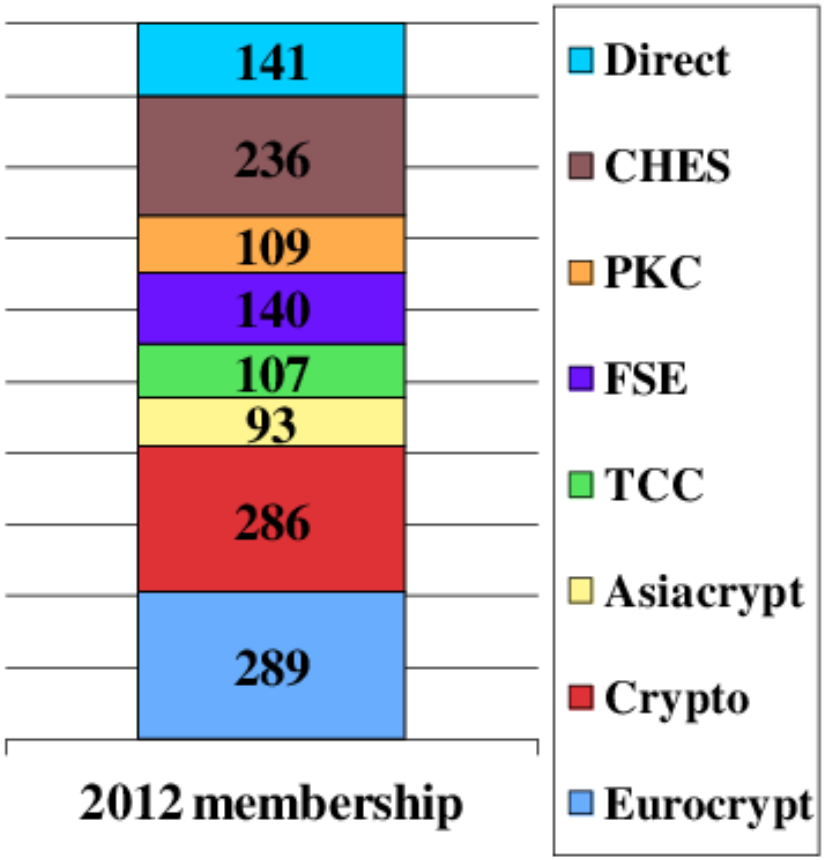


Greg Rose

treasurer@iacr.org


2013 Conferences and Workshops
500
400
300
200
100
0
EC
CR
AC
TCC
FSE
PKC
CHES
2013
2013
2012

2013 Membership



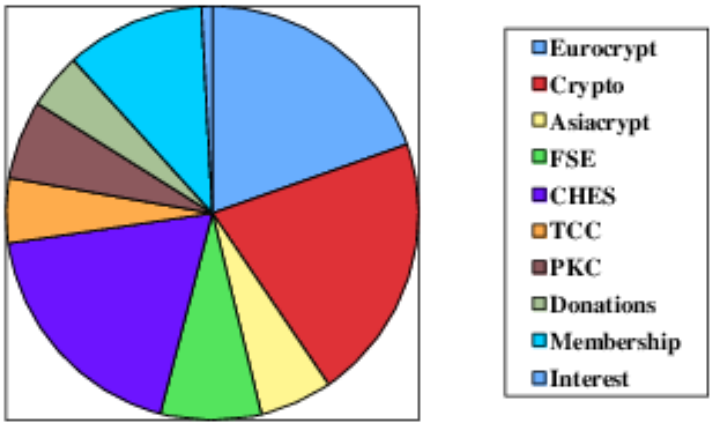
2013 Membership fees collected in 2012:

- Conferences and Workshops
- Directly through IACR
- Now US$50/25 -- decreased
- 1401 down 10%

