International Association for Cryptologic Research

Christian Cachin
President, IACR

CRYPTO 2015

Membership meeting

- About IACR
  - Publications
  - Conferences
  - Cryptology Schools
- Online services

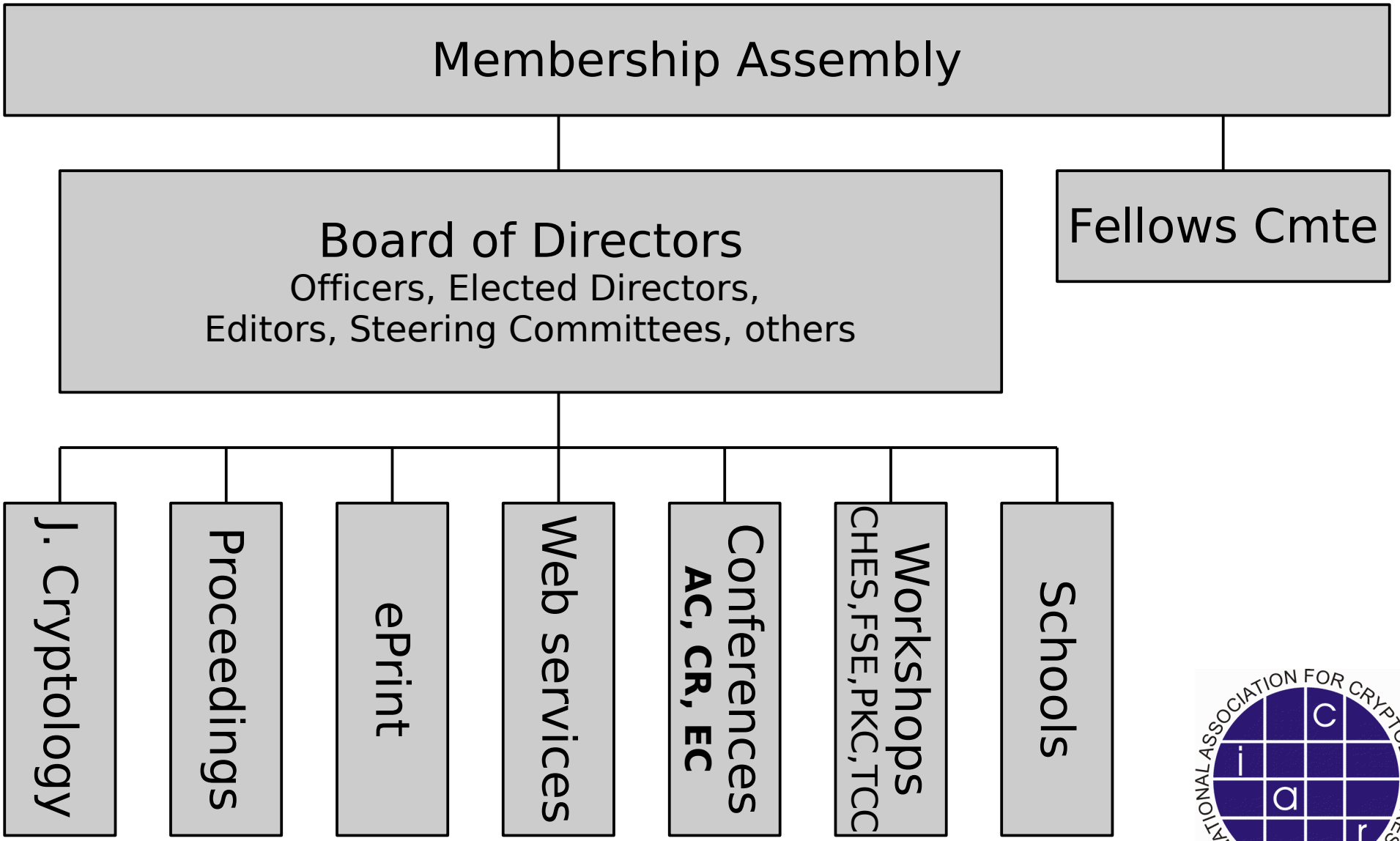
- Financial report
- Membership report

- Publications
- Parallel sessions
- Open discussion
- 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

