International Association for Cryptologic Research

Michel Abdalla
IACR President

Eurocrypt 2022

Membership meeting agenda

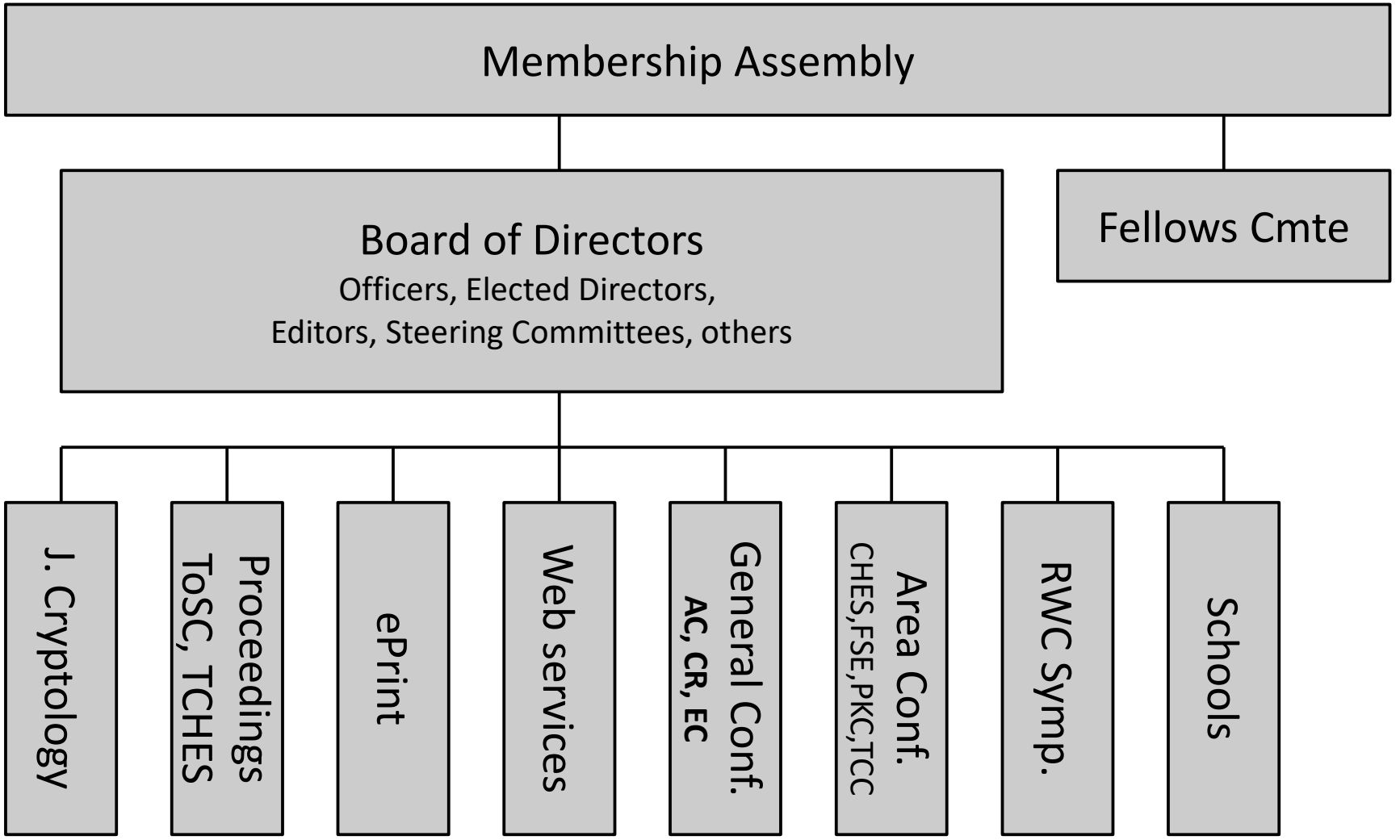
- About IACR
  - Publications
  - Conferences
  - Journal of Cryptology
- Financial report
- Membership report
- Online services
- Future events
- Recent developments
- Open discussion

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

- 4 officers and 3 Directors will be elected in 2022
  - iacr.org/elections/2022/

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
- 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

- Upcoming schools
  - PQC Mini-School 2022, July 12-15, 2022, Taipei, Taiwan
  - 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

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.