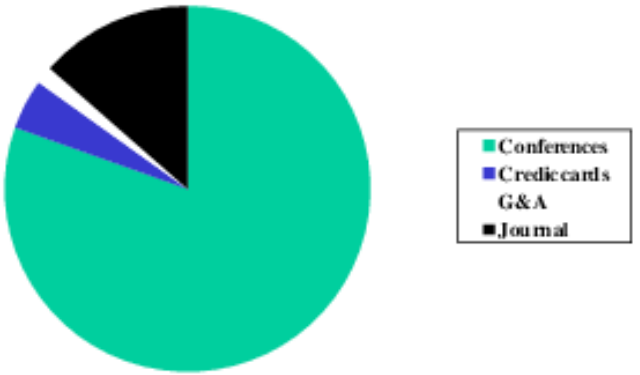
Profit&Loss FY2013

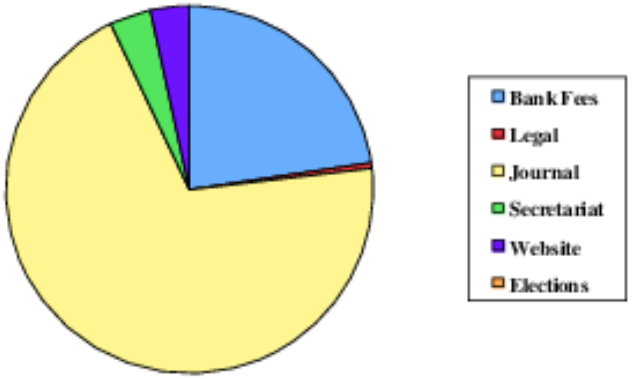
(not final)

Income (828k$)



Expenses (835k$)





2013 Highlights

- Board agrees to subsidize students in budget process
- Target break-even (or slight loss) budgets
- Keep minimal overhead - less than 2%

- Proposal accepted: 2015 Membership fee $50/$25, Journal electronic for all, $20 extra for paper copy of the Journal.
  - Paper copy not yet implemented.

Membership secretary report

2014

abhi shelat

Eurocrypt 2014

2014

1401

Members

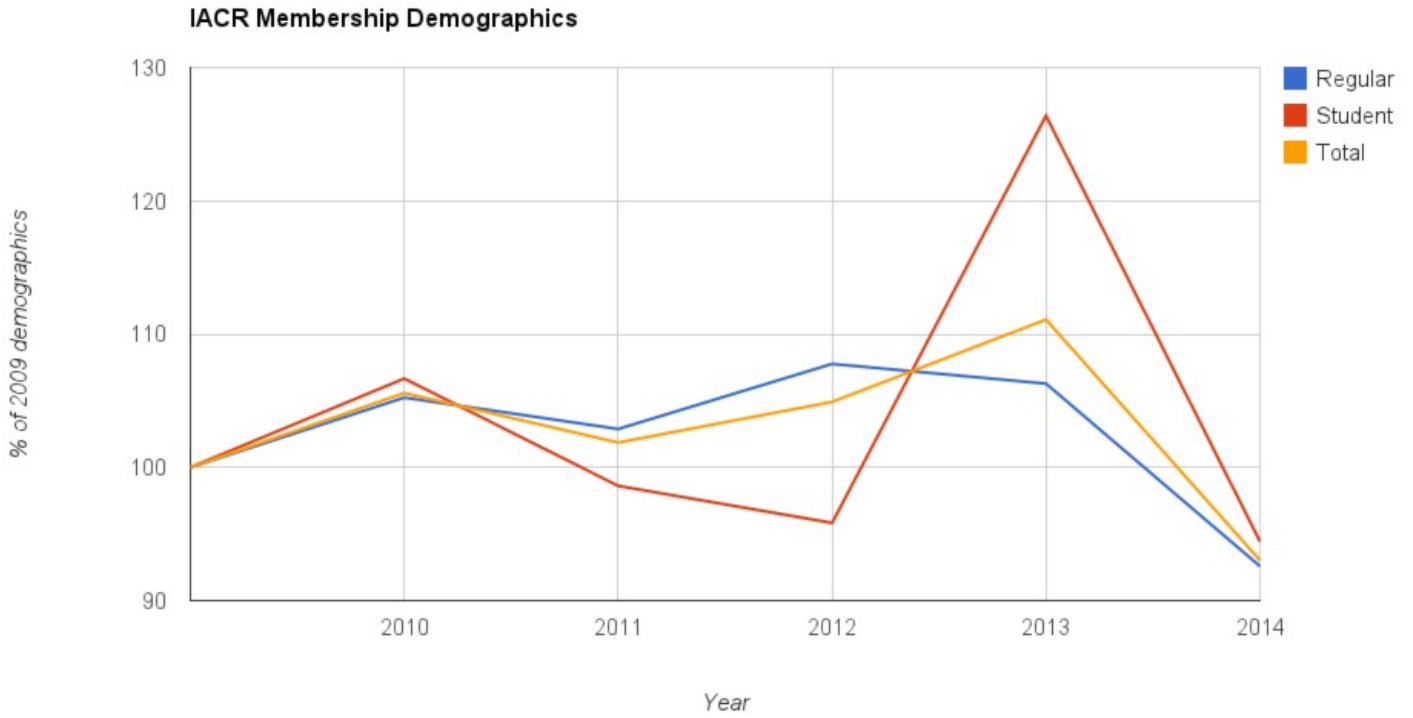
(1673 in 2013)