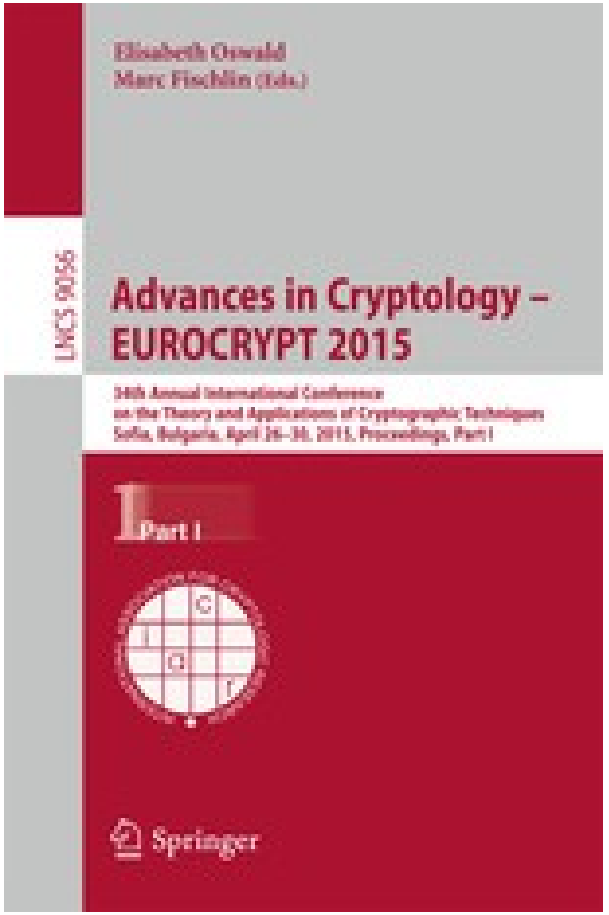
- www.iacr.org/bod.html

- Election of 3 Director positions every year
  - Nomination information is online
    - www.iacr.org/elections/2015/
  - Using Helios online voting

Journal of Cryptology

- Editor in Chief
  - Ivan Damgård
- Read online
  - www.iacr.org/services/springer.php
- Paper delivery is now opt-in for $20 extra
  - Change that in your membership data online
- Online submission 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 since 2014

- IACR reviews proposals and supports some schools each year
  - Educational, typically 1-week, learning required (Summer/Winter/Spring/Fall school)
  - Financial support for speakers etc. and publicity

- Next proposals are due December 31
  - Committee chaired by Michel Abdalla
  - http://www.iacr.org/schools/

Cryptology Schools 2015

- Summer school on elliptic curve cryptology, 23-25 Sep. 2015, Bordeaux (FR)
  - http://ecc2015.math.u-bordeaux1.fr/
- School on Design and Security of Cryptographic Algorithms and Devices, 18-23 Oct. 2015, Sardinia (IT)
  - https://www.cosic.esat.kuleuven.be/summer_school_sardinia_2015/index.html

Cryptology Schools 2016

- Summer School in Cryptocurrencies, Kos (GR), 30 May-2 June, 2016
  - No website yet
  - Organizers: Foteini Baldimtsi, Aggelos Kiayias, Sarah Meiklejohn

IACR Fellows

- The IACR Fellows Program recognizes outstanding IACR members for technical and professional contributions that:
  - Advance the science, technology, and practice of cryptology and related fields;
  - Promote the free exchange of ideas and information about cryptology and related fields;
  - Develop and maintain the professional skill and integrity of individuals in the cryptologic community;
  - Advance the standing of the cryptologic community in the wider scientific and technical world and promote fruitful relationships between the IACR and other organizations.

