International Association for Cryptologic Research

Christian Cachin
President, IACR

Crypto 2017

Membership meeting

- About IACR
  - Publications
  - Conferences
  - Journal of Cryptology
- Financial report
- Membership report
- Online services
- Symposium on Real-World Cryptography
- Transactions on Cryptographic Hardware and…
- Conflict-of-interest policies
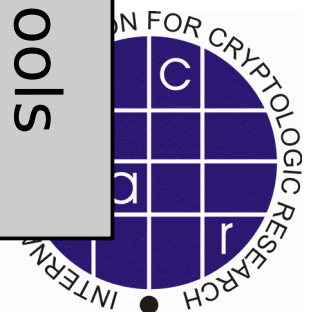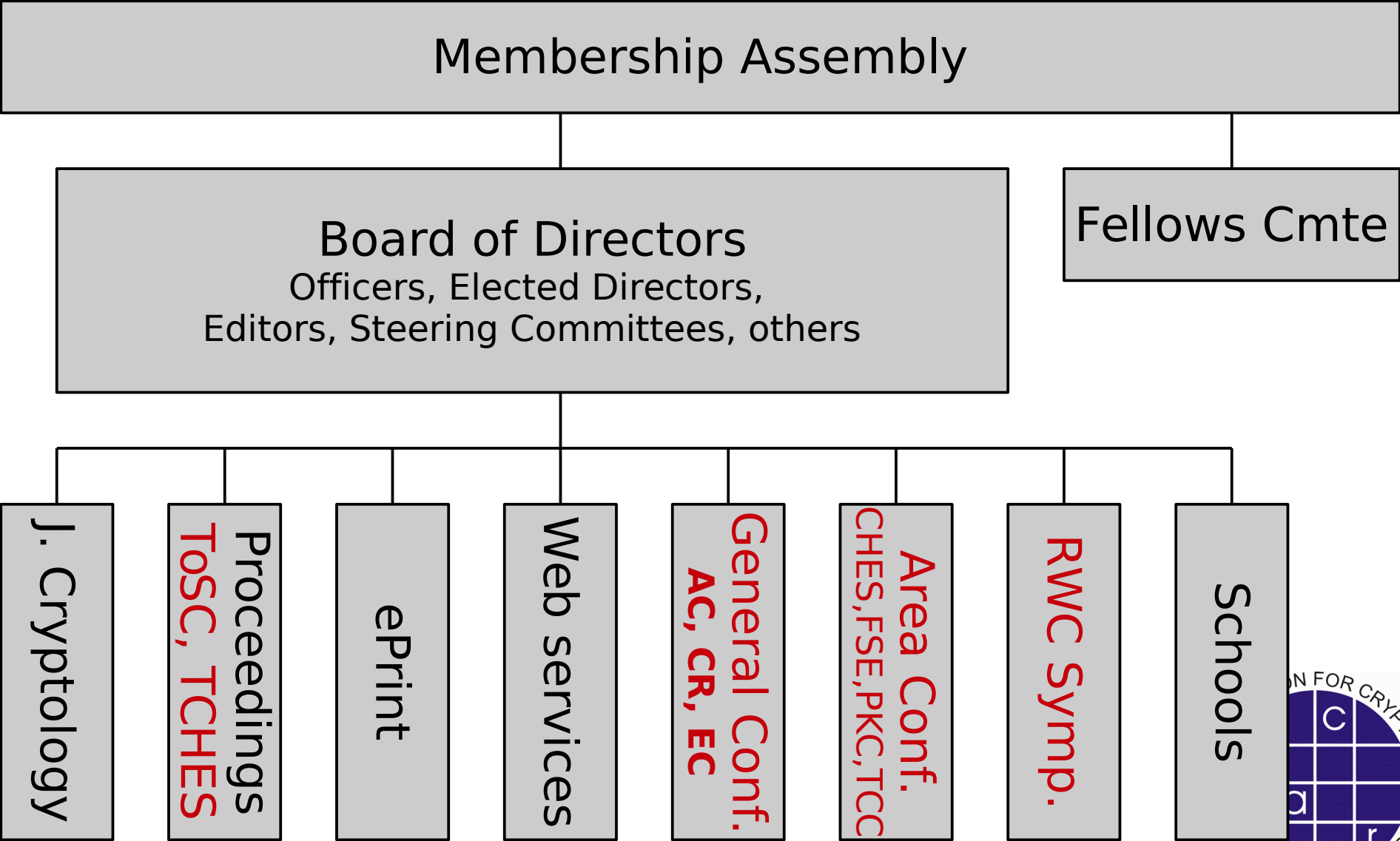- Open discussion
- Future events

