International Association for Cryptologic Research

Christian Cachin
President, IACR

Crypto 2018

Membership meeting

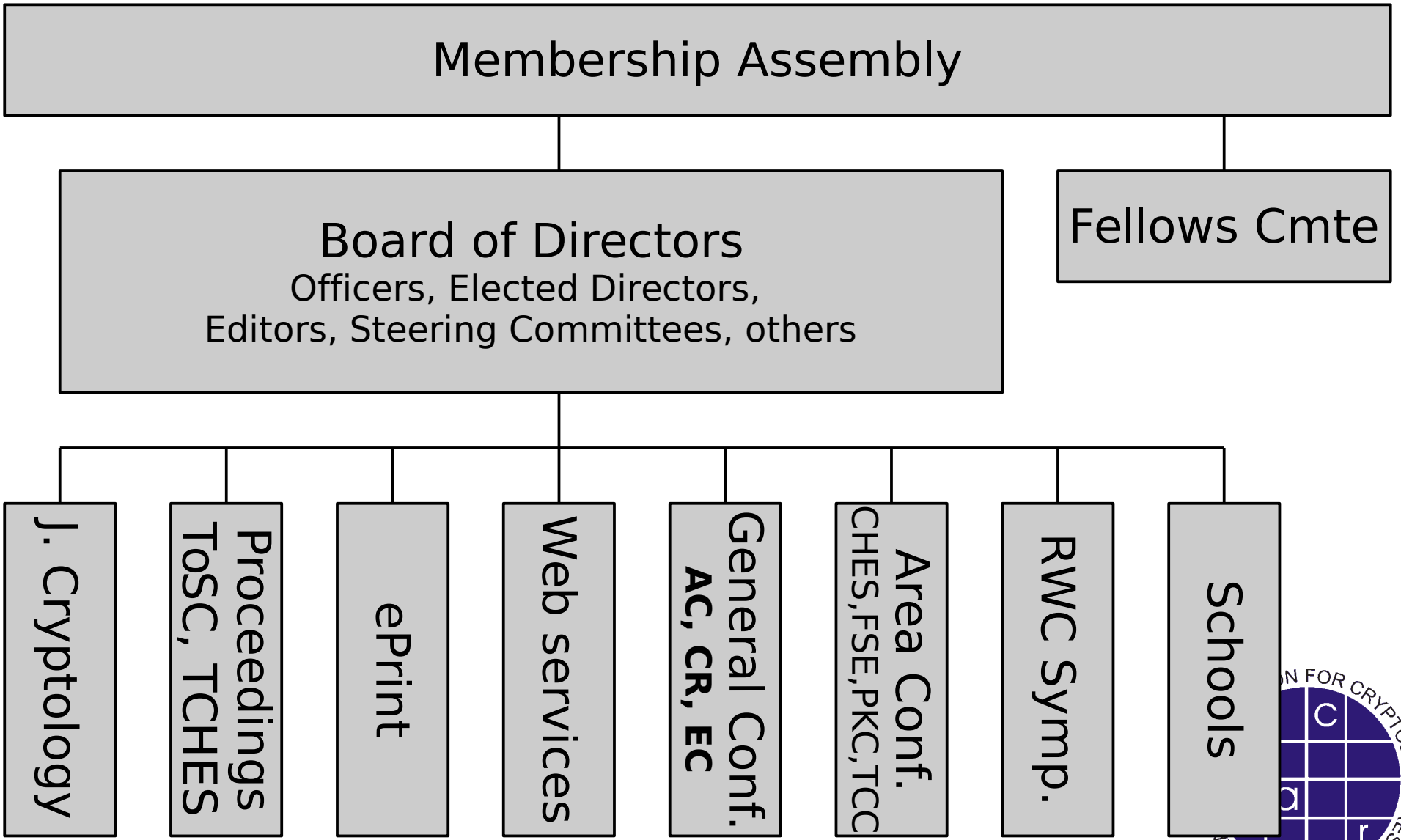
- About IACR
  - Publications
  - Conferences
  - Journal of Cryptology
- Financial report
- Membership report
- Online services
- Recent work in the Board
- Open discussion
- Future events

