

# International Association for Cryptologic Research

Michel Abdalla  
IACR President

Asiacrypt 2021



# Membership meeting agenda

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

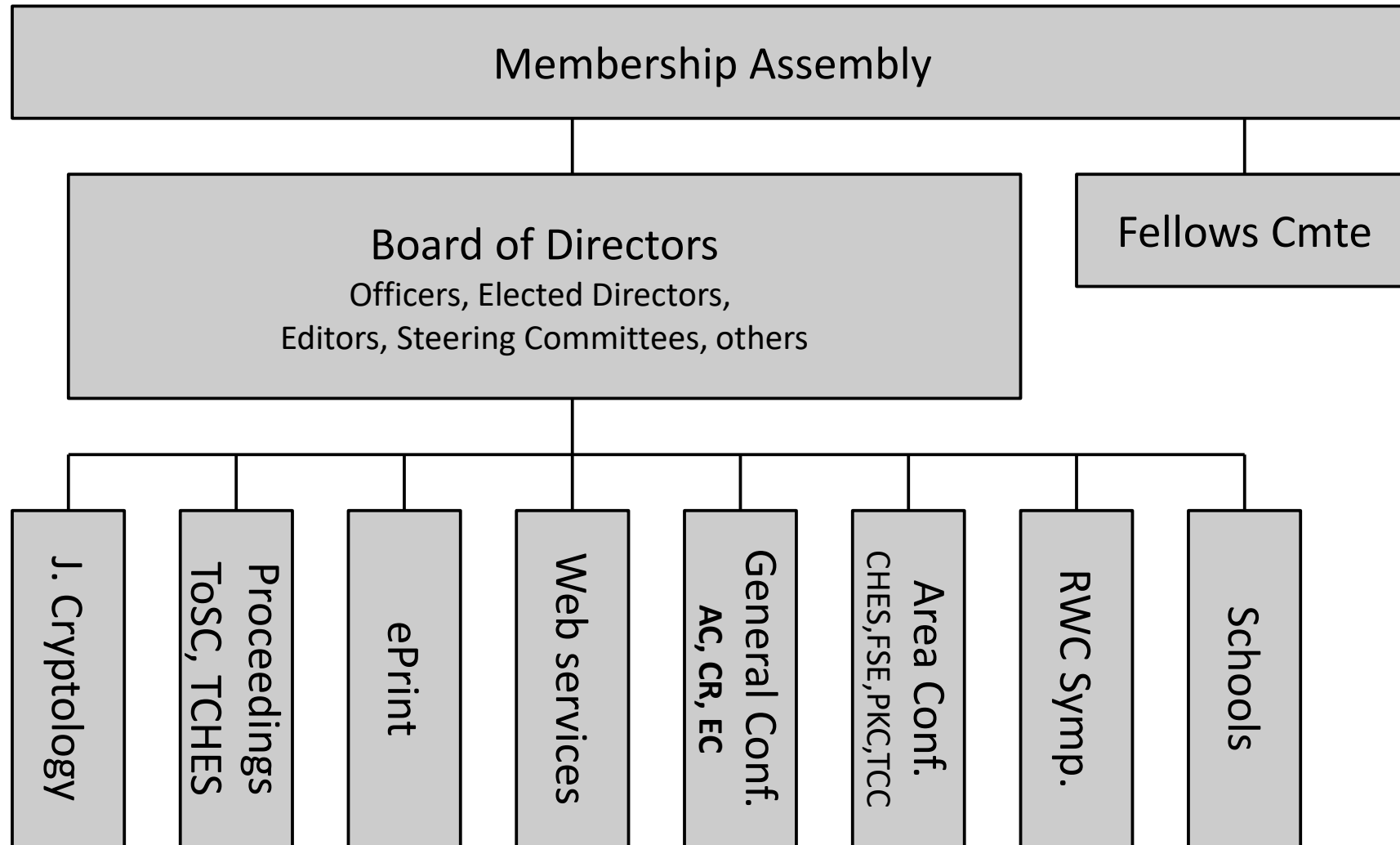


# IACR

- **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/](https://iacr.org/docs/)



