International Association for Cryptologic Research

Christian Cachin
President, IACR

CRYPTO 2014 (updated)

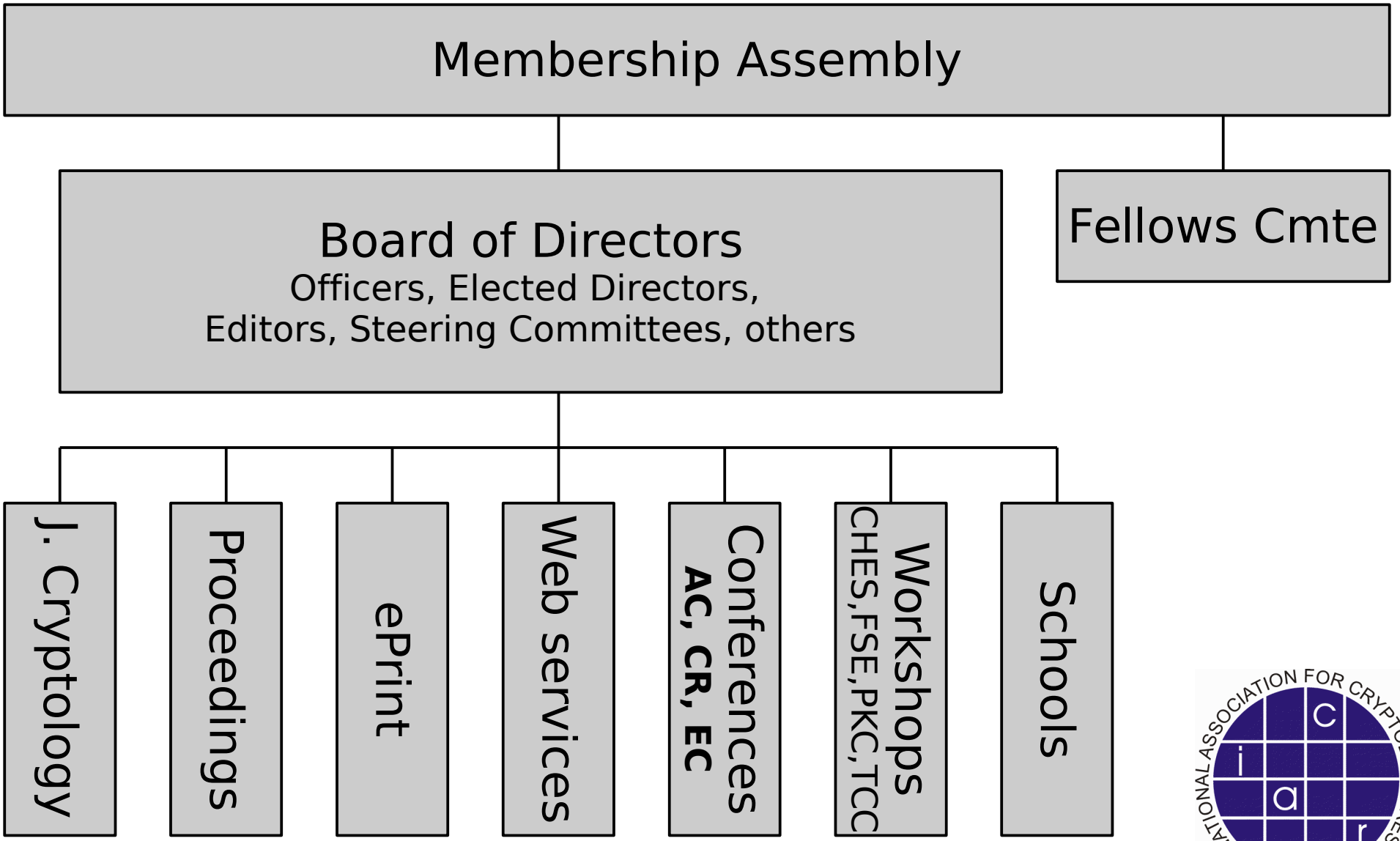
Membership meeting

- About IACR
  - Publications
  - Conferences
  - Services
- Communications Secretary
- Cryptology Schools
- Publications and conferences
- Membership report
- Financial 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)

