International Association for Cryptologic Research

Michel Abdalla
IACR President

Eurocrypt 2023

Membership meeting agenda

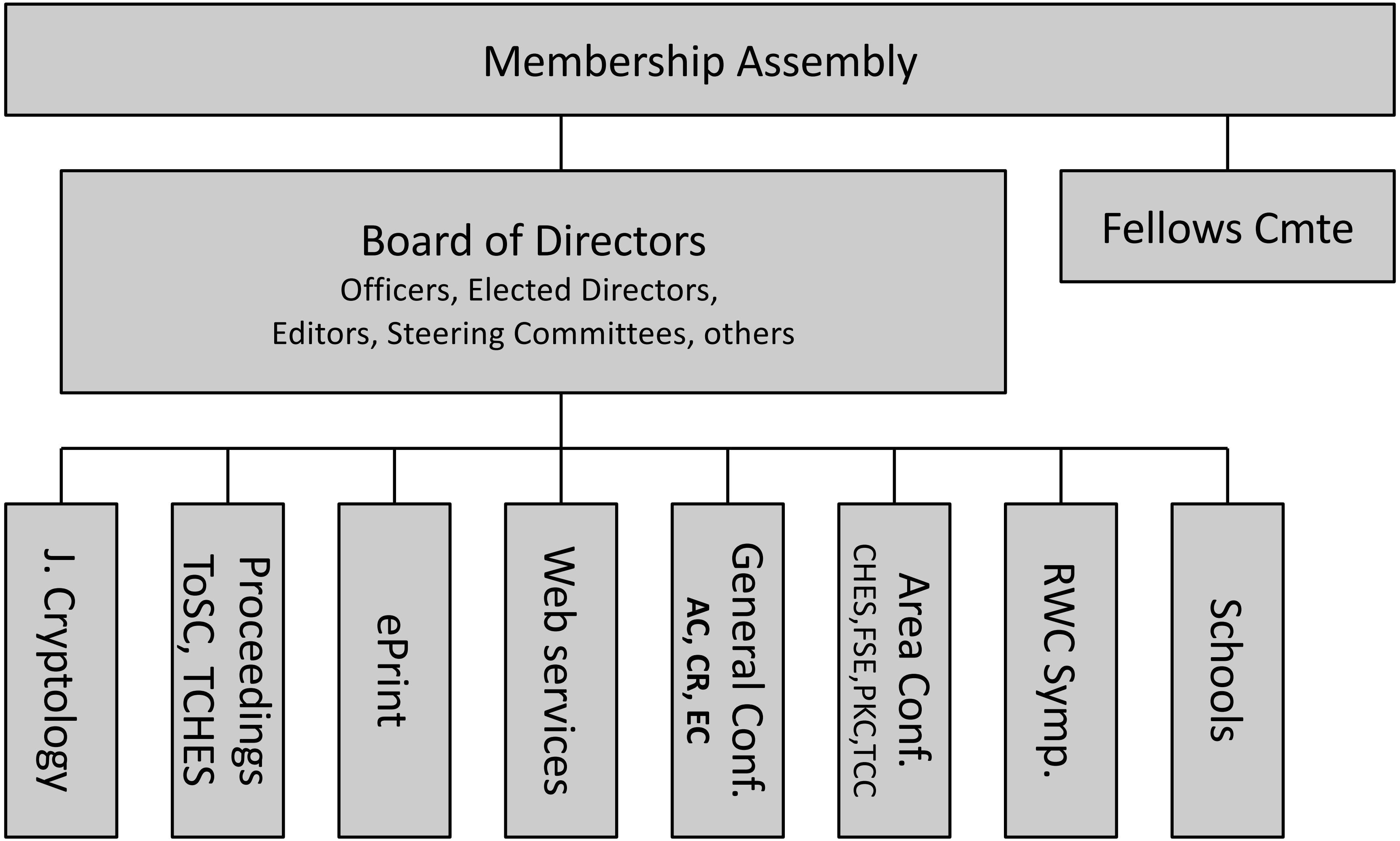
- About IACR
    - Publications
    - Conferences
    - Journal of Cryptology
- Financial report
- Membership report
- Online services
- Future events
- Recent developments
- Open discussion

IACR

- International Association for Cryptologic Research
  - 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

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 will be elected in 2023
  - iacr.org/elections/2023/