# One picture



# Membership

- Everyone attending an IACR event becomes a member in the **next calendar year**
  - By attending Eurocrypt 2021, you become an IACR member for 2022
- Membership fee of **\$50** (**\$25** students)
- You can also become a member online
- If you **do not attend** a conference in **year Y**, you can renew your membership online for **year Y+1** until September



# 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](http://iacr.org/bod.html)
- Each year you elect 3 Directors
  - [iacr.org/elections/2021/](http://iacr.org/elections/2021/)
  - New elected directors: **Jian Guo, Anna Lysyanskaya, Bo-Yin Yang**



# 2021 IACR Board of Directors

## Officers

Michel Abdalla, President (2020-2022)  
Shai Halevi, Vice-President (2020-2022)  
Brian LaMacchia, Treasurer (2020-2022)  
Joppe Bos, Secretary (2020-2022)

## Directors

Masayuki Abe (2021-2023)  
Marc Fischlin (2020-2021)  
Nadia Heninger (2019-2021)  
Tancrede Lepoint (2021-2023)  
Anna Lysyanskaya (2019-2021)  
Bart Preneel (2020-2022)  
Peter Schwabe (2020-2022)  
Francois-Xavier Standaert (2020-2022)  
Moti Yung (2021-2023)

## Other Board Members

Foteini Baldimtsi, Communications Secretary (2019-2022)  
Lejla Batina, Eurocrypt 2021 General Chair (2019-2021)  
Allison Bishop, Crypto 2022 General Chair (2021-2022)  
Colin Boyd, Eurocrypt 2022 General Chair (2020-2022)  
Jian Guo, Asiacrypt 2021 General Chair (2020-2021)  
Vladimir Kolesnikov, Crypto 2021 General Chair (2020-2021)  
Vincent Rijmen, Editor-in-Chief, Journal of Cryptology (2021-2023)  
Douglas Stebila, Membership Secretary (2017-2022)  
Bo-Yin Yang, Asiacrypt 2022 General Chair (2021-2022)



# Journal of Cryptology



- Current Editor in Chief
  - **Vincent Rijmen**
- Read online
  - [iacr.org/publications/access.php](http://iacr.org/publications/access.php)
- Paper delivery is opt-in for **\$40** extra
  - When you pay yearly membership

<https://iacr.org/jofc/>





# IACR Transactions on Symmetric Cryptology (ToSC)

- FSE-ToSC is a conference-journal hybrid
  - ToSC Publishes the proceedings of FSE
  - Publication in ToSC gives presentation at FSE
- Journal with rapid and strict review schedule
- Online only, published by IACR & RUB library
  - [tosc.iacr.org](http://tosc.iacr.org)
- **Gold open access**

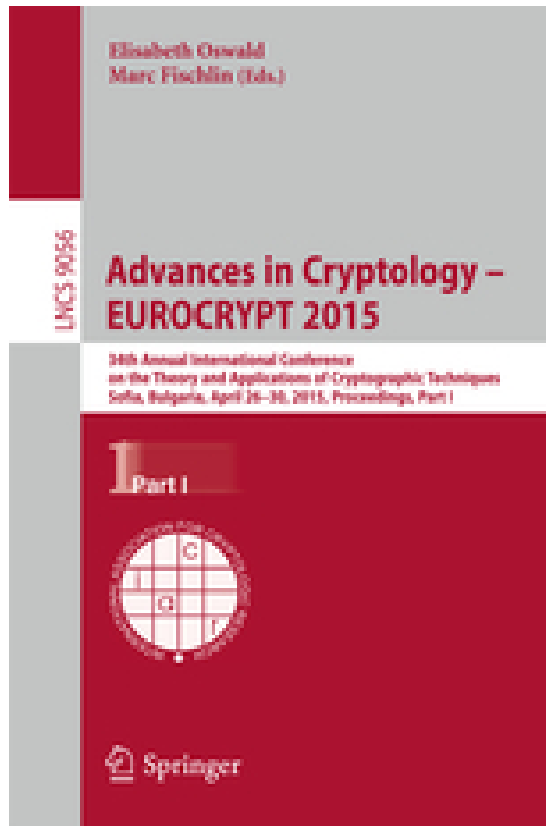


# IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)

- **CHES-TCHES is a conference-journal hybrid**
  - TCHES Publishes the proceedings of CHES
  - Publication in TCHES gives presentation at CHES
- Journal with rapid and strict review schedule
- Online only, published by IACR & RUB library
  - [tches.iacr.org](http://tches.iacr.org)
- **Gold open access**