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

- Everyone attending an IACR event becomes a member in next calendar year

- Membership fee of $50 ($25 students)

- Become a member online

- If you don't attend a conference in a calendar year, renew your membership online 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)

- www.iacr.org/bod.html

- In-person meetings at Eurocrypt and Crypto

Journal of Cryptology

- Current editor in Chief
  - Kenny Paterson

- Read online
  - www.iacr.org/publications/access.php

- Paper delivery is opt-in for $20 extra
  - When you pay yearly membership

- Online submission reviewing system

IACR Transactions on Symmetric Cryptology (ToSC)

- New in 2017, replacing Proceedings of FSE

- Journal with rapid and strict review schedule

- Online only, published by IACR & RUB library

  - tosc.iacr.org

- **Gold open access**

- Publication in ToSC gives presentation at FSE
  - Conference-journal hybrid (PVLDB, PoPETS ...)

ToSC operation

- **Editors in Chief for 2017**
  - Florian Mendel & María Naya-Plasencia

- **Schedule**
  - 4 submission deadlines/year and 4 review periods

  - Decision after approx. 2 months
    - Accept
    - Conditional accept
    - Major revision ($\rightarrow$ must resubmit after 3 or 6 months; decision will be accept or reject, not another revision)
    - Reject (a different paper can be submitted later)

  - Papers accepted by January 20xx must be presented at FSE 20xx

IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)

- New in 2018, replacing Proceedings of CHES

- Journal with rapid and strict review schedule

- Online only, published by IACR & RUB library
  - tches.iacr.org

- **Gold open access**

- Publication in ToSC gives talk at CHES
  - Conference-journal hybrid (PVLDB, PoPETS …)

- First submissions due 15 Oct 2017

TCHES operation (like ToSC)

- Editors in Chief for 2018
  - Matthieu Rivan & Daniel Page

- Yearly schedule
  - 4 submission deadlines and review periods
    - 15-Apr / 15-Oct / 15-Jan / 15-Apr

  - Decision after approx. 2 months
    - Accept
    - Conditional accept/minor revision
    - Major revision ($\rightarrow$ must resubmit after 3 or 6 months; decision will be accept or reject, not another revision)
    - Reject (a different paper can be submitted later)

  - Papers accepted by July 20xx to be presented at CHES 20xx

Conference proceedings
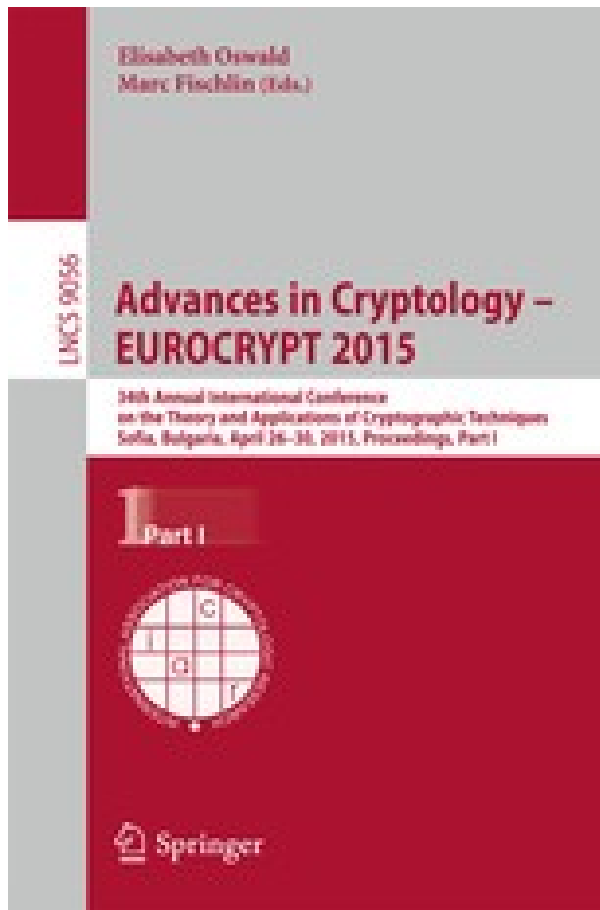
- ASIACRYPT
- CRYPTO
- EUROCRYPT
- PKC
- TCC

- 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, 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
  - www.iacr.org/schools/

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 – 2017

- Jan Camenisch
- Louis Guillou
- Kwangjo Kim
- Christof Paar
- Kenneth G. Paterson

Nominations for 2018 Fellows due by 31 Dec.