1061 Regular+

340 Students

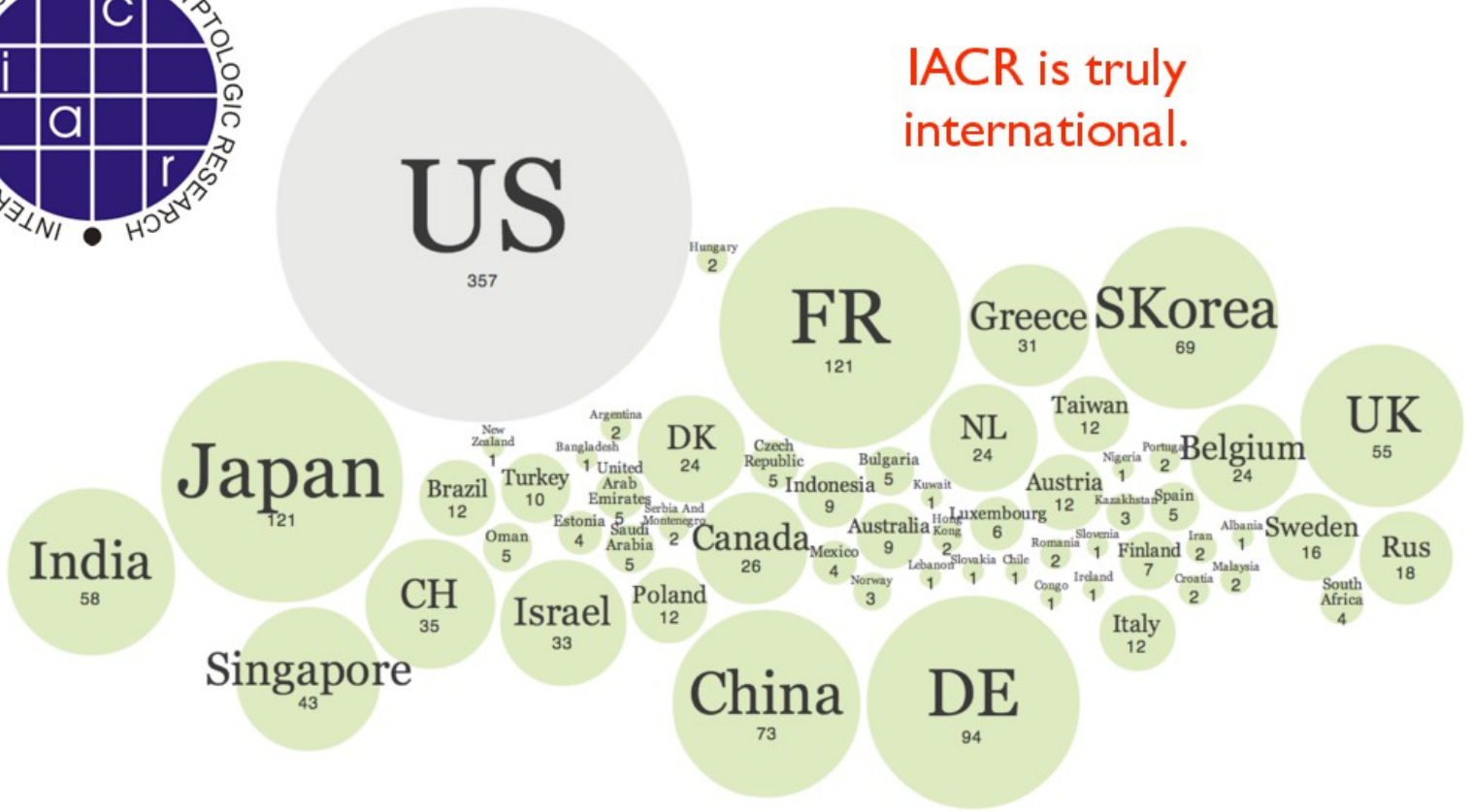