# Conference proceedings



- ASIACRYPT
- CRYPTO
- EUROCRYPT
- PKC
- TCC
  
- Online for members
  - [www.iacr.org/proceedings](http://www.iacr.org/proceedings)
- Gold open-access  $\geq$  3yr
  - [link.springer.com](http://link.springer.com)



# Cryptology ePrint Archive

- [eprint.iacr.org](http://eprint.iacr.org)
- Preprints, full versions, corrected versions, revised versions ...
- Joppe Bos & Tancrède Lepoint, editors



# 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
  - Isogeny-based Cryptography School (31 Jan – 4 Feb 2022, Bristol)
  - School on Combinatorial Techniques in Cryptography (April 2022, Malta)
- **Next proposals are due December 31**
  - IACR Schools Committee
  - [www.iacr.org/schools/](http://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.

2021, Asiacrypt – **Andrew Yao**

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.



# IACR Fellows – 2021



Craig  
Gentry



Yehuda  
Lindell



Josef  
Pieprzyk



Leonid  
Reyzin



Ingrid  
Verbauwhede

Information on website

[www.iacr.org/fellows/](http://www.iacr.org/fellows/)





# 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 2021

- A provable-security treatment of the key-wrap problem
  - Phillip Rogaway, Thomas Shrimpton
  - Eurocrypt 2006
- New proofs for NMAC and HMAC: Security without collision-resistance
  - Mihir Bellare
  - Crypto 2006
- Simulation-sound NIZK proofs for a practical language and constant size group signatures
  - Jens Groth
  - Asiacrypt 2006
- <https://iacr.org/testoftime/>



# Financial report

Brian LaMacchia



# Membership report

Douglas Stebila



# IACR membership

Regular members: \$50

Student members: \$25

Senior members\*: \$0

- $\geq 65$  years of age  
and
- $\geq 20$  years of IACR membership total

You are a member for 2021 if:

- You attended an IACR conference in 2020 (and did not opt out of membership)
- Or you renew your membership for 2021 online by September 30, 2021

Attending **Asiacrypt 2021**  
makes you a  
**member for 2022**  
(unless you opted out)

\* If you are eligible for senior membership, email [membership@iacr.org](mailto:membership@iacr.org) to have it activated.



# Membership website

<https://register.iacr.org/membership>

- Update contact info
- View membership history
- Renew your membership
- View list of recent and upcoming mailed issues of Journal of Cryptology
- Download copies of receipts from IACR conferences all in one place (since 2017)
- View recent conference attendee list (For attendees who opted in to be listed)



# Benefits of membership

- Online access to all current and past IACR publications
- Eligibility to run for IACR leadership positions and vote in IACR elections, referenda, and membership meetings
- Eligibility to nominate and be nominated for IACR Fellows
- Supporting your international scholarly society
- Receiving newsletters and notifications about events
- Optional paper subscription to the Journal of Cryptology (\$40/year)

