International Association for Cryptologic Research

Michel Abdalla
IACR President

Eurocrypt 2025

Membership meeting agenda

- About IACR
  - Publications
  - Conferences
  - Services
  - Awards
- Membership report
- Financial report
- Recent developments
- Open discussion
- IACR events

IACR

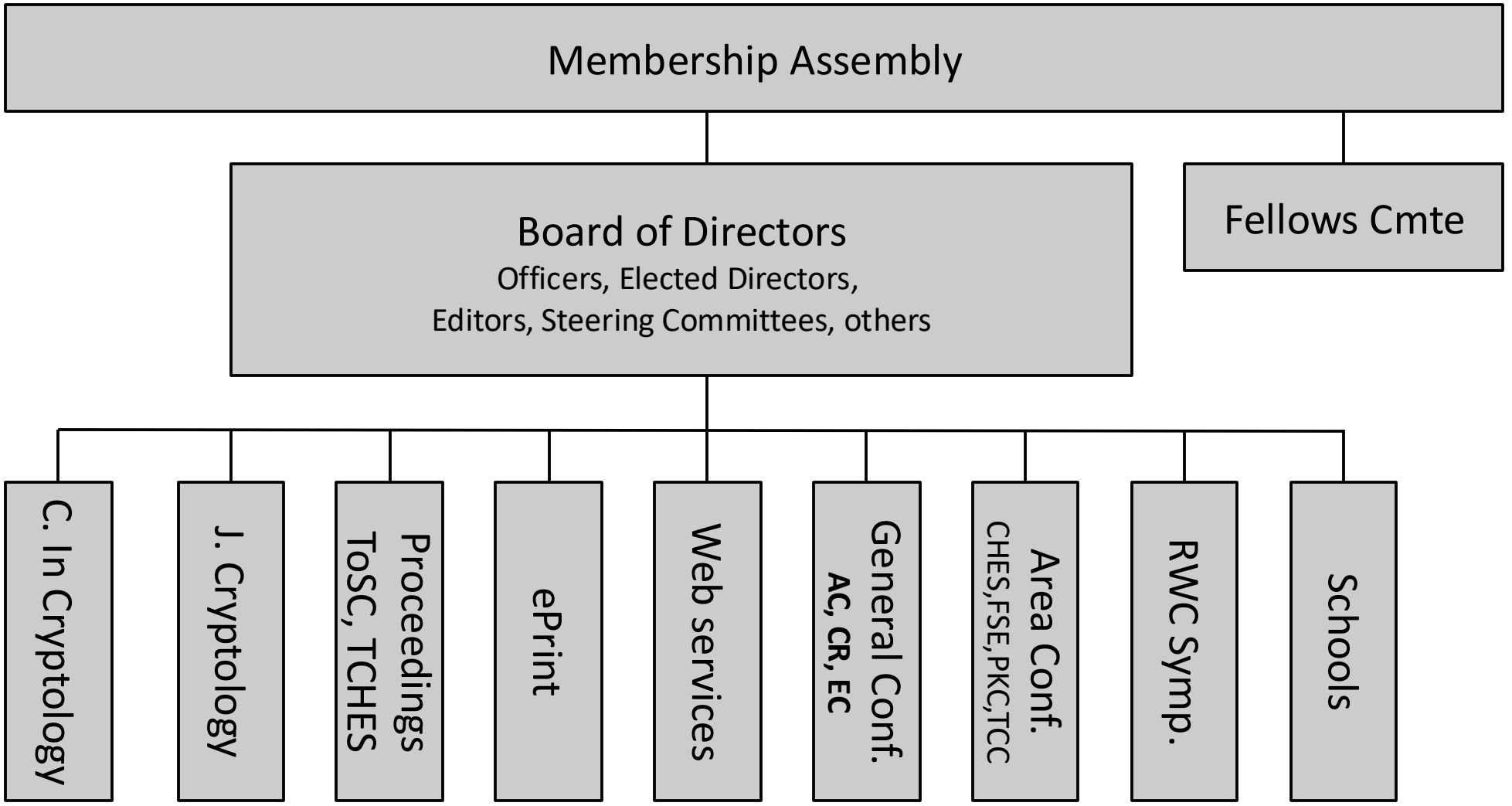
- International Association for Cryptologic Research

The IACR is a non-profit organization devoted to supporting the promotion of the science of cryptology.