Board of Directors

- 4 Officers
- 9 elected Directors
- Appointed Directors and observers

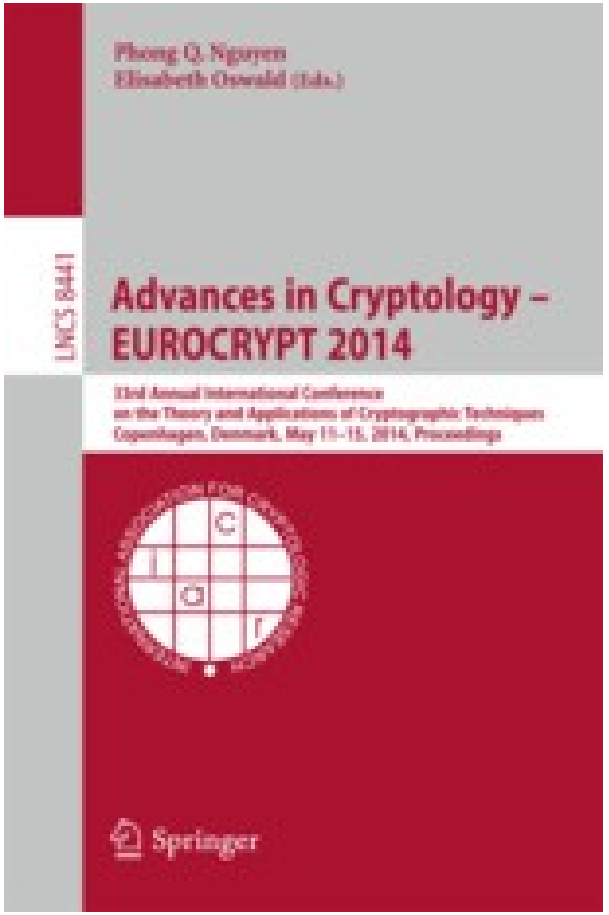
- www.iacr.org/bod.html

- Election of 3 Director positions in 2014
  - Nominations are open
    - www.iacr.org/elections/2014/
  - Using Helios online voting

Journal of Cryptology

- Editor in Chief
  - Matt Franklin (-2014)
  - Ivan Damgård (2014-)
- New from 2014
  - Paper delivery is opt-in
    - Contact membership secretary by email to continue receiving paper issues
  - Online submission and reviewing system

Proceedings



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

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

Cryptology Schools

- New initiative,
  - First 3 IACR Cryptology Schools have been chosen
- IACR reviews proposals and supports some schools each year
  - Educational, typically 1-week, learning required (Summer/Winter/Spring/Fall/...)
  - Financial support for speakers etc. and publicity
- Next proposals due Dec. 31
  - Committee chaired by Michel Abdalla
  - http://www.iacr.org/schools/

First IACR Cryptology Schools

- School on Cryptographic Attacks
  - Oct 13-17, Porto, Portugal
  - http://attackschool.di.uminho.pt/
- School on Design and security of cryptographic algorithms and devices
  - July 5-10, 2015 (tent.), location tbd.
  - Svetla Nikova and Lars Knudsen
- ASK 2014 (Asian Workshop on Symmetric Key Cryptography)
  - Dec. 19-22, 2014, Chennai, India
  - http://ask.crypto.sg/

Online services

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

Communications Secretary

- Christopher Wolf has resigned
  - Newsletter editor and Comm. Sec. 2009-2014
  - Created many interactive services on www.iacr.org
- New team for communications

Mike Rosulek

Yu Yu

Cryptography Research Fund for Students

- With 1 Mio. $ donation from CRI, the IACR has created Cryptography Research Fund for Stud.
- Will be used to greatly increase student sponsorship for IACR events
  - Waive registration fee for student speakers at EUROCRYPT, CRYPTO, ASIACRYPT, CHES, FSE, TCC and PKC
  - Expand support for Cryptology Schools
  - And more ideas are welcome

Parallel sessions?!