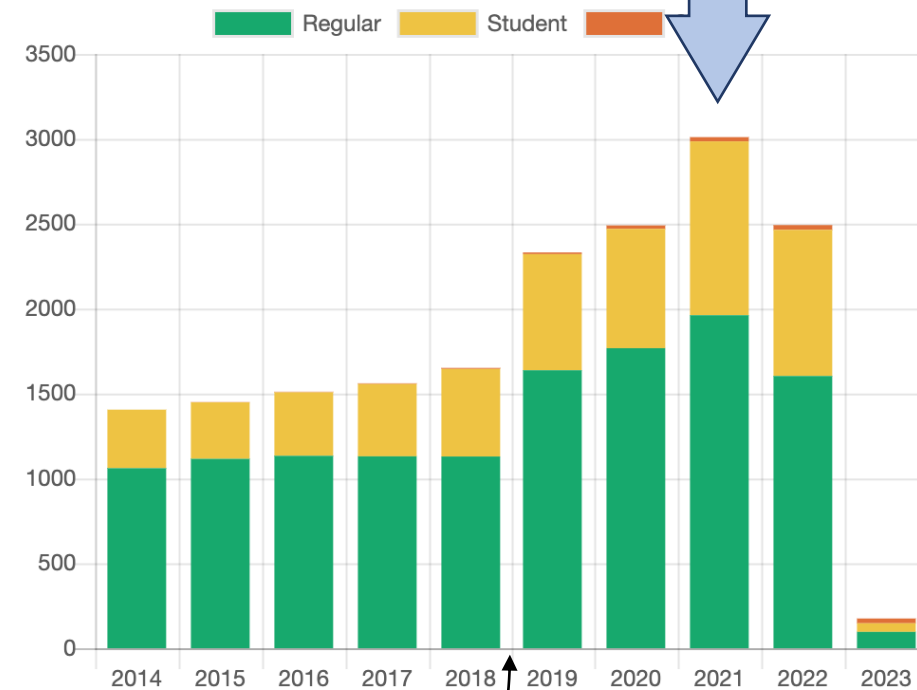


# Membership statistics by year

## Member class by year

Year	Regular	Student	Senior	Total
2014	1060	345	0	1405
2015	1115	333	2	1450
2016	1133	374	3	1510
2017	1130	426	4	1560
2018	1129	516	6	1651
2019	1637	684	10	2331
2020	1767	703	20	2490
2021	1961	1024	25	3010
2022	1603	861	28	2492
2023	96	51	28	175

## Member class by year



≥ 3000  
members for  
2021 –  
a new record!

RWC joins IACR





# Membership geography – 2021

## Membership by country

<b>United States</b>	990
<b>France</b>	203
<b>Germany</b>	201
<b>China</b>	185
<b>Japan</b>	166
<b>United Kingdom</b>	156
<b>Korea, Republic of</b>	108
<b>Switzerland</b>	99
<b>Israel</b>	88
<b>Netherlands</b>	85
<b>Belgium</b>	77
<b>Canada</b>	73
<b>India</b>	69
<b>Australia</b>	49
<b>Singapore</b>	40

## Membership by continent

<b>Europe</b>	1113
<b>North America</b>	1089
<b>Asia</b>	727
<b>Oceania</b>	57
<b>South America</b>	18
<b>Africa</b>	6

# Online services

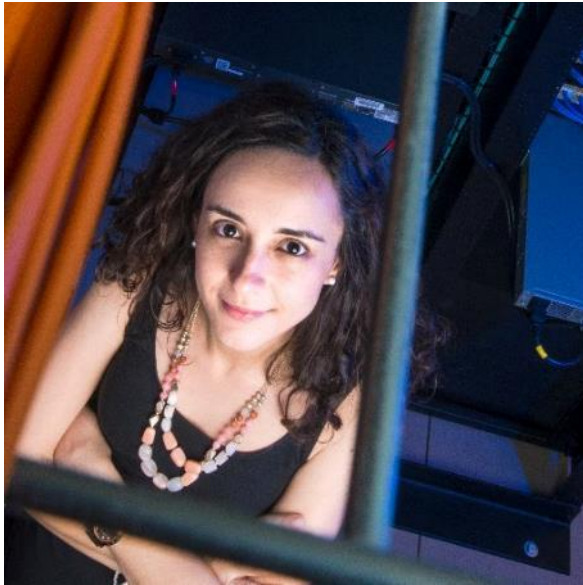
[iacr.org](http://iacr.org)

[ia.cr](http://ia.cr)



# Thanks to the team!

- Foteini Baldimtsi
  - Communications Secretary



- Yu Yu
  - Webmaster





# International Association for Cryptologic Research

[Events](#) ▾[Publications](#) ▾[News](#) ▾[Services](#) ▾[Members](#) ▾[About](#) ▾

## IACR News

Here you can see all recent updates to the IACR webpage. These updates are also available:



via email



via RSS feed



via Twitter



via Weibo



via Facebook

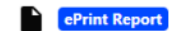
Filter news by

All news ▾

### 20 May 2019

#### [Pixel: Multi-signatures for Consensus](#)

*Manu Drijvers, Sergey Gorbunov, Gregory Neven, Hoeteck Wee*



Multi-signatures enable a group of signers to jointly generate a short and efficiently verifiable signature on a common message. They are commonly used in proof-of-stake and permissioned blockchains, where reaching consensus usually involves a committee of nodes signing the next block. Adaptive corruptions, however, pose a common threat to such designs, because the adversary can corrupt committee members after they certified a block (and possibly after they sold their stake) and use their signing keys to fork the chain by certifying a different block, thereby undermining the