  - Purpose is to further research in cryptology and related fields
  - Founded in 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
C. In Cryptology
J. Cryptology
Proceedings
ToSC, TCHES
ePrint
Web services
General Conf.
AC, CR, EC
Area Conf.
CHES,FSE,PKC,TCC
RWC Symp.
Schools

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

- 4 Officers and 3 Directors will be elected in 2025
  - iacr.org/elections/2025/

IACR Publications

- Journal of Cryptology - https://iacr.org/jofc
- Conference-journal hybrids
  - Published by IACR & RUB library
  - **ToSC** - IACR Transactions on Symmetric Cryptology - tosc.iacr.org
  - **TCHES** - IACR Transactions on Cryptographic Hardware and Embedded Systems - tches.iacr.org
- IACR Communications in Cryptology - https://cic.iacr.org/
- Conference proceedings
  - Published by Springer
  - ASIACRYPT, CRYPTO, EUROCRYPT, PKC, TCC
- Cryptology ePrint Archive - eprint.iacr.org

Online services (iacr.org, ia.cr)

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

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

- Recent and Upcoming schools
  - **ASCrypto 2025: Advanced School on Cryptology and Information Security in Latin America**
    Sep 29-30, 2025, Medellin, Colombia
  - **IACR Summer School on Security and Privacy 2025**
    Sep 1-5, 2025, Graz, Austria
  - **Spring School on Symmetric Cryptography 2025**
    March 10–14, 2025, Rome, Italy

- Next proposals are due **June 30th**
  - IACR Schools Committee
  - https://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.

2024, Asiacrypt – Paul Kocher

2025, Eurocrypt – Kenny Paterson

2026, Crypto – Joan Daeman

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.

- https://iacr.org/fellows/

IACR Fellows – 2025

Joan Daemen

Thomas Johansson

Anna Lysyanskaya

Pascal Paillier

J.R. RAO

Alon Rosen

Elaine Shi

Bo-Yin Yang

IACR Test-of-Time Award

- Given yearly for each one of the three IACR General Conferences
  - Eurocrypt, Crypto, and Asiacrypt
- For a paper with a lasting impact on the field
- Award at conference Y-crypt in year X to honor a paper published at Y-crypt in year X - 15
- Selected by a yearly committee
  - Two members appointed by Board
  - Three program chairs of year X
- https://iacr.org/testoftime/

IACR Test-of-Time Award 2025

- On Ideal Lattices and Learning with Errors over Rings
  - Vadim Lyubashevsky, Chris Peikert and Oded Regev
  - Eurocrypt 2010

The RSA Conference (RSAC) Award for Excellence in Mathematics

- An annual award given at the RSA conference
- Co-sponsored by the IACR

RSAC Award 2025

Shai Halevi

- For remarkable contributions to many areas of cryptography, including fundamental theory, advanced cryptographic primitives, secure multi-party computations, homomorphic encryption, and cryptographic code obfuscation

Victor Shoup

- For multiple influential contributions to cryptography, spanning both theoretical and practical aspects

Membership report

Bertram Poettering

Financial report

Brian LaMacchia

Current topics

Recent work in the Board

- Find details online: iacr.org/docs/minutes/
- Planning for increasing scale of paper submissions
- Possible reorganization of the publication landscape
- Policies, guidelines, statements
- Strategic planning at Crypto 2024 and Eurocrypt 2025
- Monthly virtual online meetings

Strategic planning meetings

- Identify short and long terms goals for the IACR
  - Necessary strategic needs, strongly desired, good to have

- Topics
  - **Planning for increasing scale of paper submissions**
  - **Potential staffing and operational resilience**
  - Publication models
  - Policies and guidelines

The Challenge Raised By Growth

Conflicts:

- 20% and above acceptance rates for flagship conferences
- Relatively low registration fees and manageable numbers of tracks
- 25-minute presentations allocated to each paper

Some alternatives:

- Decreasing acceptance rates
- Increasing registration fees and parallel tracks
- De-coupling papers from presentations

Currently working on possible proposals to discuss with the membership.

Policies, guidelines, statements

- Working on a new policy on statements by the board
- Code of conduct Revision

Call for Volunteers

IACR could use some more volunteer help on several fronts!

- Technical operations:
  - Useful skills:
    - python (to work on publish.iacr.org)
    - PHP and/or javascript (to work on hotcrp extensions)
    - Large language models/LLaMA (to work on copy editing tools)

  ➔ Contact Kevin McCurley (iacrcc@digicrime.com)

- Code of Conduct (potential expansion to a committee):
  - Seeking volunteers across a wide range of seniority

  ➔ Contact Tal Rabin

Open discussion

Thank you for your attention!