International Association for Cryptologic Research

Michel Abdalla
IACR President

Bo-Yin Yang
IACR Director

Asiacrypt 2024

Membership meeting agenda

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

IACR

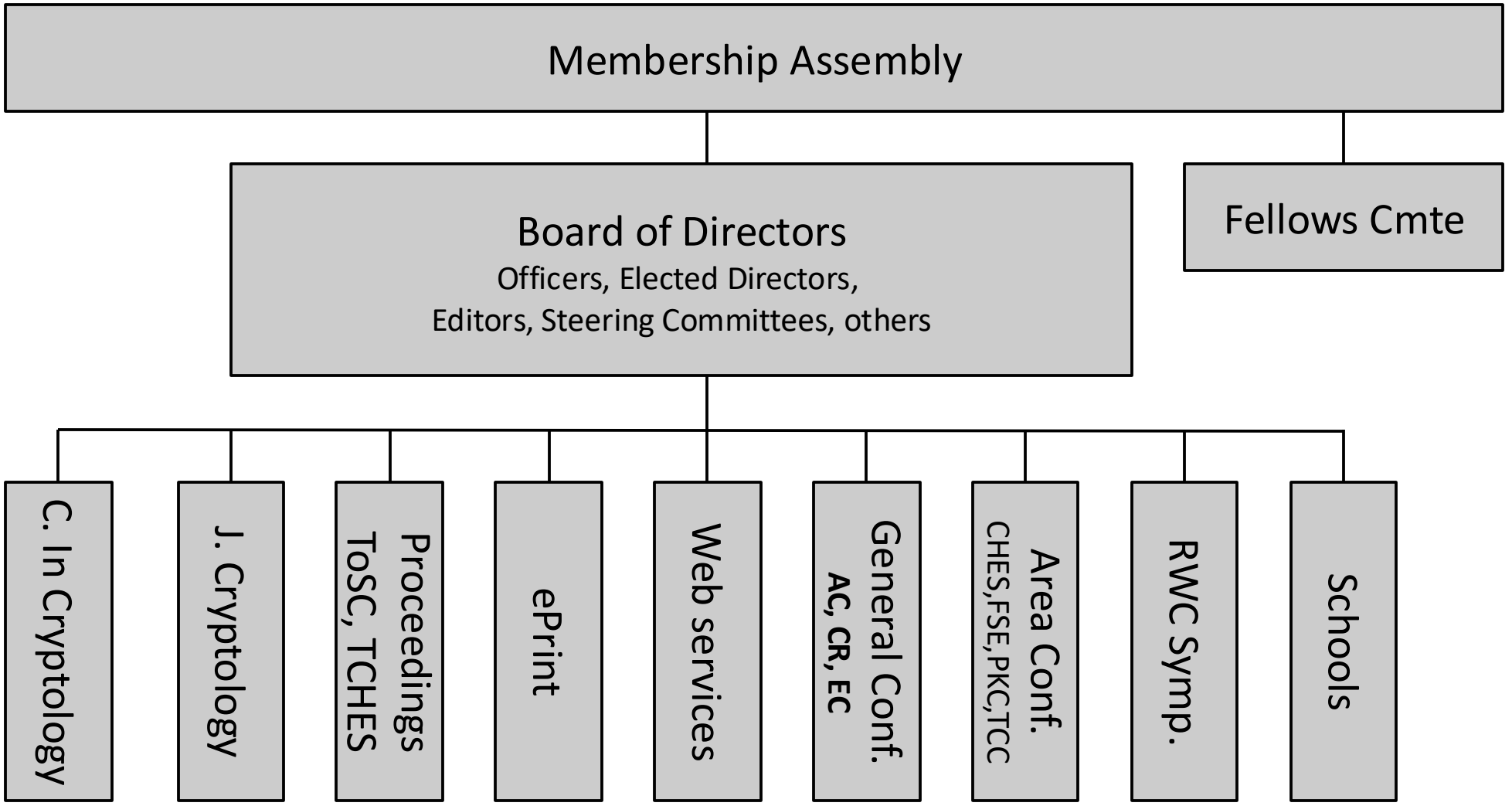
- International Association for Cryptologic Research

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

- 3 Directors were re-elected in 2024
  - iacr.org/elections/2024/

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
  - **Spring School on Symmetric Cryptography 2025**
    March 10–14, 2025, Rome, Italy
  - **Summer School on Security, Privacy and Correctness**
    Sept 23–27, 2024, Graz, Österreich
    Foundations and Applications of Zero-Knowledge Proofs
    Sept 2–6, 2024, Edinburgh, UK

- Next proposals are due **December 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.