[Expand](#) ▾

#### [New Code-Based Privacy-Preserving Cryptographic Constructions](#)

*Khoa Nguyen, Hanh Tang, Huaxiong Wang, Neng Zeng*



Code-based cryptography has a long history but did suffer from periods of slow development. The field has recently attracted a lot of attention as one of the major branches of post-quantum cryptography. However, its subfield of privacy-preserving cryptographic constructions is still rather underdeveloped. e.g. important building blocks such as zero-knowledge range proofs and set membership proofs, and even proofs of knowledge of





# Open Positions in Cryptology

IACR provides a listing of open positions with a focus on cryptology. To advertise a job opportunity, please use the button to the right.

[Submit a job](#)

Submissions should include the organization, title, description, a URL for further information, contact information, and a closing date (which may be "continuous"). The job will be posted for six months or until the closing date. Submissions in other formats than text will not be posted. There can be no attachments.

This is intended to be a free service from an IACR member to the IACR membership. The content of the job posting is the responsibility of the person requesting the posting and not the IACR. Commercial enterprises who want to advertise their openings should identify at least one of their employees who is a member of IACR.



# CryptoDB

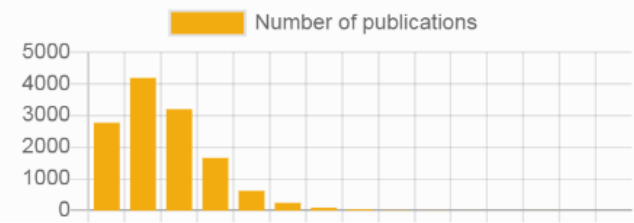
General ▾ Publications ▾ People ▾

## Collaboration between authors

This page contains statistics about coauthorship, including the most coauthored papers, the authors with the most coauthors, and the distribution of the number of authors.

## Distribution of number of authors on a paper

As of 2019, there is a [single paper](#) with 17 authors.



# Asiacrypt 2021



December 6-10, 2021  
Virtual

[Home](#)

[Technical Program](#) ▾

[Participate](#) ▾

[Sponsors](#)

[Contact](#)

Asiacrypt 2021, the 27th Annual International Conference on the Theory and Application of Cryptology and Information Security, will take place virtually on December 6-10, 2021. Asiacrypt 2021 is organized by the [International Association for Cryptologic Research \(IACR\)](#).

[Join the conference](#)

[Registration is open](#)

## Important Dates

May 27 2021	Submission deadline at 11:59 UTC (noon)
Jul 20 2021	First round notification
Jul 26 2021	Rebuttal deadline
Aug 25 2021	Final notification
Sep 20 2021	Final version due
Dec 6 2021	Conference begins

## Website Updates

Dec 2 2021	A page on <a href="#">how to participate</a> has been added
Nov 24 2021	The <a href="#">rump session</a> submission guidelines are up, get your guitars and stand-up routines ready!
Nov 16 2021	A <a href="#">tentative program</a> is available.
Nov 16 2021	Information about the <a href="#">invited talks</a> has been added
Oct 29 2021	List of <a href="#">accepted papers</a> now available
Oct 22 2021	<a href="#">Registration</a> is open
Sep 23 2021	Switch to a virtual event





The screenshot shows the Asiacrypt Portal interface. At the top, there are navigation tabs: "Rooms" (highlighted), "Program", "Chat", "Whiteboard", and "Conduct". Below the tabs, the main content area is titled "Social rooms" and includes a "Create a room" button, a "Join a random room" button, and a search bar with the text "Search rooms and people...".

On the left side, there is a "Asiacrypt Portal Instructions" section with the following text:

**Asiacrypt Portal Instructions**

- To attend a talk, choose the "Program" tab at the top and click on a Zoom link. If that tab does not show up, your network firewall is probably the problem.
- For socializing, you can choose the "Rooms" tab and join a video chat room. Be the first and others will join you.
- The "Chat" tab allows you to talk with others. You will receive a username/password for chat.iacr.org.
- For help, contact virtual-conferences@iacr.org
- More information may be found on the conference website.

