

# International Association for Cryptologic Research

Michel Abdalla  
IACR President

Crypto 2020



# Membership meeting agenda

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

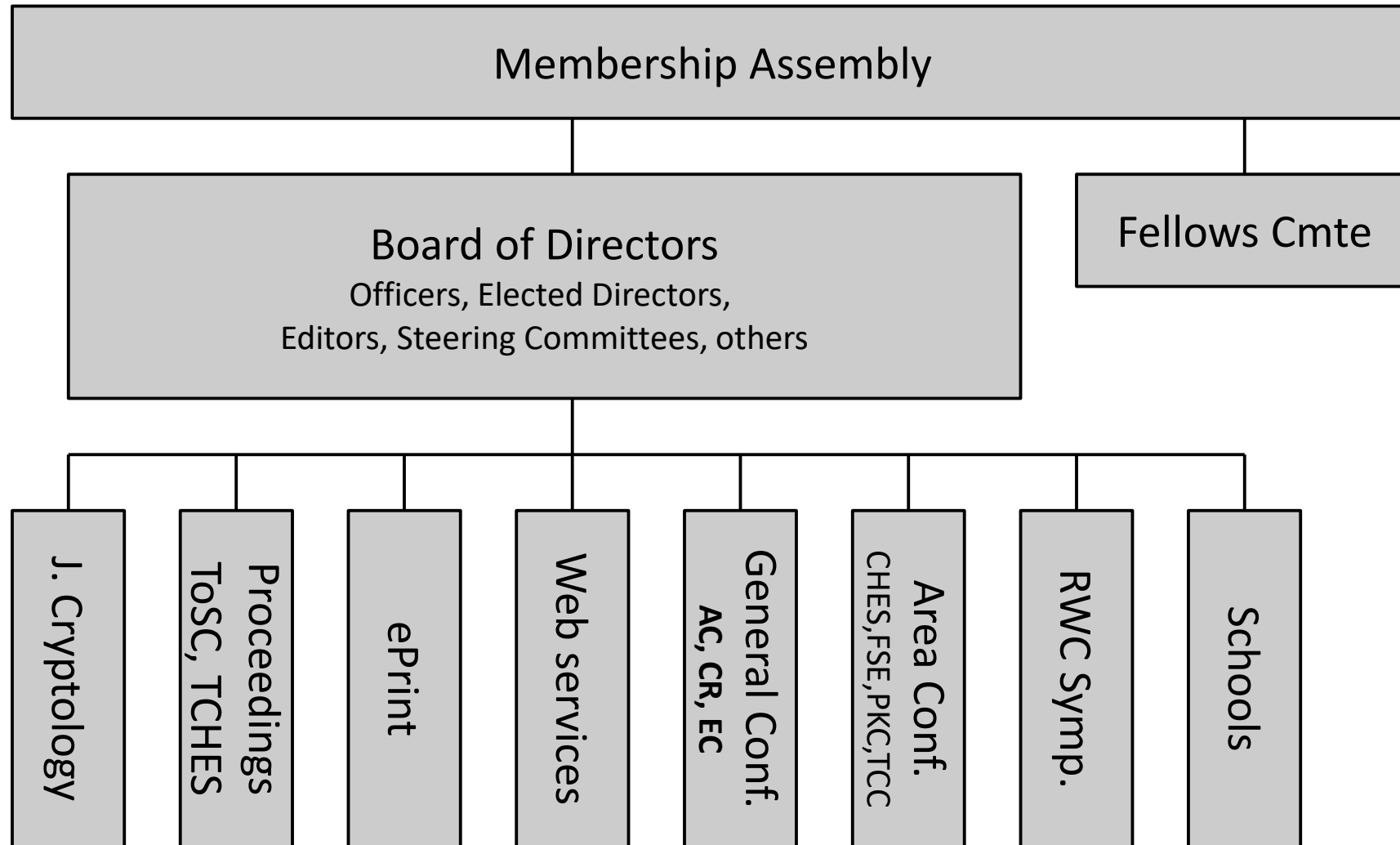


# IACR

- **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 Crypto 2020, you are a member of the IACR for 2021
- Membership fee of **\$50** (**\$25** students)
- You can also become a member online
- If you **did not attend** a conference **last year**, renew your membership online for **this year** 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/2020/](http://iacr.org/elections/2020/)