IACR Fellows – 2015

- Ernie Brickell
- Joe Kilian
- Kaisa Nyberg
- Tatsuaki Okamoto
- Bart Preneel
- Tal Rabin

- Nominations for 2016 Fellows due by 31 Dec.
  - www.iacr.org/fellows/

Communications

- Communications secretary and webmaster

Mike Rosulek

Yu Yu

Online services

- Find us on Facebook: facebook.com/theiacr
- IACR news and announcements
  - www.iacr.org
  - Twitter: @IACR_News // weibo.com/iacr
- Cryptology ePrint Archive
  - Sasha Boldyreva & Nigel Smart
- Online access to proceedings
- Calendar of events
- Open positions
- Book reviews
- Ph.D. genealogy database
- Bibliography (CryptoDB)
- IACR Archive

Statements and petitions

- Petition in response to Australia's Defence Trade Controls Act
  - To be signed online by members
- New mechanism to organize petitions among members
  - www.iacr.org/petitions/
- IACR has also made a statement in support of Bimal Roy (Former head of Indian Statistical Institute)
  - Quick action taken by the Board

More volunteers needed!

- Content administration
- Video editing
- Programming
  - Familiar with LAMP?
- Contact <president@iacr.org>

Cryptography Research Fund for Students

- With 1 Mio. $ donation from CRI, the IACR has created Cryptography Research Fund for Students in 2014
- Being used to sponsor student participation at IACR events
  - Waive registration fee for student speakers at EUROCRYPT, CRYPTO, ASIACRYPT, CHES, FSE, TCC and PKC
  - Support for Cryptology Schools
  - More ideas are welcome

Financial report

Membership report

Conferences and publications

- Field has grown, and still growing
- Publishing and research environment changing
  - Speed, open-access, archival publications
- Cryptography research has many dimensions
  - Practice & theory
  - Europe & Americas & Asia-Pacific
- IACR should continue to support growth and respond to current needs

Publisher

- IACR is currently re-assessing publisher for proceedings
  - Current agreement with Springer for proceedings in LNCS, can be revised after 2016
- FSE intends to become a journal-conference hybrid from 2017 onward
  - Similar to PVLDB, PoPETS, JETS
- Re-assessment is therefore necessary

Change in FSE publications

- Switch from LNCS proceedings to journal with green or gold open access
  - 4 submission deadlines per year and 4 review periods
  - Decision in 3 months: Accept, Reject, Revise & Resubmit (1x, within 3-6 months)
  - Papers accepted by January 20xx have to be presented at FSE 20xx

- Motivation
  - Thorough 2-round review for a journal
  - More polished submissions and final versions
  - Obtain ISI impact factor by 2020 (important for funding agencies in Europe and Asia)

Open Access

- Green-OA
  - Authors may publish their versions of a paper freely online (home page, eprint repositories), access to main publication is limited
- Gold-OA
  - Main publication is accessible freely (online)
- IACR currently has
  - Gold-OA with 4-yr embargo period
  - Green-OA (e.g., author versions on eprint archive)
- Move to Gold-OA? What cost? Who pays?

Who pays for Gold-OA?

- Cost for publishing arises at time of publication, there is no revenue in the future
- Readership of scientific literature
  - Authors (scientists, society members, conference attendees) vs.
    Non-authors (patent lawyers/offices, companies...)
- Currently authors pay (library budgets) and non-authors pay (subscriptions)
- Gold-OA shifts complete cost to authors

Benefits of Gold-OA

- Final publications are available freely & openly online
  - No complex authorization
  - No confusion due to multiple versions, such as in Green-OA
- Widest possible dissemination, also to researchers without access to libraries or poorer countries

How to pay for Gold-OA?