The main content area displays several "Social rooms" with "Join" buttons:

- Share your gossip**: Be the first in this room!
- The future of publishing**: *What should we do with eprint?* Be the first in this room!
- The future of conferences**: *Will they ever be the same?* Be the first in this room!
- Grad student lounge**: *Others are also welcome* Be the first in this room!
- Postdoc Lounge**: *Others are also welcome* Be the first in this room!



# Thanks (2) to the team!

- Kay McKelly



- Kevin McCurley





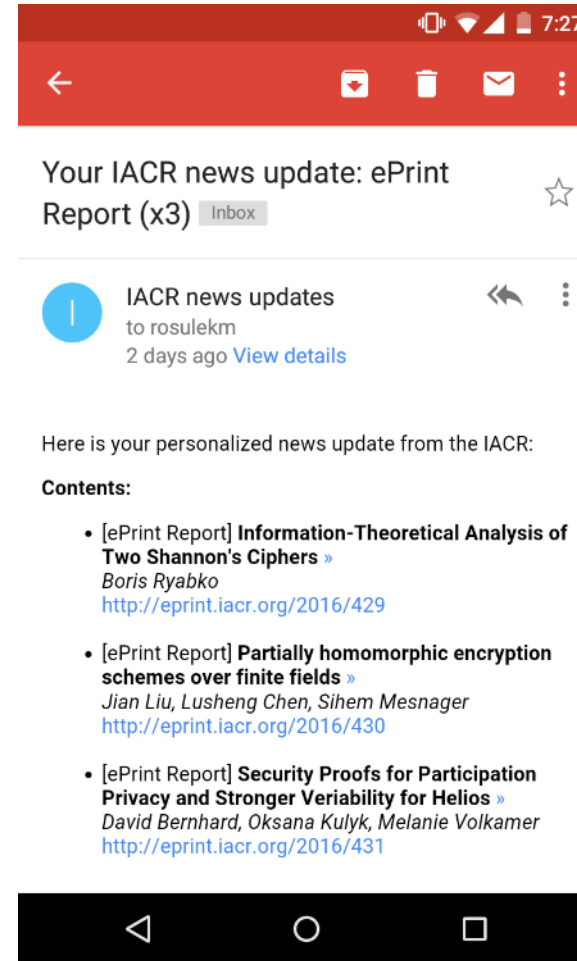
# All online services

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



# IACR news alerts

- Receive alerts about:
  - General announcements
  - New eprint reports
  - Job openings in cryptology
  - New events (conferences)
- Receive alerts via:
  - Facebook: [fb.com/theiacr](https://fb.com/theiacr)
  - Twitter: [twitter.com/iacr\\_news](https://twitter.com/iacr_news)
  - Weibo: [weibo.com/iacr](https://weibo.com/iacr)
  - Email: [iacr.org/news](http://iacr.org/news)



# IACR publications portal

- [ia.cr/pubs](https://ia.cr/pubs)
- Conference proceedings available:
  - **all years**: Publisher version, IACR members only
  - **after 2 years**: “IACR version”, public access
  - **after 3 years**: Publisher version, open access



The screenshot shows the IACR Publications portal. At the top, there is a navigation bar with the IACR logo and the text "International Association for Cryptologic Research". Below the navigation bar, there is a search bar and a list of menu items: Events, Publications, News, Services, Members, and About. The main content area is titled "Access IACR Publications" and includes a sub-header "Advances in Cryptology - CRYPTO". Below this, there is a table with columns for Year, Publisher version, IACR Archive, and CryptoDB. The table lists data for the years 2015 through 2019.