# 2020 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 (2018-2020)  
Marc Fischlin (2020-2021)  
Nadia Heninger (2019-2021)  
Tancrede Lepoint (2018-2020)  
Anna Lysyanskaya (2019-2021)  
Bart Preneel (2020-2022)  
Peter Schwabe (2020-2022)  
Francois-Xavier Standaert (2020-2022)  
Moti Yung (2018-2020)

## Other Board Members

Foteini Baldimtsi, Communications Secretary (2019-2022)  
Lejla Batina, Eurocrypt 2020 General Chair (2019-2020)  
Colin Boyd, Eurocrypt 2021 General Chair (2020-2021)  
Jian Guo, Asiacrypt 2021 General Chair (2020-2021)  
Kwangjo Kim, Asiacrypt 2020 General Chair (2019-2020)  
Kenny Paterson, Editor-in-Chief, Journal of Cryptology (2017-2019)  
Leo Reyzin, Crypto 2020 General Chair (2019-2020)  
Douglas Stebila, Membership Secretary (2017-2020)  
Vladimir Kolesnikov, Crypto 2021 General Chair (2020-2021)



# Journal of Cryptology



- Editor in Chief
  - Current: **Kenny Paterson**
  - 2021-2023: **Vincent Rijmen**
- Read online
  - [iacr.org/publications/access.php](https://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**

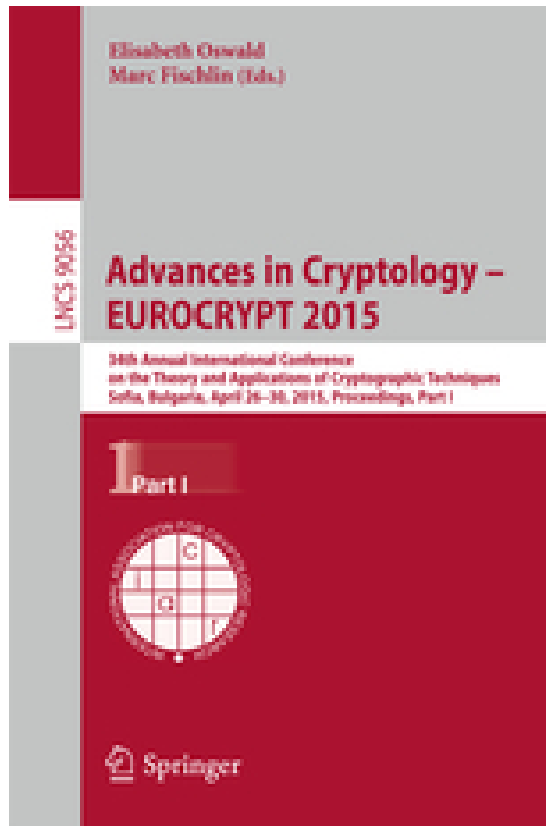


# IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)

- **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 ...
  - Record is 124 revisions, then withdrawn
- Joppe Bos & Tancrede 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 (UK)
  - Encrypted Search (Morocco)
  - Theory and Practice of Multi-Party Computation (Denmark)
- **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.