Membership Demographics

2014



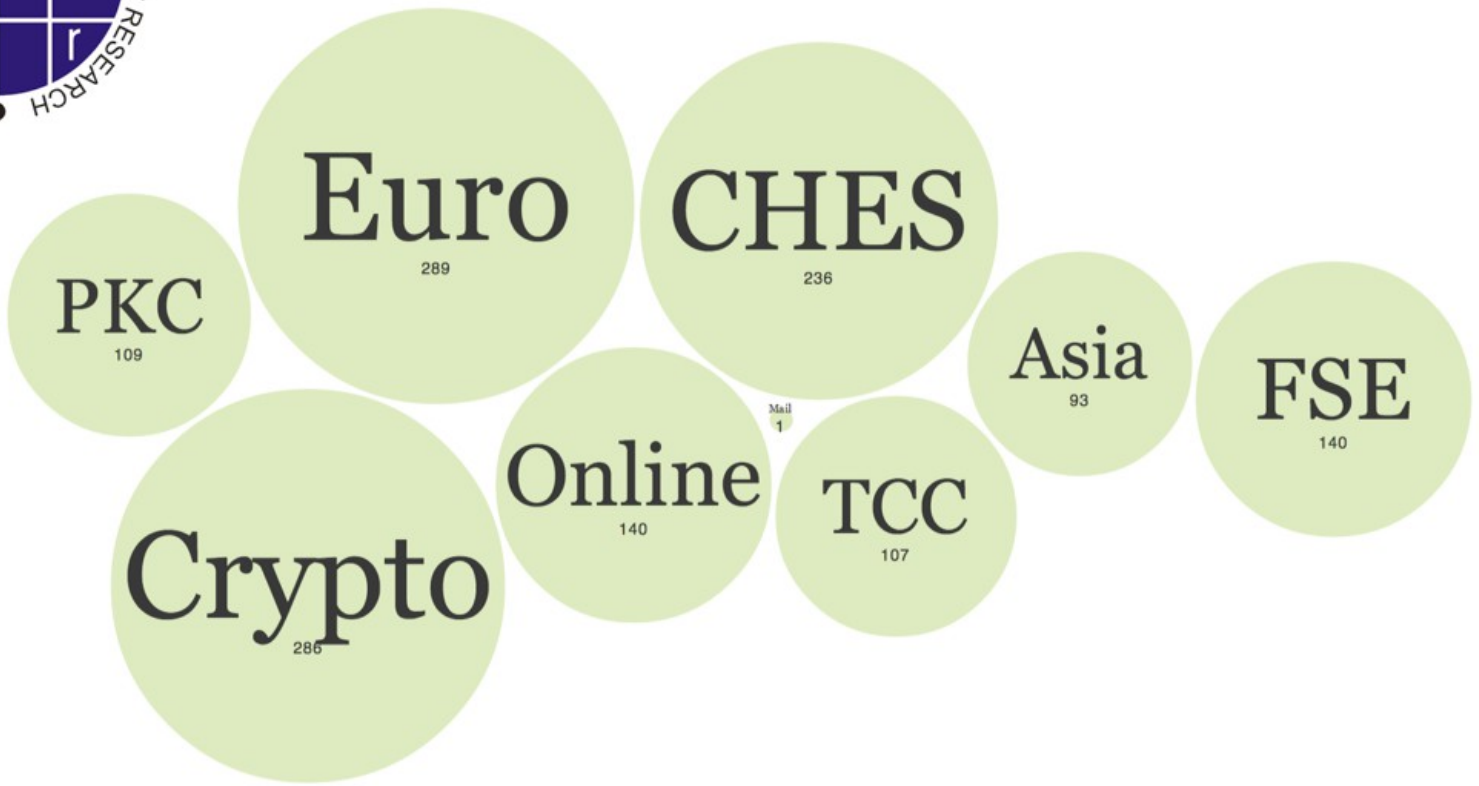
Lowest since 2009.