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

Finanical report

- Brian LaMacchia

Membership report
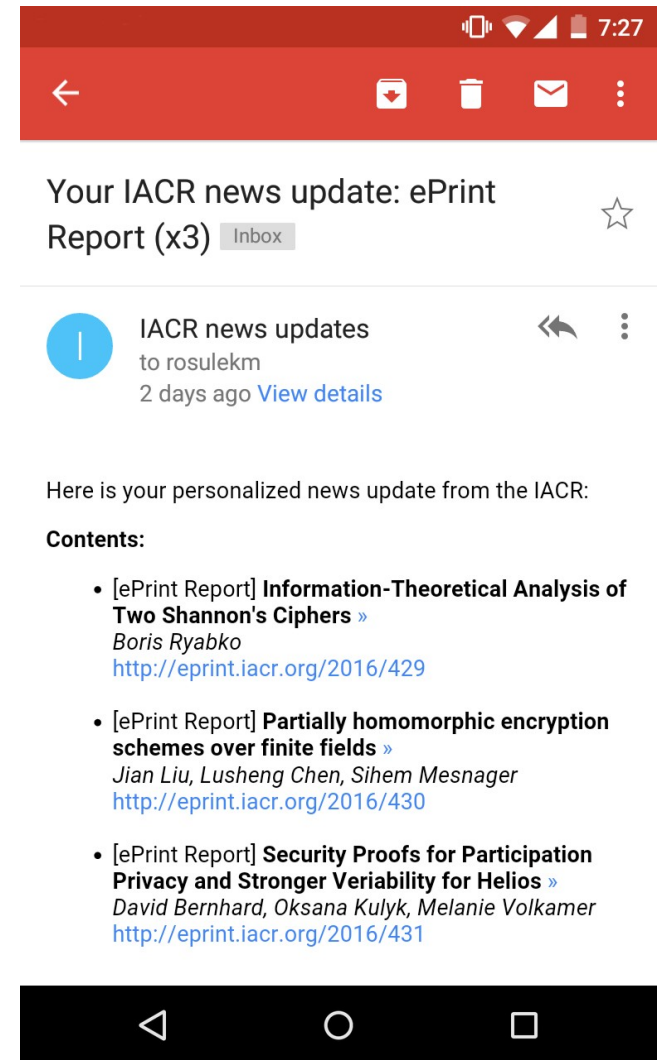
- Douglas Stebila

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

Your IACR news update: ePrint Report (x3) [Inbox]

IACR news updates
to rosulekm
2 days ago View details

Here is your personalized news update from the IACR:

Contents:

- [ePrint Report] **Information-Theoretical Analysis of Two Shannon's Ciphers** »
  Boris Ryabko
  http://eprint.iacr.org/2016/429

- [ePrint Report] **Partially homomorphic encryption schemes over finite fields** »
  Jian Liu, Lusheng Chen, Sihem Mesnager
  http://eprint.iacr.org/2016/430

- [ePrint Report] **Security Proofs for Participation Privacy and Stronger Veriability for Helios** »
  David Bernhard, Oksana Kulyk, Melanie Volkamer
  http://eprint.iacr.org/2016/431

IACR publications portal

ia.cr/pubs

- Conference proceedings available:
  - all years: Springer version, IACR members only
  - after 2 years: "IACR version", public access
  - after 3-4 years: Springer version, open access

All online services

- Cryptology ePrint Archive

- Access to proceedings (Springer & IACR versions)

- Open positions in cryptology

- Calendar of events

- Museum of historic papers

- 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

Videos & presentations

- Parallel sessions make it more important to have recordings

- Publication on Youtube channel
  - www.youtube.com/user/TheIACR
  - Thanks to Kevin McCurley for many hours of work!

- IACR consent & copyright form asks for permission to release
  - Video recording of talk (voice vs. full video)
  - Presentation material (static PDF)

- IACR decided in 2016 that recording and publi-cation of video and presentation occurs by default
  - with exceptions possible

Video maintainer needed

- Help all General Chairs with format

- Process recordings

- Publish on current channel

- Archive for future use

- Please come talk to me (president@iacr.org)

Current topics

2017 Elections

- Yearly election of 3 Director positions
  - www.iacr.org/elections/2017

- Schedule
  - Aug-Sep 24: Nomination phase
  - Oct-Nov: Online election using Helios

- Committee
  - **Tal Rabin**, Michel Abdalla, Bart Preneel

Symposium on Real-World Cryptography (RWC)

- Started as "Real-World Cryptography Conference"
  - Small workshop 2012, enormous growth until 2017

- Not another academic conference!
  - Industry – academia dialogue
  - Researchers, developers, operators, users ... of cryptography in real-world systems.
  - Collection of invited and contributed talks

- RWC has merged with IACR to form
  - IACR Symposium on Real-World Cryptography
  - rwc.iacr.org

- Next RWC will be 10-12 Jan 2018, Zurich (CH)

Conflict of interest policy

- Current guidelines for IACR conference PC:

  - Editor/PC decides on what constitutes a conflict according to high standards of scientific integrity
    - Attempt to avoid conflicts of interest by not assigning submissions to friends, colleagues, students, or PhD advisors of any of the authors.