2020, Crypto – **Silvio Micali**

2021, Asiacrypt – **Andrew Yao**



# IACR Fellows

IACR Fellows are outstanding IACR members, recognized for technical and professional contributions that

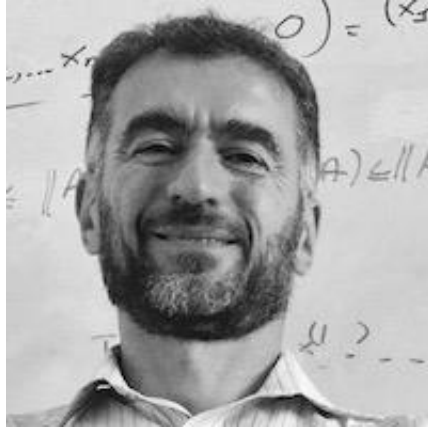
- Advance the science, technology, and practice of cryptology and related fields;
- Promote the free exchange of ideas and information about cryptology and related fields;
- Develop and maintain the professional skill and integrity of individuals in the cryptologic community;
- Advance the standing of the cryptologic community in the wider scientific and technical world and promote fruitful relationships between the IACR and other organizations.



# IACR Fellows – 2020



Yevgeniy  
Dodis



Rosario  
Gennaro



Xuejia  
Lai



Tal  
Malkin



David  
Naccache

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 2020

- Fuzzy Identity-Based Encryption
  - Amit Sahai, Brent Waters
  - Eurocrypt 2005
- Finding collisions in the full SHA-1
  - Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu
  - Crypto 2005
- Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log
  - Pascal Paillier, Damien Vergnaud
  - Asiacrypt 2005
- <https://iacr.org/testoftime/>



# Financial report

Brian LaMacchia



# Membership report

Douglas Stebila



# Online services

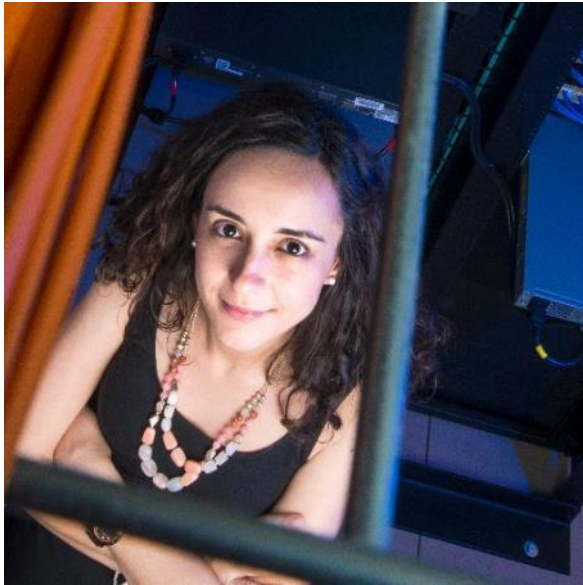
[iacr.org](http://iacr.org)

[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

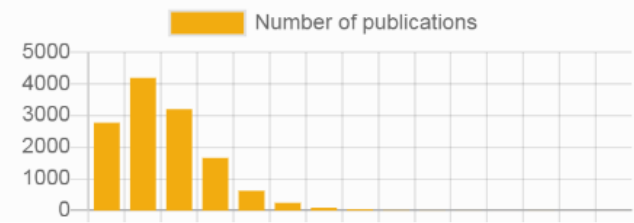
General ▾ Publications ▾ People ▾

# 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.







# International Association for Cryptologic Research

Events ▾

Publications ▾

News ▾

Services ▾

Members ▾

About ▾



Suggestions from local search as you type. Hit enter to search with Google.