- Since "CRYPTO" 1981 and "EUROCRYPT" 1982
  - Single track of talks, Mon-Thu, Tue afternoon "free"
- Format has not changed much
  - Typically 30-40 papers
    http://www.iacr.org/publications/statistics.html
- But field has grown a lot (topics *and* people)
- Many discussions ...
  - Frustration by authors and researchers
  - Parallel tracks have been discussed at almost every membership and Board meeting since late 1990s

Parallel sessions?!

- In 2011, Board sent message to PCs
  - *... are expected to accept substantially more papers than used to be the case and to work with their General Chair for the logistics to make this possible.*

- Numbers of papers

	'*10*	'*11*	'*12*	'*13*	'*14*
– CRYPTO	39	42	48	61	60
– EUROCRYPT	33	31	41	41	38
– ASIACRYPT	35	40	43	54	??

Parallel sessions?!

- At CRYPTO'14 Board of Directors decided
  - *... for the three IACR conferences in 2015 to have parallel sessions for a significant part of the program*
- In the sense of a trial for conferences in 2015
  - Membership will decide after 2015 whether to stay with this format
- Program Chairs and PCs are responsible for the scientific program

Publications format

- CS and cryptography have adopted conferences as most important publ. venue
  - Elsewhere and early on in CS, light-weight publication at conference precedes journal
  - Authors write 35 or 80 pages, but publish only 20
  - 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

Submission format

- How should conference submissions be formatted?
- Different from submission to publication
  - Creates uncertainty about result
  - Extra work for authors
- Hence submission should be as similar as possible to publication

Submission format

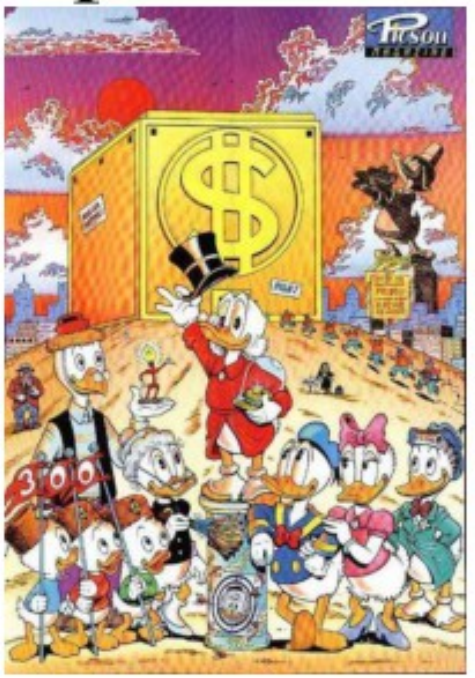
- At CRYPTO'14 Board of Directors decided to work with PCs to move towards harmonizing submission and publication format

- Implementation
  - Submission in LNCS or LNCS-like format
    - Details TBD — we have many LaTeX hackers here!
  - Main text *same length* as final version (about 20p)
    - No special title page, and including references
  - Followed by *supplementary material* of any length (proofs, formal models, parameters ...)