IACR 2014 Membership Distribution



IACR 2014 Membership Distribution

by conference



Gender statistics (Vote)

- How diverse is our field?

- BoD decision
  - A total gender count will be collected per event (with no further subdivisions) by an optional question, but data is not recorded in a personally identifiable way.
- Implementation on the registration form:
  - Gender
    - ( ) male; ( ) female; ( ) specify: _____; ( ) decline.

- Vote

Open discussion

Next events in 2014

- Crypto 2014, 17-21 Aug., UCSB, Santa Barbara
  - Sasha Boldyreva (GC)
  - Juan Garay & Rosario Gennaro (PC)
  - IACR Distinguished Lecture by Mihir Bellare
- CHES 2014, 23-26 Sep., Busan (Korea)
  - Kwangjo Kim (GC)
  - Lejla Batina & Matt Robshaw (PC)
- Asiacrypt 2014, 7-11 Dec., Kaohsiung (Taiwan)
  - D.J. Guan (GC)
  - Palash Sarkar & Tetsu Iwata (PC)

Conferences 2015

- Eurocrypt 2015, 26-30 Apr., Sofia (BG)
  - Svetla Nikova & Dimitar Jetchev (GC)
  - Elisabeth Oswald & Marc Fischlin (PC)
- Crypto 2015, 16-20 Aug. (tent.), UCSB, Santa Barbara
  - Thomas Ristenpart (GC)
  - Rosario Gennaro & NN (PC)
- Asiacrypt 2015, 7-11 Dec., Kaohsiung (Taiwan)
  - Steven Galbraith (GC)
  - Tetsu Iwata & Jung Hee Cheon (PC)

Conferences 2016

- Eurocrypt 2016, Spring, Somewhere in Europe
  - Contact Michel Abdalla and president@iacr.org
- Crypto 2016, 14-18 Aug. (tentative), UCSB, Santa Barbara
  - ???
- Asiacrypt 2016, 4-8 Dec., Hanoi (Vietnam)
  - Phan Duong Hieu & Ngo Bao Chau (GC)
  - Jung Hee Cheon & ??? (PC)

Workshops 2015

- FSE 2015, 8-11 Mar., Istanbul (Turkey)
  - Hüseyin Demirci (GC)
  - Gregor Leander (PC)
- PKC 2015, Gaithersburg, MD / NIST (US)
  - Rene Peralta (GC)
  - Jonathan Katz (PC)
- TCC 2015, 22-25 Mar., Warsaw (Poland)
  - Stefan Dziembowski (GC)
  - Yevgeniy Dodis & Jesper Buus Nielsen (PC)
- CHES 2015, 6-9 Sep. (tent.), St-Malo (FR)
  - E. Prouff, G. Renault & M. Rivain (GC)
  - Helena Handschuh &Tim Güneysu (PC)