- Board has decided to revise this policy, make it more precise and more prominent

Policy CRYPTO 2017

- The following constitutes a conflict of interest
  - Colleagues from the same institution as any of the authors
  - Current or recent (< 1 year) student/advisor or postdoc/advisor relationship
  - Family member

Policy ACM CCS 2016

- A conflict (...) includes anyone with close personal or professional relationship to any of the authors, such as
  - close family members,
  - people from the same department/group,
  - and recent collaborators (e.g. collaborated on a joint paper in the last two years).
- It also includes anyone in a position of substantial influence on (or by) the authors, such as advisor or advisee (at any time in the past), line-of-management relationship, grant program manager, etc.

Principles for an IACR CoI policy suggested by Board

- A reviewer has an automatic conflict with an author if they
  - Were advisor/advisee at any time;
  - Shared institutional affiliation within 2 years;
  - Published $\geq$ 2 papers in the prior 3 years;
  - Are in the same family.

- Detailed document is being created and will be published

- See also related policies
  - IEEE S&P http://www.ieee-security.org/TC/SP2017/cfpapers.html
  - ACM TOPS http://tops.acm.org/conflict-of-interest.cfm
  - ACM SIGPLAN conferences http://sigplan-pages.sigplan.hosting.acm.org/Resources/Policies/Review/

Board discussions

- Directors and officers are elected by membership
  - Should there be limits on number of terms?

- How to run conferences carbon-neutral?
  - Virtual events? offering carbon-compensation option? place IACR reserves in sustainable investments?

Open discussion

Upcoming events

Cryptology Schools 2017

- Advanced School of Cryptography 2017 (ASCcrypto)
  - 17-19 Sep 2017, Havana, Cuba
  - http://latincrypt.matcom.uh.cu/content/ascrypto-2017

Future General Conferences

- Asiacrypt 2017, 3-7 Dec, Hong Kong (HK)
  - Duncan Wong & SM Yiu (GC)
  - Tsuyoshi Takagi & Thomas Peyrin (PC)
  - asiacrypt.iacr.org/2017/

- Eurocrypt 2018, 29 Apr-3 May, Tel Aviv (IL)
  - Orr Dunkelman (GC)
  - Jesper Buus Nielsen & Vincent Rijmen (PC)
  - eurocrypt.iacr.org/2018/

Future General Conferences

- Crypto 2018, 19-23 Aug, UCSB, Santa Barbara
  - Tal Rabin (GC)
  - Hovav Shacham & Sasha Boldyreva (PC)

- 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 & NN (PC)

- Asiacrypt 2019, 8-12 Dec, Kobe (JP)
  - Mitsuru Matsui (GC)
  - Steven Galbraith & NN (PC)

Future Area Conf. & Symp.

- ## CHES 2017, 25-28 Sep, Taipei (TW)
  - Bo-Yin Yang & Chen-Mou Cheng (GC)
  - Naofumi Homma & Wieland Fischer (PC)

- ## TCC 2017, 12-15 Nov, Baltimore (US)
  - Abhishek Jain (GC)
  - Yael Kalai & Leonid Reyzin (PC)

- ## RWC 2018, 10-12 Jan, Zurich (CH)
  - Emilia Käsper & Anja Lehmann (GC)

Future Area Conf. & Symp.

- FSE 2018, 5-7 Mar, Bruges (BE)
  - Elena Andreeva (GC)
  - Florian Mendel & María Naya-Plasencia (ToSC EIC)

- PKC 2018, 25-28 Mar, Rio de Janeiro (BR)
  - Ricardo Dahab (GC)
  - Michel Abdalla (PC)

- CHES 2018, 9-12 Sep, Amsterdam (NL)
  - Ileana Buhan & Peter Schwabe (GC)
  - Matthieu Rivan & Daniel Page (PC/EiC)

- TCC 2018, 12-14 Nov (tent.), Goa (IN)
  - Shweta Agrawal & Manoj Prabhakaran (GC)
  - Amos Beimel & Stefan Dziembowski (PC)

Future Area Conf. & Symp.

- FSE 2019, 25-87 Mar, Paris (FR)
  - Jérémy Jean (GC)
  - NN (ToSC EIC)

See you at Goleta Beach