Rebuttals and sticky reviews

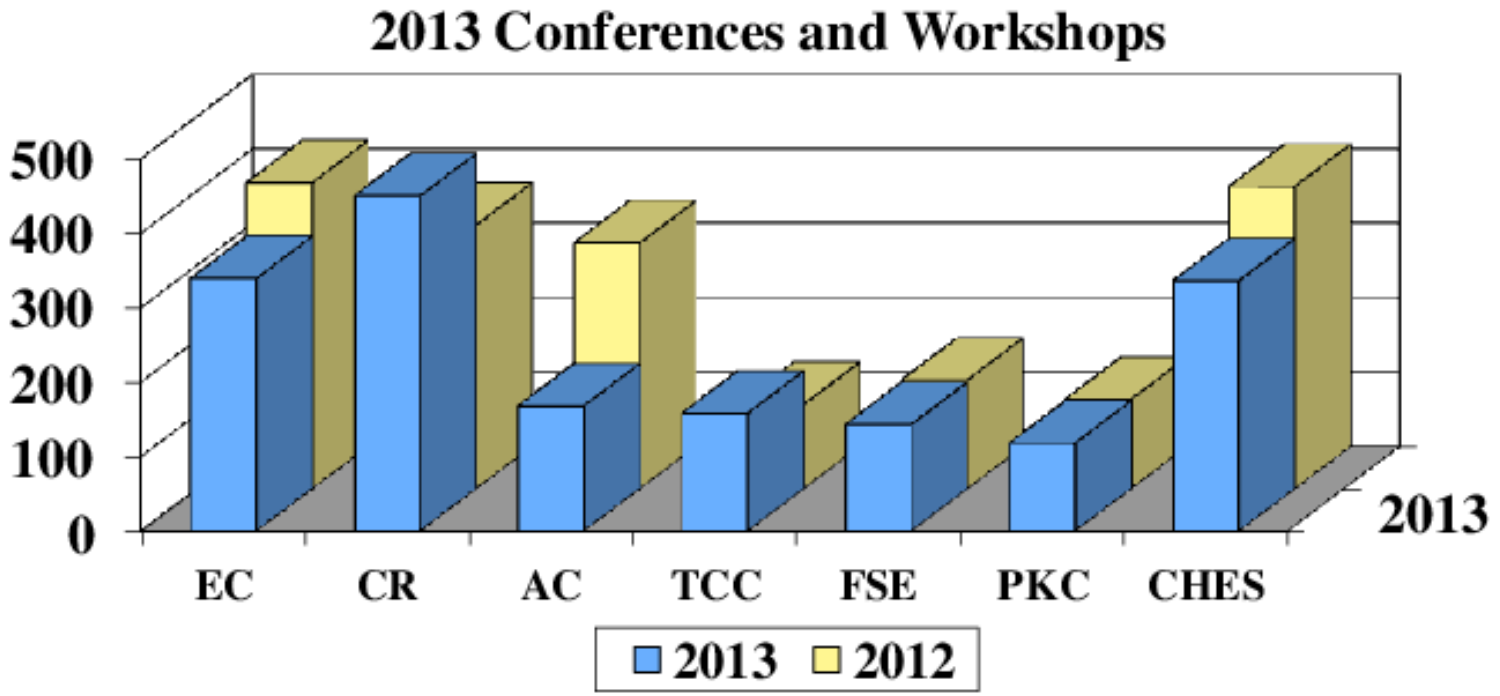
- Interactive communication with reviewers?
- CRYPTO '14 and EUROCRYPT '15 have already a rebuttal phase
- To enable feedback across re-submissions IACR explicitly encourages *sticky reviews*
  - Authors include responses to previous reviews
  - In supplemental material
  - Reviewers possibly different, remain anonymous