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)

- For all information – iacr.org/docs/

One picture


Membership Assembly
Board of Directors
Officers, Elected Directors,
Editors, Steering Committees, others
Fellows Cmte
J. Cryptology
Proceedings
ToSC, TCHES
ePrint
Web services
General Conf.
AC, CR, EC
Area Conf.
CHES,FSE,PKC,TCC
RWC Symp.
Schools

Membership

- Everyone attending an IACR event becomes a member in next calendar year
- Membership fee of $50 ($25 students)
- You can also become a member online
- If you did not attend a conference last year, renew your membership online for this year until September

Board of Directors

- 4 Officers
- 9 elected Directors
- Appointed Directors
  - Includes General Chairs of EC/CR/AC conferences
- Observers
  - Representing Steering Committees of Asiacrypt and Area Conferences (CHES, FSE, PKC, TCC, RWC)

- iacr.org/bod.html

- Each year we elect 3 Directors
  - Committee 2018, chair: Masayuki Abe
  - iacr.org/elections/2018/

Journal of Cryptology

- Current editor in Chief
  - Kenny Paterson
- Read online
  - iacr.org/publications/access.php
- Paper delivery is opt-in for ~~$20~~$40 extra
  - When you pay yearly membership
- Online submission reviewing system

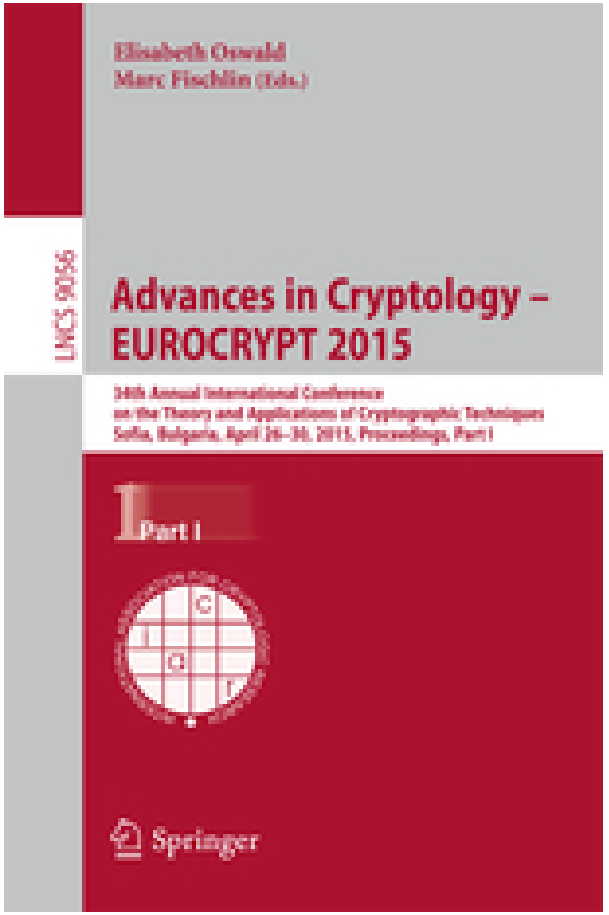
IACR Transactions on Symmetric Cryptology (ToSC)

- FSE-ToSC are a conference-journal hybrid
  - ToSC Publishes the proceedings of FSE
  - Publication in ToSC gives presentation at FSE
- Journal with rapid and strict review schedule
- Online only, published by IACR & RUB library
  - tosc.iacr.org
- **Gold open access**

IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)

- CHES-TCHES are a conference-journal hybrid
  - TCHES Publishes the proceedings of CHES
  - Publication in TCHES gives presentation at CHES
- Journal with rapid and strict review schedule
- Online only, published by IACR & RUB library
  - tches.iacr.org
- **Gold open access**