Nigel



Search

**Nigel P. Smart**

Katholieke Universiteit Leuven

**Results 2011**

News: Election

**Dawson, Halevi, Shoup, Smart named 2016 IACR Fellows**

News: Award

**Future Directions in Computing on Encrypted Data**

News: Event: Bristol, United Kingdom, November 10 - November 11

**IACR Publication Reform - Open Discussion**

News: Announcement

**CAPA: The Spirit of Beaver Against Physical Attacks**

CRYPTO 2018, Oscar Reparaz, Lauren De Meyer, Begül Bilgin, Victor Arribas, Svetla Nikova, Ventzislav Nikov, Nigel P. Smart

**Modes of Operation Suitable for Computing on Encrypted Data**

TOSC 2017, Dragos Rotaru, Nigel P. Smart, Martijn Stam

**More Efficient Constant-Round Multi-party Computation from BMR and SHE**

TCC 2016, Yehuda Lindell, Nigel P. Smart, Eduardo Soria-Vazquez

**Efficient Constant Round Multi-party Computation Combining BMR and SPDZ**

CRYPTO 2015, Yehuda Lindell, Benny Pinkas, Nigel P. Smart, Avishay Yanai

**Benchmarking Privacy Preserving Scientific Operations**

Eprint: 2019/354, Abdelrahman Aly, Nigel P. Smart

Report

only

ified a

the

Expand ▾



# Crypto 2020



August 17-21, 2020  
Virtual

[Home](#)

[Technical Program](#) ▾

[Participate](#) ▾

[Sponsors](#)

[Contact](#)

Crypto 2020 will take place virtually on August 17-21, 2020, with [affiliated events](#) August 14-16. Crypto 2020 is organized by the International Association for Cryptologic Research (IACR).

[Register now!](#)

[Join affiliated events](#)

[Join the main event](#)

We had a brief interruption in registration on Saturday morning. Registration is open again, but if you have trouble, [contact the general chair](#)

## Important Dates

11 Feb 2020	Submission deadline at 21:00 UTC
3 Apr 2020	Reviews sent out for rebuttal
10 Apr 2020	Rebuttal deadline
15 May 2020	Paper notification

## Website Updates

18 Aug 2020	Thanks to PlatON for being a sponsor
1 Aug 2020	Thanks to Google for being a sponsor
31 Jul 2020	Thanks to J.P. Morgan for being a sponsor
20 Jul 2020	<a href="#">Affiliated events</a> updated



Gallery **Rooms** Chat Program Scavenger hunt

Microphone icon Video icon Exit video

**Video room list** [Join a random room](#)

Search rooms and people..

You are not in any room. If you would like to join a video conference, join a room under the Rooms tab.

<b>Cards against cryptography (anyone know where to play?)</b> Be the first in this room! <a href="#">Join</a>	<b>Cryptographic Elections</b> Be the first in this room! <a href="#">Join</a>
<b>Covid Contact Tracing</b> Be the first in this room! <a href="#">Join</a>	<b>Beach Barbecue</b> Be the first in this room! <a href="#">Join</a>
<b>New applications of cryptography</b> Be the first in this room! <a href="#">Join</a>	<b>Where's the beer?</b> Be the first in this room! <a href="#">Join</a>
<b>Grad Student Lounge</b> Be the first in this room! <a href="#">Join</a>	<b>Postdoc Lounge</b> Be the first in this room! <a href="#">Join</a>
<b>Let's have strawberries and shrimp</b> Be the first in this room! <a href="#">Join</a>	<b>Santa Barbara Memories</b> Be the first in this room! <a href="#">Join</a>