IACR Preliminary Financial Report 2013

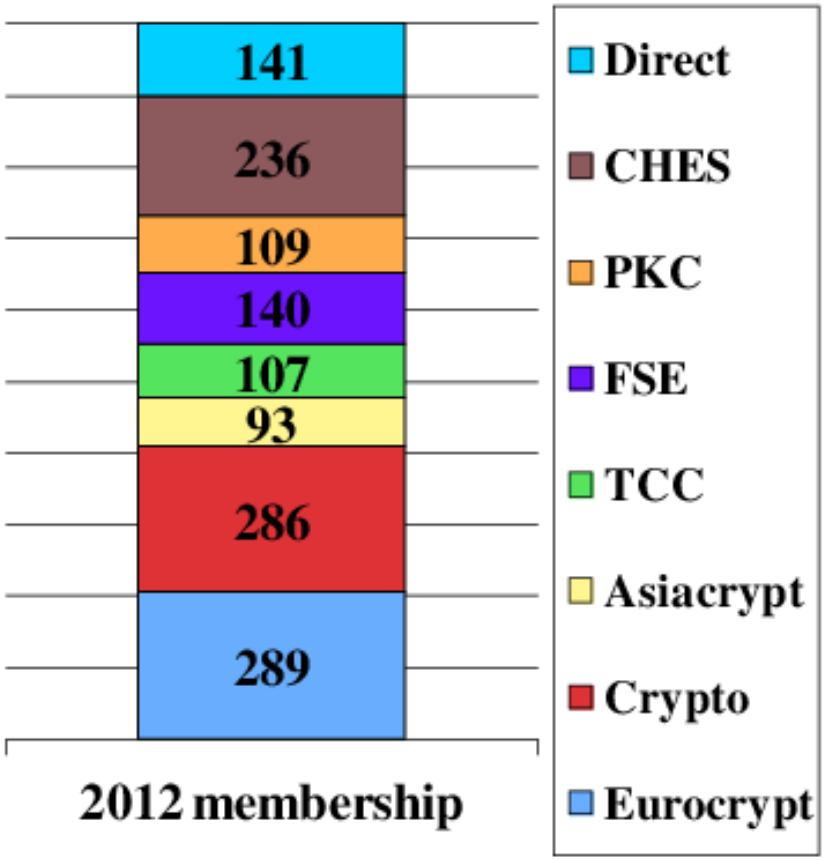


Greg Rose

treasurer@iacr.org



2013 Membership

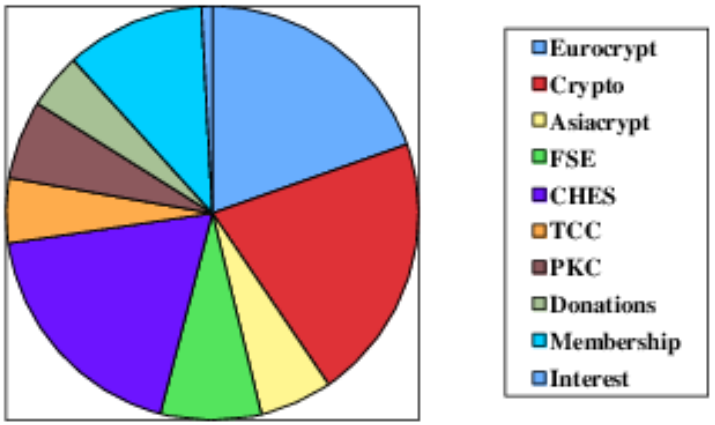


2013 Membership fees collected in 2012:

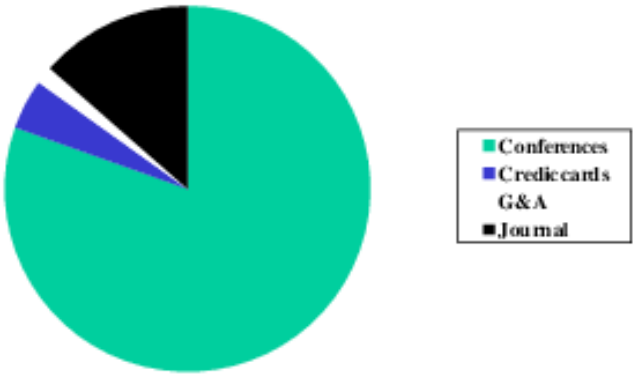
- Conferences and Workshops
- Directly through IACR
- Now US$50/25 -- decreased
- 1401 down 10%

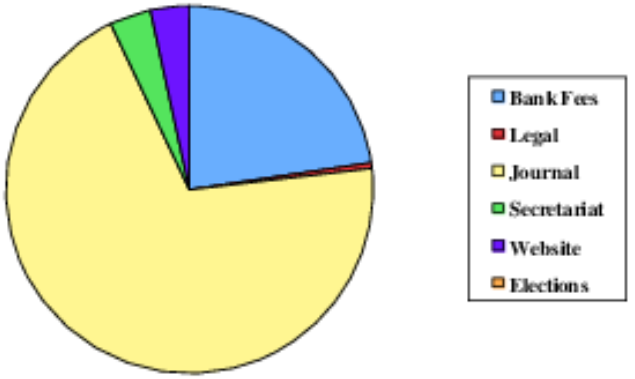
Profit&Loss FY2013
(not final)