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 (in progress)
- Conference proceedings
  - Published by Springer
  - ASIACRYPT, CRYPTO, EUROCRYPT, PKC, TCC
- Cryptology ePrint Archive - eprint.iacr.org

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
  - Summer School on Privacy-Preserving ML, July 31st-August 3rd, 2023, Warsaw, Poland
  - Summer School on Security and Privacy, September 4-8, 2023, Graz, Austria
  - Summer School in PQC, August 1-5, 2022, Budapest, Hungary
  - Summer School on Privacy-Preserving ML, August 1-4, 2022, Copenhagen, Denmark
  - IACR-VIASM Summer School on Cryptography, August 24-30, 2022, Hanoi, Vietnam

- Next proposals are due June 30
  - 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.

2022, Eurocrypt – Ingrid Verbauwhede

2023, Crypto – Hugo Krawczyk

2024, Asiacrypt – Paul Kocher

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 – 2023

Jung Hee Cheon

Stanisław Jarecki

Marc Joye

Jesper Buus Nielsen

Rafael Pass

Giuseppe Persiano

Reihaneh Safavi-Naini

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 2023

- Efficient Non-interactive Proof Systems for Bilinear Groups
  - Jens Groth, Amit Sahai
  - Eurocrypt 2008
- On the Indifferentiability of the Sponge Construction
  - Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche
  - Eurocrypt 2008

Financial report

Brian LaMacchia

Membership report

Bertram Poettering

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 ...

Upcoming events

2022 General Conferences

- Eurocrypt 2022, 30 May – 3 Jun, Trondheim (Norway)
  - Colin Boyd (GC)
  - Orr Dunkelman & Stefan Dziembowski (PC)
- Crypto 2022, 14 – 18 Aug, UCSB, Santa Barbara (US)
  - Allison Bishop (GC)
  - Yevgeniy Dodis & Thomas Shrimpton (PC)
- Asiacrypt 2022, 4 – 8 Dec, Taipei (Taiwan)
  - Kai-Min Chung & Bo-Yin Yang (GC)
  - Shweta Agrawal & Dongdai Lin (PC)

2023 General Conferences

- Eurocrypt 2023, 24 – 27 April, Lyon, France
  - Damien Stehlé (GC)
  - Carmit Hazay & Martijn Stam (PC)

- Crypto 2023, 20 – 24 Aug, UCSB, Santa Barbara (US)
  - Britta Hale (GC)
  - Helena Handschuh & Anna Lysyanskaya (PC)

- Asiacrypt 2023, 4 – 8 Dec, Guangzhou, China
  - Jian Weng & Fangguo Zhang (GC)
  - Jian Guo & Ron Steinfeld (PC)

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, Aug, UCSB, Santa Barbara (US)
    - Tancrède Lepoint (GC)
    - Leo Reyzin & Douglas Stebila (PC)

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

2023 Area Conf. & Symp.

- FSE 2023, 20-24 Mar, Beijing, China + Kobe, Japan
  - Bin Zhang, Meiqin Wang (GC)
  - Christina Boura, Bart Mennink (ToSC EiC)

- RWC 2023, 27-29 Mar, Tokyo, Japan
  - Kazue Sako (GC)
  - Anja Lehmann (CTC), Nadia Heninger and Nick Sullivan (ITC)

- PKC 2023, 7-10 May, Atlanta, Georgia, US
  - Daniel Genkin, Joseph Jaeger (GC)
  - Sasha Boldyreva and Vladimir Kolesnikov (PC)

2023 Area Conf. & Symp.

- CHES 2023, 10 – 14 Sept, Prague, Czechia
  - Hana Kubátová & Martin Novotný (GC)
  - Diego F. Aranha & Marcel Medwed (TCHES EiC)

- TCC 2023, 29 Nov – 2 Dec, Taipei, Taiwan
  - Kai-Min Chung & Bo-Yin Yang (GC)
  - Guy Rothblum & Hoeteck Wee (PC)

Current topics

Recent work in the Board

- Find details online: iacr.org/docs/minutes/
- Co-sponsorship of the RSA Conf. Excellence in the Field of Mathematics Award
- New ePrint site
- New IACR journal
- Strategic planning

Strategic planning meeting at Eurocrypt 2023

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

- Topics
  - Organization’s vision and mission statements
  - Conference format - How to better handle growth
  - Reorganization of the publication landscape

Open discussion

Thank you for your attention!