# International Association for Cryptologic Research

Michel Abdalla
IACR President

Crypto 2025

# Membership meeting agenda

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

# IACR

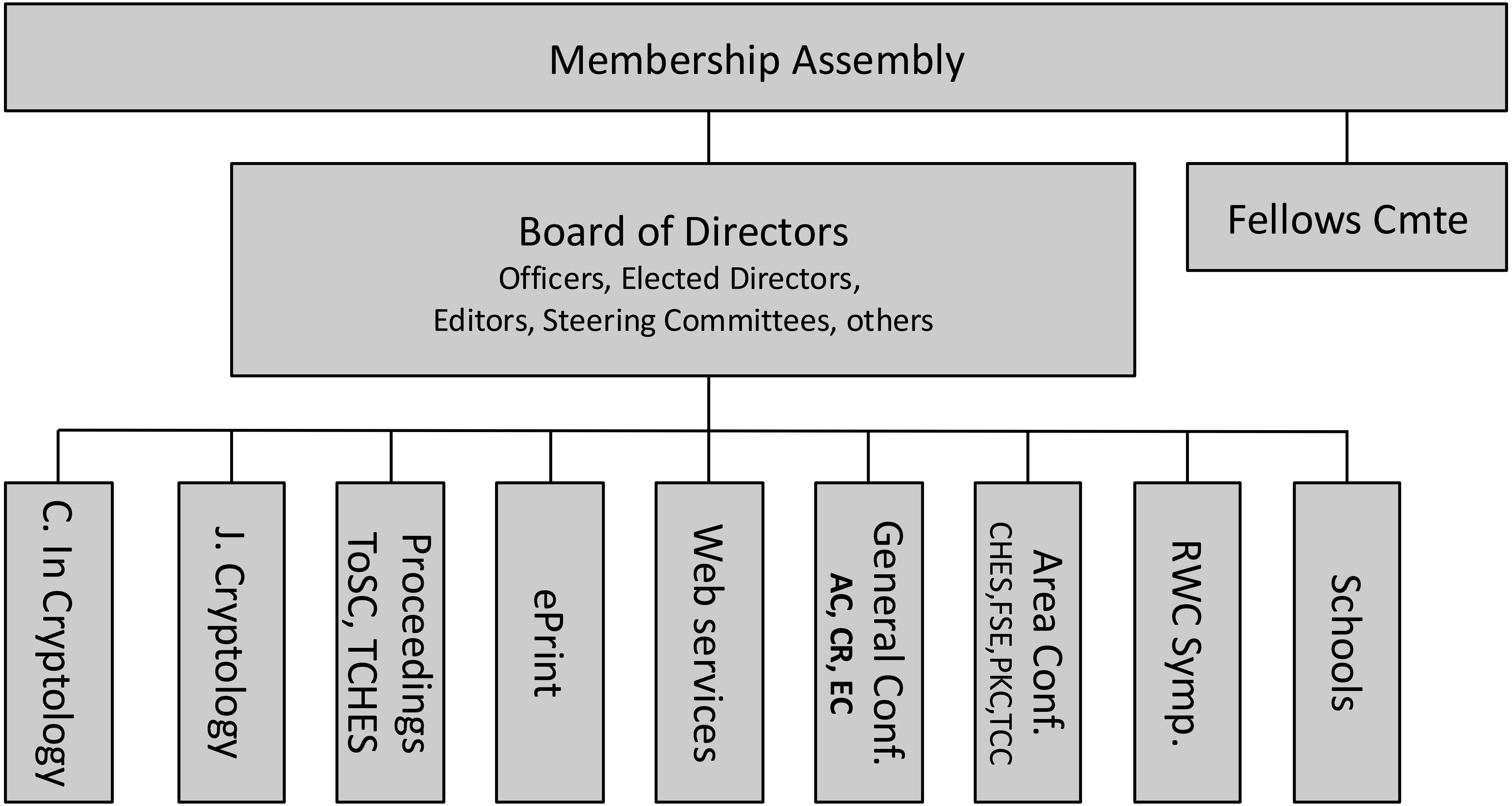
- International Association for Cryptologic Research

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

- 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

# 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 **December 31st**
  - 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

- Cryptographic Extraction and Key Derivation: The HKDF Scheme
  - Hugo Krawczyk
  - Crypto 2010

- Factorization of a 768-bit RSA modulus
  - horsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev and Paul Zimmermann
  - Crypto 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 2025 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
  - Potential relocation of Crypto

# Policies, guidelines, statements

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

# Changes for Crypto at UCSB for 2026-2028

- **Construction impacts**

  UCSB will be demolishing Santa Rosa Hall and replacing it with a new dorm starting in 2026. The construction is expected to last from June 2026 until Fall 2028, impacting Crypto for the next three summers. The current plan is for Crypto to use the Manzanita Village dorms during this time.

- **The “NUD”**

  UCSB’s administration has starting imposing a new surcharge – the “Non-University Differential” (a.k.a. the NUD) -- on the cost of certain UCSB services for non-University groups like the IACR.  The NUD for 2025 is ~26%, but for 2026 it will rise to about ~56.5%.  At present, for what we use at Crypto the impact is mostly to the cost of A/V services.