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

CRYPTO 2014

2014

1437 Members

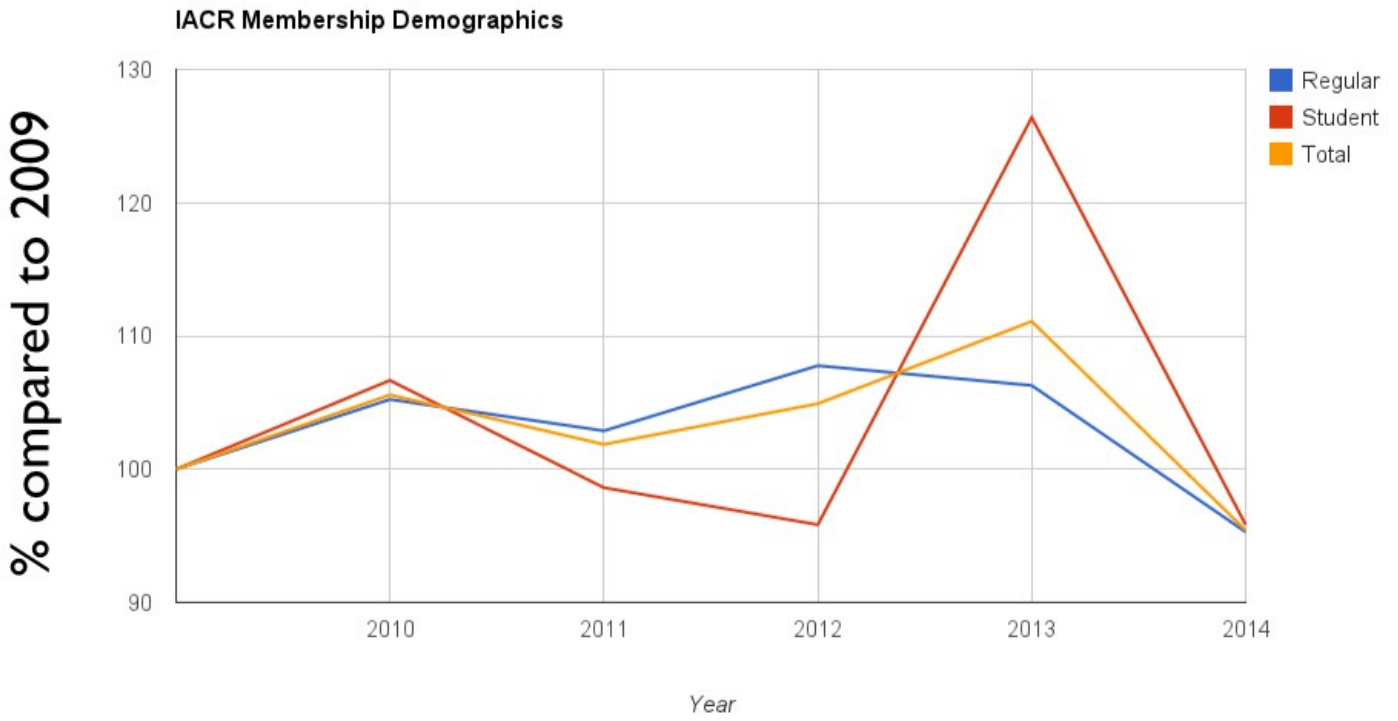
(1673 in 2013)