2022 IACR Fellows will be announced in a few weeks

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/

Test-of-time award 2022

- An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries
  - Yehuda Lindell, Benny Pinkas
  - Eurocrypt 2007
- Deterministic and Efficiently Searchable Encryption
  - Mihir Bellare, Alexandra Boldyreva, Adam O'Neill
  - Crypto 2007
- Faster Addition and Doubling on Elliptic Curves
  - Daniel J. Bernstein, Tanja Lange
  - Asiacrypt 2007
- https://iacr.org/testoftime/

Financial & Membership reports

Brian LaMacchia

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)

Future 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)

Future Area Conf. & Symp.

- CHES 2022, 18 – 21 Sept, Leuven, Belgium
  - Benedikt Gierlichs, Svetla Nikova (GC)
  - Sonia Belaïd & Thomas Eisenbarth (TCHES EiC)
- TCC 2022, 7 – 10 Nov, Chicago, USA
  - David Cash (GC)
  - Eike Kiltz, Vinod Vaikuntanathan (PC)
- RWC 2023, Mar, Tokyo, Japan
  - Kazue Sako (GC)
  - NN (PC)

Future Area Conf. & Symp.

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

- PKC 2023, May, Atlanta, Georgia, US
  - Daniel Genkin, Joseph Jaeger (GC)
  - Sasha Boldyreva and Vladimir Kolesnikov (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
- Creation of a new IACR journal

New IACR Journal

Joppe Bos

Discussion: Publication Venues and Proposed New IACR Journal

Mid 2020: The Board received a proposal for a new Journal from various members and decided to form a Committee to investigate the options: see https://tinyurl.com/36dcrbp7.

Original authors
Paulo Barreto
Seny Kamara
Michael Naehrig
Elisabeth Oswald
Tom Ristenpart
Nigel Smart

IACR New Journal Committee
Joppe Bos (chair)
Nadia Heninger
Anna Lysyanskaya
Kevin McCurley
Elisabeth Oswald
Bart Preneel
Peter Schwabe
Nigel Smart
Francois-Xavier Standaert
Moti Yung

Motivation for the new journal

The field of cryptography is growing → this is a good thing!

Perceived problems

- Increased reviewing load
  - Submission to multiple conferences (high rejection rates)
  - Submission to journal after published at a conference
- Limited number of slots at conference
  - Good papers sometimes rejected because of insufficient reviews, low confidence, etc
    → waste of everybody's time

Results

- Increased frustration of authors with reviewers, and vice-versa
- Re-submit acceptable papers numerous times
- Papers contain over-hyped claims to impress reviewers to get in
- Students spending travel budgets just to publish a paper
- Traveling for conferences **just** to publish a paper is bad for the environment, bad for diversity, and a bad use of tax-payer funded research dollars
- Conferences become dull as papers are selected due to publication as opposed to talk criteria

High-Level Goals – IACR Communications in Cryptology

- ✓ Diamond or Gold Open Access publishing model
- ✓ Fast and consistent turnaround time (decision in 3 months for regular paper)
- ✓ Allow for scaling to handle the current (and future) size of the field
- ✓ Respect all areas of the community (theory/applied/practice, symmetric/public key/ protocols/implementation, geographic area)
- ✓ Reduce overall reviewing load for our community
- ✓ Allow another outlet for our community to publish without the need to travel to conferences
- ✓ Not compete with but complement our successful flagship and area conferences (including the IACR transactions).

