International Association for Cryptologic Research

Christian Cachin
President, IACR

EUROCRYPT 2015

Membership meeting

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

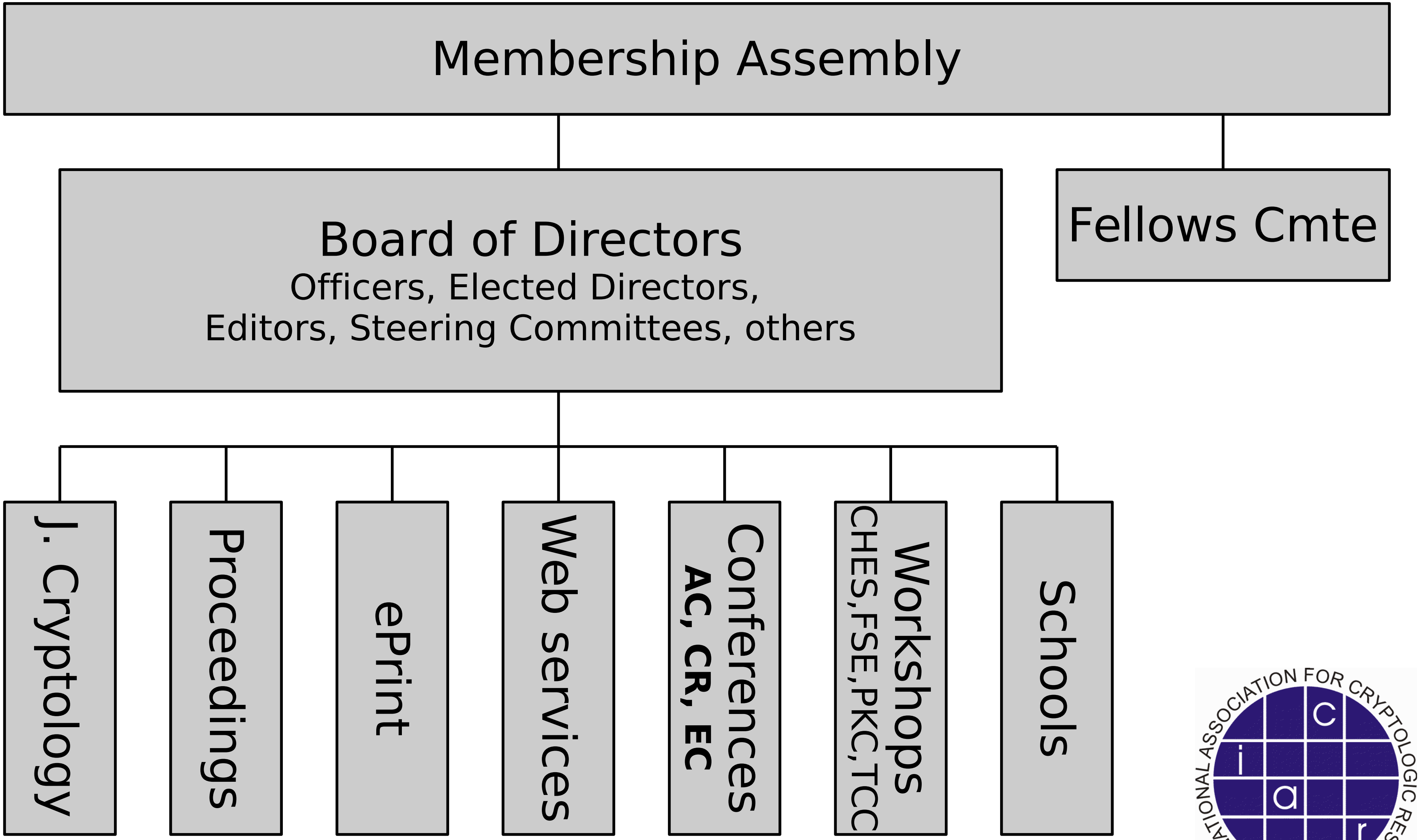
- Financial report
- Membership report

- Parallel sessions
- Submissions and publications
- 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

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 will appear later
    - www.iacr.org/elections/2015/
  - Using Helios online voting