Year	Publisher version	IACR Archive	CryptoDB
2019:	Publisher version (Vol 1) Publisher version (Vol 2) Publisher version (Vol 3)		Bibliographic info
2018:	Publisher version (Vol 1) Publisher version (Vol 2) Publisher version (Vol 3)		Bibliographic info
2017:	Publisher version (Vol 1) Publisher version (Vol 2) Publisher version (Vol 3)		Bibliographic info
2016:	Publisher version (Vol 1) Publisher version (Vol 2) Publisher version (Vol 3)	IACR version	Bibliographic info
2015:	Publisher version (Vol 1) Publisher version (Vol 2)	IACR version	Bibliographic info



# Your IACR



# Upcoming events



# 2021 General Conferences

- Crypto 2021, 15 – 19 Aug, Online
  - Vladimir Kolesnikov (GC)
  - Tal Malkin & Chris Peikert (PC)
- Eurocrypt 2021, 17 – 21 Oct, Zagreb (Croatia)
  - Lejla Batina & Stjepan Picek (GC)
  - Anne Canteaut & François-Xavier Standaert (PC)
- Asiacrypt 2021, 5 – 9 Dec, Online
  - Guo Jian (GC)
  - Wang Huaxiong & Mehdi Tibouchi (PC)



# Future 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, TBD
  - NN (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.

- RWC 2022, 10 – 12 Jan, Amsterdam (The Netherlands)
  - Lejla Batina, Joan Daemen, Peter Schwabe (GC)
  - Dan Boneh, Helena Handschuh (PC)
- PKC 2022, 7 – 11 Mar, Yokohama (Japan)
  - Junji Shikata & Yohei Watanabe (GC)
  - Goichiro Hanaoka (PC)
- FSE 2022, 20 – 25 Mar, Athens (GR)
  - Christina Boura (GC)
  - Itai Dinur & Gaëtan Leurent & Bart Mennink (ToSC EiC)



# Future Area Conf. & Symp.

- CHES 2022, Sept, Beijing, China
  - Liji Wu, Guoqiang Bai, Zhe Liu, Junfeng Fan (GC)
  - Sonia Belaïd & Thomas Eisenbarth (TCHES EiC)
- TCC 2022, 7 – 10 Nov, Chicago (US)
  - David Cash (GC)
  - Eike Kiltz & Vinod Vaikuntanathan (PC)



# Current topics



# Recent work in the Board

- Find details online: [iacr.org/docs/minutes/](https://iacr.org/docs/minutes/)
- COVID-19 Impact
- Hybrid conference implementation
- Creation of a new IACR journal
- Co-sponsorship of the RSA Conf. Excellence in the Field of Mathematics Award
- IACR online seminars



# COVID-19 impact on IACR conferences

- Most conferences were converted to an all-digital format
  - Starting with Eurocrypt 2020 (May 11-15, 2020)
- No FSE 2021
- Two hybrid conferences so far
  - Eurocrypt 2021
  - TCC 2021
- Some affiliated workshops were converted to a virtual format



# Virtual conference implementation

- Participation
  - Pre-recorded videos
  - Live sessions via Zoom and/or YouTube
  - Live chat on [chat.iacr.org](https://chat.iacr.org)
  - Small group video conferencing via the conference portal
- Use of Zoom and YouTube
  - **Does NOT constitute an endorsement** of these technologies by the IACR
- Technology choices
  - Zoom: Primarily because of reliability and ability to scale
  - Zulip: Similar to Slack but could be self-hosted
  - YouTube: Static videos and streaming



# New IACR Journal

Joppe Bos



# IACR New Journal Committee - An update

Proposed journal name:

## **IACR Communications in Cryptology**

### **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 at the start for diamond open access: < 100 USD / paper**

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 one hour 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?



# Next steps

Keep in mind: the goal of the new journal is to **complement** not replace  
→ Extending the reach of the IACR to people who like to publish results without necessarily want to present their work at one of our conferences

## Next steps

The Board has agreed in principle to the creation of the New Journal.

Lots of work to be done: hosting, metadata, costs, etc

Alignment with (the steering committees of) JoC + Transactions will take place



## Mini-FAQ

- What about the Journal of Cryptology?  
→ Still **the** Journal for the highest-quality papers.
- What about the Transactions?  
→ Still considered the top-places for papers in their areas.  
Note: not all areas have dedicated conferences.
- What is the difference to the ePrint Archive?  
→ Papers in the journal are fully reviewed and low-quality papers are obviously rejected  
→ Again, the New Journal complements it will not replace!

**What do you think about this new IACR journal?**

Let us know at: [newjournal@iacr.org](mailto:newjournal@iacr.org)



# Open discussion



**Thank you for your attention!**