1092 Regular+

345 Students

Membership Demographics

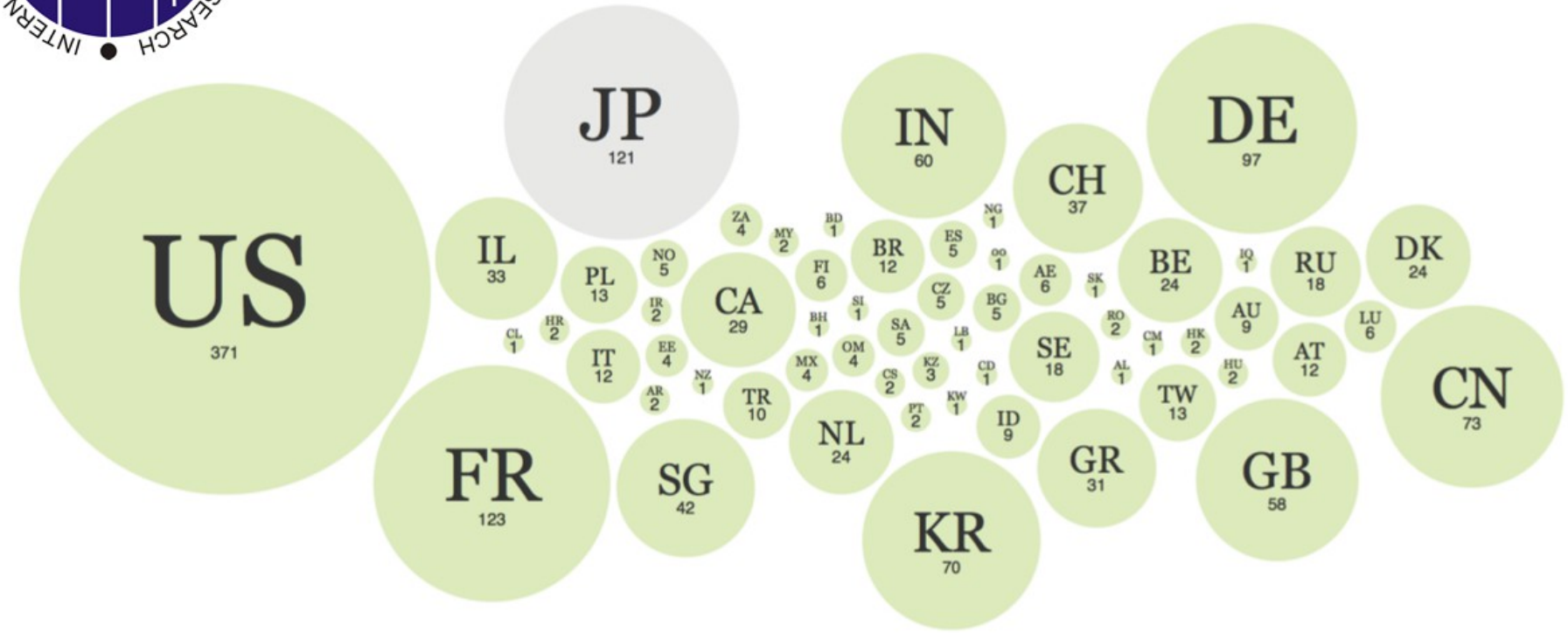
2014



Lowest since 2009.