- Membership fee of IACR
  - In past, 75% of membership fee covered the subscription of the Journal of Cryptology
- Charge to conference attendees
  - Now attendees pay nothing for electronic access
  - In past, paid $50 for proceedings
- Author page charges (APC)
- IACR reserves

Poll

- Should IACR move to Gold-OA?
  YES NO
- If yes, membership fee increase
  $0 $50 $100
- If yes, increase in registration fee
  $0 $50 $100
- If yes, author charge (per paper)
  $0 $150 $300 $500

Parallel sessions in 2015

- Since "CRYPTO" 1981 and "EUROCRYPT" 1982
  - Single track of talks, Mon-Thu, Tue afternoon "free"

- In early years, typically 30 papers
- More recently, 50-60 papers
  - http://www.iacr.org/publications/statistics.html

- The field has grown a lot (topics *and* people)

- After many discussions ... in 2014 the Board of Directors decided

  ... for the three IACR conferences in 2015 to have parallel sessions for a significant part of the program

Parallel sessions here

- Opinions?
- Poll
  - Pro / neutral / against

Parallel sessions in the future

- IACR ensures continuity over different events
- Parallel sessions are a trial for the conferences (EC, CR, AC) in 2015
- After 2015, the membership will decide whether to stay with this format in an online vote

Submission format

- At CRYPTO '14 Board of Directors decided to work with PCs to move towards harmonizing submission and publication format
  - No technical reason for submission to be different from final version
  - More transparent when submission is same as final

- Implementation
  - Submission in LNCS format
  - Submission text has the same length as the final version (max. 30p. LNCS)
  - Followed by supplementary material of any length (proofs, formal models, extra files ...)
  - Will be the same over multiple conferences

Open discussion

Future conferences

- Asiacrypt 2015, 29 Nov.-3 Dec., Auckland, NZ
  - Steven Galbraith (GC)
  - Tetsu Iwata & Jung Hee Cheon (PC)
  - IACR Distinguished Lecture by Phil Rogaway
- Eurocrypt 2016, 8-12 May, Vienna (Austria)
  - Krzysztof Pietrzak (GC)
  - Marc Fischlin and Jean-Sébastien Coron (PC)
  - IACR Distinguished Lecture by Bart Preneel
- Crypto 2016, 14-18 Aug., UCSB, Santa Barbara
  - Brian LaMacchia (GC)
  - Matt Robshaw and Jonathan Katz (PC)

Future conferences

- Asiacrypt 2016, 4-8 Dec., Hanoi (Vietnam)
  - Phan Duong Hieu & Ngo Bao Chau (GC)
  - Jung Hee Cheon & Tsuyoshi Takagi (PC)
- Eurocrypt 2017, 15-18 May, Paris (France)
  - Michel Abdalla (GC)
  - Jean-Sébastien Coron & Jesper Buus Nielsen (PC)
- Crypto 2017, 20-24 Aug. (tent.), UCSB, Santa Barbara
  - Steve Myers (GC)
  - Jonathan Katz & NN (PC)
  - IACR Distinguished Lecture by Shafi Goldwasser

Future conferences

- Asiacrypt 2017, 3-7 Dec., Hong Kong (HK)
  - Duncan Wong & SM Yiu (GC)
  - Tsuyoshi Takagi & NN (PC)

Future IACR-workshops

- CHES 2015, 13-16 Sep., St-Malo (FR)
  - E. Prouff, G. Renault & M. Rivain (GC)
  - Helena Handschuh & Tim Güneysu (PC)
- TCC 2016-A, 10-13 Jan., Tel Aviv (IL)
  - Ran Canetti & Iftach Haitner (GC)
  - Eyal Kushilevitz & Tal Malkin (PC)
- PKC 2016, 6-9 Mar., Taipei (TW)
  - Chen-Mou Cheng & Kai-Min Chung (GC)
  - Giuseppe Persiano & Bo-Yin Yang (PC)
- FSE 2016, 20-23 Mar., Bochum (DE)
  - Gregor Leander (GC)
  - Thomas Peyrin (PC)

Future IACR-workshops

- CHES 2016, 16-19 Aug., UCSB, Santa Barbara
  - Cetin Kaya Koc & Erkay Savas (GC)
  - Benedikt Gierlichs & Axel Poschmann (PC)
- **TCC 2016-B, Nov./Dec.**
  - Proposals being reviewed by TCC Steering Committee
- PKC 2017, March 28-31, Amsterdam (NL)
  - Marc Stevens (GC)
  - Serge Fehr (PC)

See you at the next event

- Barbecue at Goleta Beach, starting 18:00