Conference proceedings



- ASIACRYPT
- CRYPTO
- EUROCRYPT
- PKC
- TCC

- Online for members
  - www.iacr.org/proceedings
- Online for all (≥ 3yr)
  - link.springer.com

Cryptology ePrint Archive

- eprint.iacr.org
- More than 1000 pre-prints per year
- Sasha Boldyreva & Tancrède Lepoint, editors

Cryptology schools

- IACR reviews proposals and supports some schools each year
  - Educational, typically 1-week, focus on learning (Summer/Winter/Spring/Fall school)
  - Financial support for speakers etc. and publicity
- Upcoming schools
  - Australian Summer School on Embedded Cryptography (Dec. 2018; Adelaide, AU)
  - 1st Crypto Innovation School (Nov./Dec. 2018; Shenzhen, CN)
- Next proposals are due December 31
  - IACR Schools Committee
  - www.iacr.org/schools/

IACR Distinguished Lecture

The annual IACR Distinguished Lecture is awarded by the IACR to people who have made important contributions to cryptology research.

The lecture alternates from Eurocrypt to Crypto to Asiacrypt.

2018, Asiacrypt – Mitsuru Matsui
2019, Eurocrypt – Cynthia Dwork

IACR Distinguished Lecture

The annual IACR Distinguished Lecture is awarded by the IACR to people who have made important contributions to cryptology research.

2020, Crypto – Silvio Micali

IACR Fellows

IACR Fellows are outstanding IACR members, recognized 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 – 2018

- Juan Garay
- Yuval Ishai
- Paul Kocher
- Stafford Tavares

Nominations for 2019 Fellows are due by
15 Nov 2018 !

Information will be on website later in the year
www.iacr.org/fellows/

Financial report

- Brian LaMacchia

Membership report

- Douglas Stebila

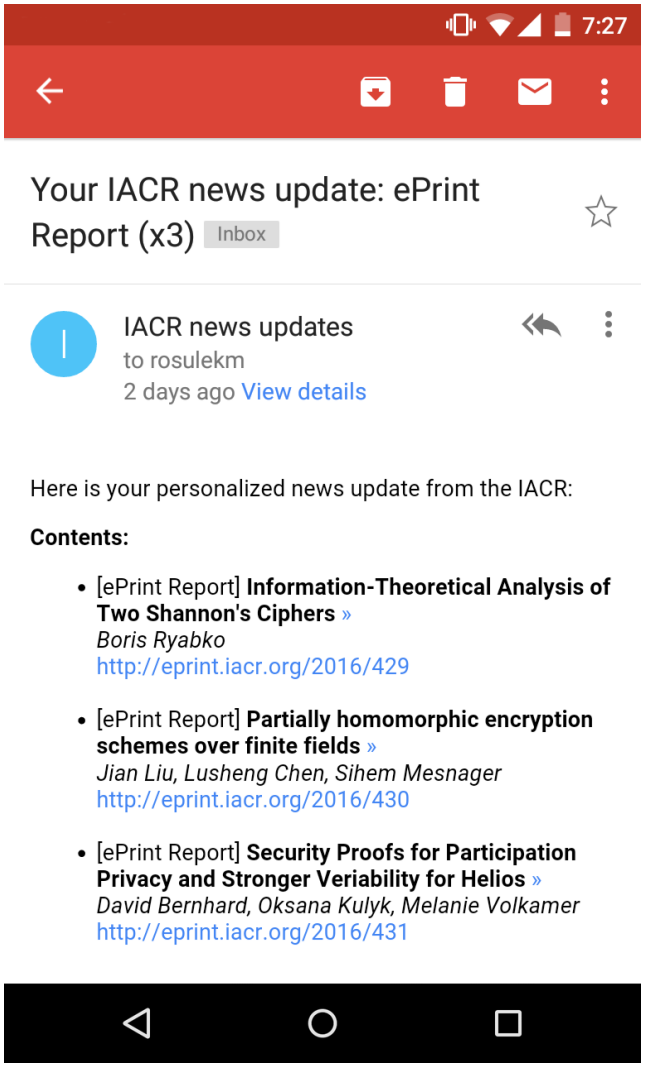
Online services

iacr.org
ia.cr

Mike Rosulek, Yu Yu

IACR news alerts

- Receive alerts about:
  - General announcements
  - New eprint reports
  - Job openings in cryptology
  - New events (conferences)
- Receive alerts via:
  - Facebook: fb.com/theiacr
  - Twitter: twitter.com/theiacr
  - Weibo: weibo.com/iacr
  - Email: iacr.org/news/subscribe