# Possibly moving away from UCSB

- The IACR’s needs as an organization are evolving
- Crypto 2025 received a record number of submissions and accepted a record number of papers
- UCSB has been the home for Crypto since the beginning and it has been an amazing venue
    - However, a renovation project starting in 2026 will affect running Crypto
    - Costs have also been increasing over the last few years
    - These trends suggest that it is time to have an open mind about other potential venues
- As a result, we are interested in proposals for other venues to host Crypto in 2027 or 2028, in addition to the proposal we already have from UCSB.
- If you are interested in submitting a proposal, please indicate interest by contacting the Board by September 30th, 2025; a complete proposal should be submitted to the Board by December 31, 2025.

# 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

➔ Member Survey on IACR Publishing and Conferences

# Survey – Question 1

*Should the IACR merge the proceedings of the three general conferences (Asiacrypt, Crypto, and Eurocrypt) into a single journal-style publication, with three deadlines throughout the year and maintenance of reviewing state throughout the year?*

- **For**: A consolidated reviewing process would reduce the overall burden of reviewing on the community. In particular, it would prevent papers from being freshly reviewed each time they are resubmitted within a year. If we introduce outcomes like Minor and Major Revision, reviewers and authors would be able to take their time and work together more effectively in producing a final version. This should also reduce randomness in outcomes.
- **Against**: Authors would lose the potential benefits of being able to resubmit and get different reviewers. Existing rankings of our current proceedings publications could be lost, potentially having a negative impact on junior researchers. Some submissions could experience an extended time to publication due to a lengthened revision cycle if revision options are overused. A large scale reviewing process for 1500+ submissions per year is hard and complex to manage.

# Survey – Question 2

*Should IACR pursue in-house open-access publishing for papers accepted at general conferences?*

- **For**: As our own publisher, IACR could provide open access and have full control over our publication pipeline and processes. The infrastructure for this has already been built for CiC. However, supporting IACR general conferences would introduce a new level of scaling. For more information about CiC infrastructure and how it manages to keep costs relatively low, see arXiv: 2504.10424. We could also potentially reduce the current complexity of having formally published versions, author versions, and eprint versions all as separate things maintained by separate entities.
- **Against**: Publishing on our own requires considerable resources, which may be difficult for us to maintain as a volunteer organization. We could potentially lose access to some older publications (pre-2013), and we would lose any benefits from current rankings and reputation that Springer provides. Note that this loss would be temporary until the new format becomes generally well-accepted both within and outside our community. Springer currently pays the IACR some amount per volume published, which helps defray some conference costs; if we no longer use Springer, we would lose that benefit. (The overall amount from Springer is about 2% of IACR’s revenue.) Though it is not open access, Springer does explicitly acknowledge eprint and everyone can make a free version of their paper available there.

# Survey – Question 3

*Consider a general conference in 5 to 10 years that receives 1200 submissions. Suppose that the acceptance rate is roughly what is typical today, resulting in about 250 accepted papers, and the conference will last 4 days (not including any affiliated events). Imagine you are attending in-person.*

- **Format A**: $2000 registration fee and 6 parallel tracks where each paper has a 20-minute slot
- **Format B**: $1200 registration fee and 3 parallel tracks where each paper has a 10-minute slot.
- **Format C**: $1200 registration fee with at most 3 parallel tracks. Every paper will have some opportunity to present, though the formats may vary (e.g., some talks, some Q&A sessions, maybe posters).
- **Format D**:  $1200 registration fee where not all accepted papers are presented. Those that are presented will have varying formats (see option C for examples).

# Survey – Question 4

*There is potential to incorporate a wider variety of presentation formats into our general conferences. For each option, please rate your preference for this option on a scale of 1 to 5 stars. A rating of 1 is lowest (ew!) while a rating of 5 is highest (yay!). You can also choose not to provide a rating for an option.*

- 10-minute talks
- 20-minute talks
- Invited talks
- Lightning talks (1-2 minutes)
- Poster sessions
- Panel discussions
- Other

# Survey – Question 5

*Should at least one author be required to attend a general conference in person?*

- **For**: In-person discussion and dissemination of research is a core engine of scientific progress in our community. Without requiring travel, conferences could lose key elements that make them effective and desirable to attend. Attendees who are particularly interested in a result might lose the chance to talk to an author about it. Junior researchers could miss out on important networking and mentorship opportunities if they and/or senior researchers opt out of travel in significant enough numbers. If travel is not required, those who want to travel but need approval to do so (i.e., from employers or funding bodies) might face greater difficulties in securing the necessary permissions and funding.
- **Against**: Requiring travel places an undue burden on many researchers, including those with limited financial resources, those with visa challenges, those with safety and health concerns, and those with caregiving responsibilities. The environmental impact of travel is also an unavoidable concern. There are alternative ways to disseminate research without travel (i.e., papers, recorded talks, virtual presentations), as well as alternative ways to facilitate collaboration and networking (e.g., discord channels, virtual meetups, mentoring networks).

# Open discussion

# Thank you for your attention!