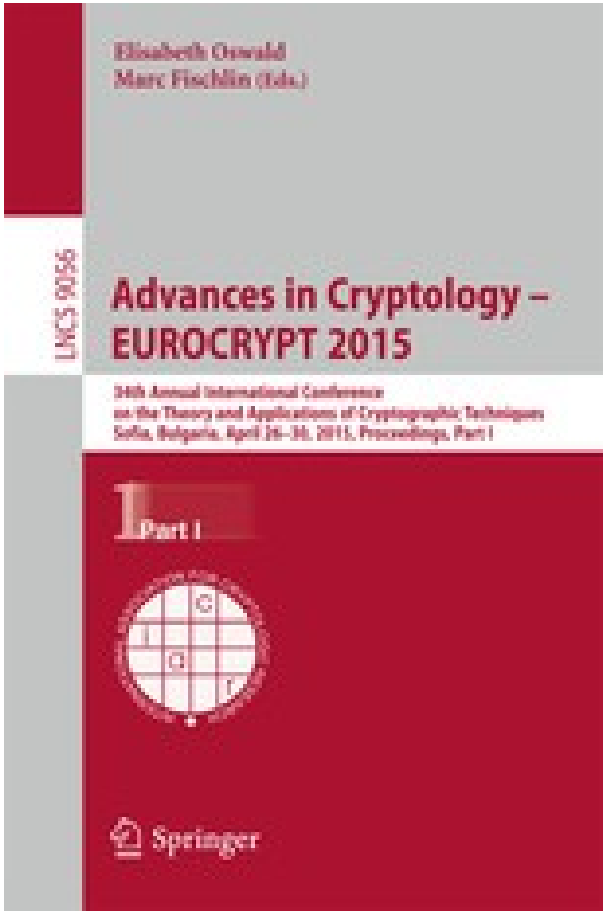
Journal of Cryptology

- Editor in Chief
  - Ivan Damgård

- Paper delivery is opt-in
  - Being implemented now

  - Online submission and reviewing system

Proceedings



Elisabeth Oswald
Marc Fischlin (Eds.)

LNCS 9056

Advances in Cryptology –
EUROCRYPT 2015

34th Annual International Conference
on the Theory and Applications of Cryptographic Techniques
Sofia, Bulgaria, April 26–30, 2015, Proceedings, Part I

Part I

Springer

- 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 June 30
  - Committee chaired by Michel Abdalla
  - http://www.iacr.org/schools/

Cryptology Schools 2015

- School on Computer-aided Cryptography, 1-4 June, 2015, College Park (US)
  - http://www.easycrypt.info/trac/wiki/SchoolUMD2015

- SAC Summer School, 10-12 Aug. 2015, Sackville (CA)
  - http://mta.ca/sac2015/s3.html

- 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

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/

Online services

- IACR news and announcements
- Cryptology ePrint Archive
  - Tal Rabin & Nigel Smart
- Online access to proceedings
- Calendar of events
- Open positions
- Book reviews
  - Edoardo Persichetti
- Ph.D. genealogy database
- Bibliography (CryptoDB)
- IACR Archive

Communications

- Communications secretary and webmaster

Mike Rosulek

Yu Yu

More volunteers needed!

- Content administration
  - Ph.D. database
- 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 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

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

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

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

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

Publisher

- IACR will soon revisit its choice of publisher
  - Current agreement with Springer for proceedings in LNCS until end of 2016

- FSE intends to become a journal-style conference from 2017 on
  - Similar to VLDB, PoPETS, JETS

- Re-assessment is therefore necessary

FSE publication after 2017

- 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)

Current discussion

- Would other IACR workshops (CHES, TCC, PKC) follow FSE to become a journal in the VLDB model?

- Would IACR conferences (EC, CR, AC) follow?
  - See discussion about "Strawman proposal for Proceedings of the IACR" in 2013

- What kind of publications and proceedings?

- What cost? Who pays?

Open discussion

Future conferences

- 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)
- Eurocrypt 2016, 8-12 May, Vienna (Austria)
  - Krzysztof Pietrzak (GC)
  - Marc Fischlin and Jean-Sébastien Coron (PC)

Future conferences

- Crypto 2016, 14-18 Aug., UCSB, Santa Barbara
  - Brian LaMacchia (GC)
  - Matt Robshaw and Jonathan Katz (PC)

- Asiacrypt 2016, 4-8 Dec., Hanoi (Vietnam)
  - Phan Duong Hieu & Ngo Bao Chau (GC)
  - Jung Hee Cheon & Tsuyoshi Takagi (PC)

- Eurocrypt 2017 ???
  - A proposal is in preparation

- Eurocrypt 2018 ???
  - If interested, then talk to a member of the Board

Future conferences

- Crypto 2017, 20-24 Aug. (tent.), UCSB, Santa Barbara

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

Future 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 workshops

- CHES 2016, late 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

- Banquet at 20:00