IACR publications portal

ia.cr/pubs

- Conference proceedings available:
  - all years: Publisher version, IACR members only
  - after 2 years: “IACR version”, public access
  - after 3 years: Publisher version, open access

All online services

- Cryptology ePrint Archive
- Access to proceedings (Springer & IACR versions)
- Open positions in cryptology
- Calendar of events
- Bibliography (CryptoDB), Petitions, PhD database ...

Cryptography Research Fund for Students

- With donation from CRI, IACR has created Cryptography Research Fund for Students
- Sponsors student participation at IACR events
  - Waive registration fee for student speakers at EUROCRYPT, CRYPTO, ASIACRYPT, CHES, FSE, TCC and PKC
  - Support for Cryptology Schools

Your IACR


We Need YOU
WE NEED YOU
WE NEED YOU
WE NEED YOU
We need YOU!
WE NEED YOU!
YOU
WE WANT YOU
WE NEED YOU To join OUR TEAM
WE NEED YOU
WE NEED YOU
We need you
WE NEED YOU!
WE NEED YOU!
WE NEED YOU
WE NEED YOU!
WE NEED YOU TO VOLUNTEER
WE WANT YOU!
WE WANT YOU
We NEED you!
We Need You!!!
WE NEED YOU
WE NEED YOU!
WE NEED YOU!
We Need Yo
VE NEED YOU
O MAKE IT HAPPE
We Need You!

Current topics

Recent work of the Board

- ... you can find the details here: iacr.org/docs/minutes/
- Have established a uniform Conflict-of-Interest policy
  - iacr.org/docs > Conflicts of Interest
- New Test-of-time Awards for Eurocrypt, Crypto, Asiacrypt (details still being worked out)
- New code of conduct
- Task force on diversity

Task force on diversity

- Established a task force to
  a) support women attending IACR events
  b) promote and support IACR and other events that advance diversity (defined broadly)
  c) improve diversity, especially representation of women and people from Asia, within IACR governance

- Volunteers wanted!
  - Contact Tal Rabin & Douglas Stebila

Code of conduct

- You have seen this already, but all events of the IACR must state this from now on:

  The IACR is committed to providing an experience free of harassment and discrimination in its events, respecting the dignity of every participant.

  Participants who violate this code may be sanctioned and/or expelled from the event, at the discretion of the General Chair(s). Serious incidents may be referred to the IACR Ethics Committee for further possible action.

  (...)

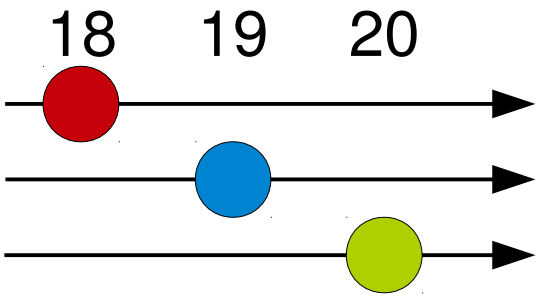
Ethics committee

- One case of harassment at a recent conference
- Plagiarism case (ban to submit to IACR for 1 year)
- Case of harassment of young B by more senior A

International ? A. C. R.