2023, Crypto – Hugo Krawczyk

2024, Asiacrypt – Paul Kocher

2025, Eurocrypt – Kenny Paterson

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 – 2024

AnneCanteaut

Joan Feigenbaum

Alfred Menezes

Kobbi Nissim

Chris Peikert

David Pointcheval

François-Xavier Standaert

Brent Waters

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 2024

- A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks
  - François-Xavier Standaert, Tal G. Malkin, Moti Yung
  - Eurocrypt 2009
- Reconstructing RSA Private Keys from Random Key Bits
  - Nadia Heninger & Hovav Shacham
  - Crypto 2009
- Dual-System Encryption
  - Brent Waters
  - Crypto 2009

IACR Test-of-Time Award 2024

- Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures
  - Vadim Lyubashevsky
  - Asiacrypt 2009
- Efficient public key encryption based on ideal lattices
  - Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, Keita Xagawa
  - Asiacrypt 2009

The RSA Conference (RSAC) Award for Excellence in Mathematics

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

RSAC Award 2024

- Craig Gentry and Oded Regev
- For major contributions to Lattice-Based Encryption, especially for the highly utilized `Learning with Error' based cryptosystem, and the first 'Fully Homomorphic Encryption' cryptosystem

Membership report

Bertram Poettering

Financial report

Brian LaMacchia

IACR events


INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
c
i
a
r

2024 General Conferences

- Eurocrypt 2024, 26 – 30 May, Zurich, Switzerland
  - Julia Hesse and Thyla van der Merwe (GC)
  - Marc Joye & Gregor Leander (PC)

- Crypto 2024, 18 – 22 Aug, UCSB, Santa Barbara (US)
  - Tancrède Lepoint (GC)
  - Leo Reyzin & Douglas Stebila (PC)

- Asiacrypt 2024, 9 – 13 Dec, Kolkata, India
  - Bimal Kr. Roy (GC)
  - Kai-Min Chung & Yu Sasaki (PC)

2025 General Conferences

- Eurocrypt 2025, 5 – 8 May, Madrid, Spain
  - Dario Fiore (GC)
  - Serge Fehr & Pierre-Alain Fouque (PC)

- Crypto 2025, Aug, UCSB, Santa Barbara (US)
  - Francisco Rodríguez-Henríquez (GC)
  - Yael Tauman Kalai & Seny Kamara (PC)

- Asiacrypt 2025, Dec, Melbourne, Australia
  - Joseph Liu (GC)
  - Goichiro Hanaoka & Bo-Yin Yang (PC)

2024 Area Conf. & Symp.

- FSE 2024, 25-29 Mar, Leuven, Belgium
  - Svetla Petkova-Nikova, Siemen Dhooghe (GC)
  - Christina Boura, Kazuhiko Minematsu (ToSC EiC)
- RWC 2024, 25-27 Mar, Toronto, Canada
  - Douglas Stebila (GC)
  - Dan Boneh, Nadia Heninger (PC)
- PKC 2024, 15-17 April, Sydney, Australia
  - Willy Susilo, Fuchun Guo (GC)
  - Qiang Tang, Vanessa Teague (PC)

2024 Area Conf. & Symp.

- CHES 2024, 4-7 September 2024, Halifax, Canada
  - Colin O'Flynn, Hilary Taylor (GC)
  - Bo-Yin Yang, Francisco Rodriguez (TCHES EiC)

- TCC 2024, 2-6 December 2024, Milan, Italy
  - Emmanuela Orsini (GC)
  - Elette Boyle, Mohammad Mahmoody (PC)

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 Eurocrypt and Crypto 2024
- 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

If trends in rapid growth continue and we keep our current conferences and formats the same, the following will be in conflict:

- 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!