Ideology

If a paper contains an original contribution relevant to the field of cryptology,
then it should be accepted, irrespective of how many other strong papers are received.

Cost per Paper

Our goal / expectation for diamond open access: < 100 USD / paper (to be covered by the IACR, not the author)

Is this realistic?

- MSP charges about $32 per page
- American Astronomical Society charges $500/paper
- The American Meteorological Association charges $1100 + $120/page.
- The American Mathematical Society charges $750-$1500 per article for their journals.
- The ACM charges $700-1300 per article for members.
- SIAM charges $2885 per article.
- London Math Society charges $1250 per article for the Transactions
- Springer (Journal of Cryptographic Engineering) charges $2780 per article

New Journal – Practical Challenges

We discussed the requirements with several companies + publishers.

- Step 1. Submission and review system
  - HotCRP, OJS, other systems?

- Step 2. Editorial management system
  - Significant time to check final versions, can we automate more?
    → Currently on average <u>one hour</u> of a PhD students time to process each submitted final version for ToSC/TCHES
  - Extracting + collecting metadata?

- Step 3. Hosting system
  - Ourselves? Use existing solutions?

Progress update

Decision 2. *The Board agrees in principle to the creating of the New Journal where*

- *HotCRP is used for the submission and review step just as we do for the Transactions.*
- *The editing step is handled similar to how the Transactions handle this currently and then work towards automating this.*
- *The hosting step is performed by ourselves and build on top of the rework done for the ePrint archive.*
- *The Board appoints the Editors in Chief withing the next two months.*

Source: IACR Board Meeting Minutes February 17, 2022
https://iacr.org/docs/minutes/virtual-2_2022bod.pdf

Goal is to “present the full proposal to our membership and asks for approval in a referendum to the members” → make sure to vote

Mini FAQ

Q. Have you considered the impact on
(1) Eurocrypt / Asiacrypt / Crypto?
A. The new journal provides an additional venue which can appeal to authors who are unwilling or unable to publish in these venues. IACR conferences are much more than just publication outlets: they offer the opportunity for researchers to meet and network. The new journal will not take any of these opportunities away.

(2) The IACR Transactions: TCHES and ToSC?
A. The Transactions have been modelled on the success of other conference/journal hybrids. CHES and FSE are the top conferences in the two respective sub-fields. These conferences bring the respective communities together. The new journal will not replace the function of the associated area conferences. We do not see the new journal as affecting the standing of the journals TCHES and ToSC within their sub-communities.

(3) the “events in Cooperation with IACR” such as SAC, AfricaCrypt, Indocrypt, Latincrypt etc?
A. We envision that some of these events may wish to publish their proceedings as “special issues” of this new journal. Thus, the new journal may provide a mechanism for such venues to raise their perception of quality in terms of moving from a conference publication to a journal publication methodology and attract more submissions.

Mini FAQ

Q. Why not just adapt the way ToSC/TCHES are working for the other area conferences?

A. Whether TCC or PKC want to adopt the Transaction model is up to their steering committees. However, the four area conferences do not cover the widening scope of cryptologic research: indeed it never was the intention of the area conferences to cover all of cryptology.
Many interesting cryptographic papers often have no home amongst the existing IACR area conferences: for example some of the work presented at RWC. A venue needs to be found for publishing papers from those sub-areas not covered by the area conferences. Such sub-areas may come and go over time, so a single publication venue for the other sub-areas in cryptology is future proof.

Q. Why not just adapt the Journal of Cryptology?

A. "Adapting" JoC would inevitably mean that JoC in its current form would no longer exist because the setup of the new journal demands different processes regarding reviewing and publishing (including Diamond Open Access). JoC is a highly valued publication venue in our community, with an established review system and culture. The new journal is neither intended as a replacement of, nor as a competitor to JoC.

What do you think about this new IACR journal?

Let us know at: newjournal@iacr.org

Open discussion

Thank you for your attention!