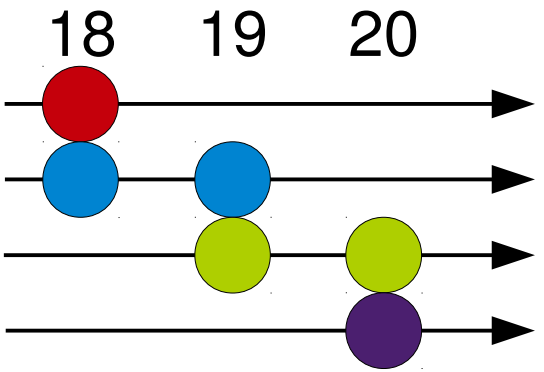
- Diversity of countries
- United States has recently increased requirements for business visitors

Program co-chair model



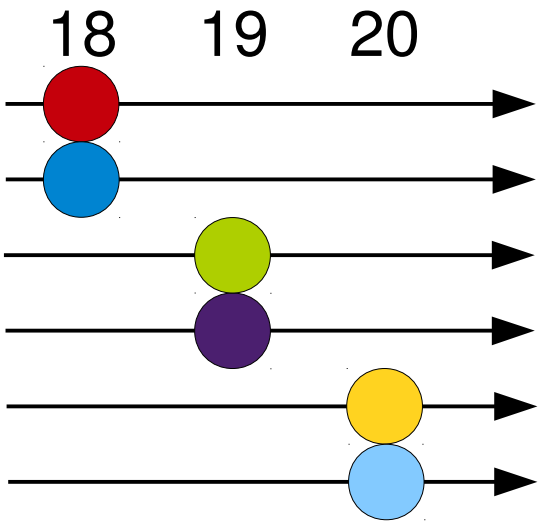
Single chair

until 2009



Rolling co-chair

TODAY



Parallel co-chair

DISCUSSION

Open discussion

Upcoming events

Future General Conferences

- Asiacrypt 2018, 2-6 Dec, Brisbane (AU)
  - Josef Pieprzyk (GC)
  - Thomas Peyrin & Steven Galbraith (PC)
  - IACR Distinguished Lecture by Mitsuru Matsui

Future General Conferences

- Eurocrypt 2019, 19-23 May, Darmstadt (DE)
  - Marc Fischlin (GC)
  - Vincent Rijmen & Yuval Ishai (PC)
- Crypto 2019, late Aug, UCSB, Santa Barbara
  - Muthu Venkitasubramaniam (GC)
  - Sasha Boldyreva & Daniele Micciancio (PC)
- Asiacrypt 2019, 8-12 Dec, Kobe (JP)
  - Mitsuru Matsui (GC)
  - Steven Galbraith & Shiho Moriai (PC)

Future General Conferences

- Eurocrypt 2020, Zagreb (Croatia)
  - Lejla Batina & Stjepan Picek (GC)
  - Yuval Ishai & Anne Canteaut (PC)
- Crypto 2020, late Aug, UCSB, Santa Barbara
  - NN (GC)
  - Daniele Micciancio & NN (PC)
- Asiacrypt 2020, 6-10 Dec, Daejeon (KR)
  - Kwangjo Kim (GC)
  - Shiho Moriai & NN (PC)

Future Area Conf. & Symp.

- CHES 2018, 9-12 Sep, Amsterdam (NL)
  - Ileana Buhan & Peter Schwabe (GC)
  - Matthieu Rivan & Daniel Page (PC/EiC)
- TCC 2018, 11-14 Nov, Goa (IN)
  - Shweta Agrawal & Manoj Prabhakaran (GC)
  - Amos Beimel & Stefan Dziembowski (PC)

Future Area Conf. & Symp.

- RWC 2019, 9-11 Jan, San Jose (US)
  - Dan Boneh (GC)
- FSE 2019, 25-28 Mar, Paris (FR)
  - Jérémy Jean (GC)
  - Florian Mendel & Yu Sasaki (ToSC EIC)
- PKC 2019, April 14-17, Beijing (CN)
  - Xiaoyun Wang (GC)
  - Dongdai Lin & Kazue Sako (PC)
- CHES 2019, 24-28 Aug, Atlanta (US)
  - Vincent Mooney, Patrick Schaumont, Yunsi Fei (GC)
  - Jorge Guajardo & Pierre-Alain Fouque (TCHES EiC)