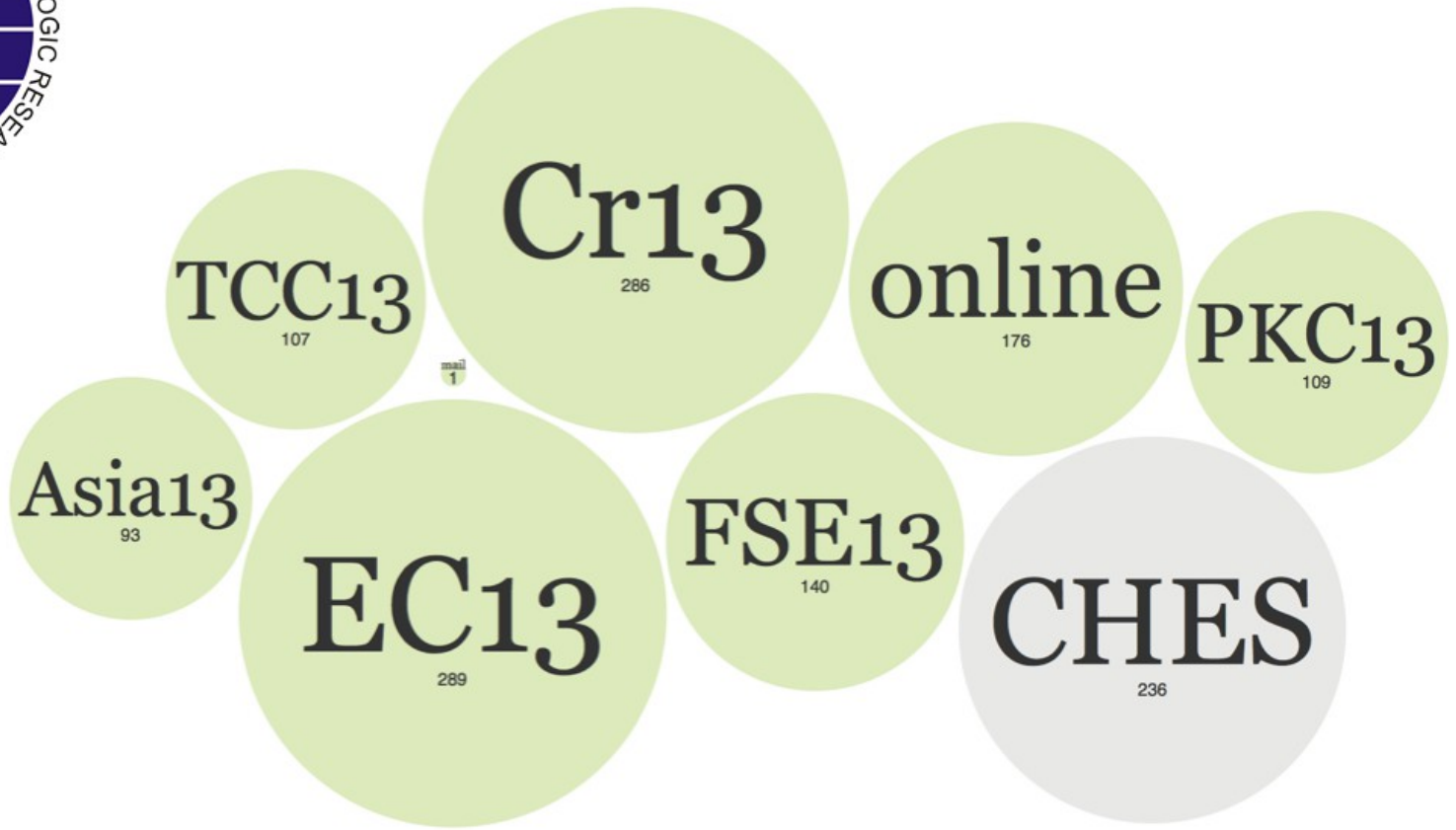
IACR 2014 Membership Distribution

IACR is truly international.



IACR 2014 Membership Distribution

by conference



Open discussion

Next events in 2014

- 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., UCSB, Santa Barbara
  - Thomas Ristenpart (GC)
  - Rosario Gennaro & Matt Robshaw (PC)
- Asiacrypt 2015, 29 Nov - 3 Dec., Auckland, NZ
  - Steven Galbraith (GC)
  - Tetsu Iwata & Jung Hee Cheon (PC)

Conferences 2016

- Eurocrypt 2016, 8-13 May, Vienna (Austria)
  - Krzysztof Pietrzak (GC)
  - Marc Fischlin and Jean-Sébastien Coron (PC)
- Crypto 2016, 14-18 Aug., UCSB, Santa Barbara
  - Brian LaMacchia (GC)
  - Matt Robshaw and ??? (PC)
- 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, 30 Mar-1 Apr., Gaithersburg (US)
  - Rene Peralta (GC)
  - Jonathan Katz (PC)
- TCC 2015, 23-25 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)

See you at the next event

- Beach barbecue starts at 18h