# Thanks (2) to the team!

- Kay McKelly



- Kevin McCurley



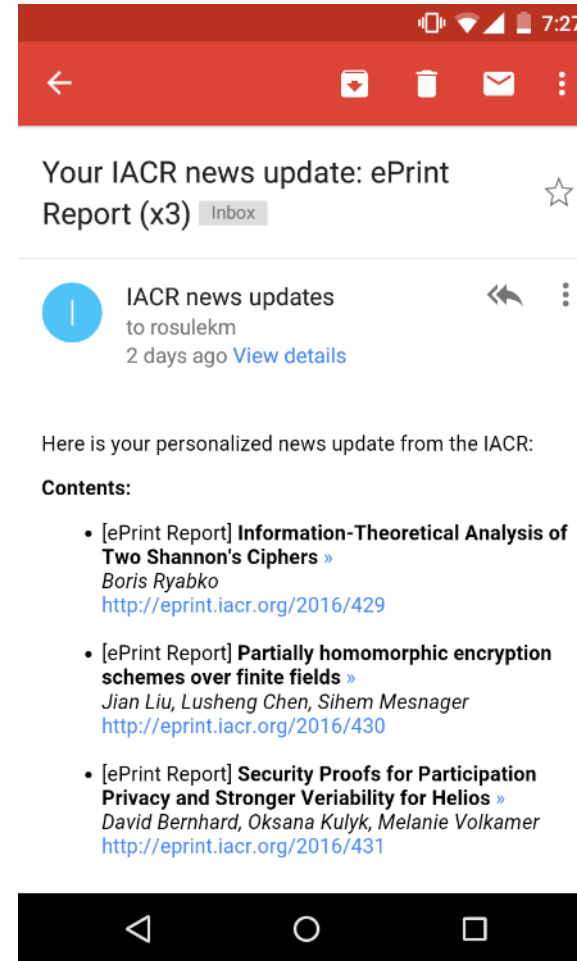
# All online services

- 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](http://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





# Current topics



# Recent work in the Board

- Find details online: [iacr.org/docs/minutes/](https://iacr.org/docs/minutes/)
- COVID-19 Impact
- Virtual conference implementation
- Parallel co-chairs
- Creation of a new IACR journal
- J. of Cryptology switch to the “continuous article publishing” model in 2021
- IACR PhD dissertation award
- IACR online seminars

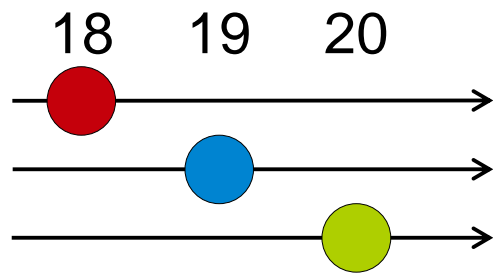


# Journal of Cryptology publication model

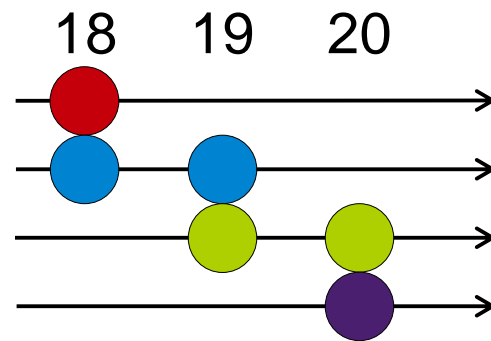
- Current system
  - Papers appear in an “online first” category before being assigned to an issue
  - The current waiting time in “online first” is 9-12 months
- “Continuous Article Publishing” (CAP) model
  - Papers will be assigned to an issue as soon as they are produced
  - An issue closes once enough papers have been entered into it
  - Papers will be indexed more quickly
  - Starts in 2021



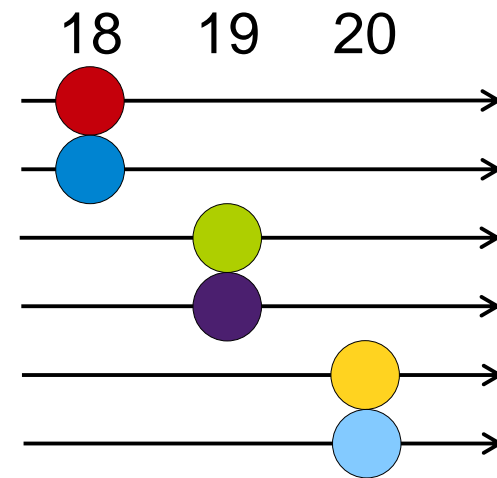
# Parallel program co-chairs



Single chair  
until 2009



Rolling co-chair  
TODAY



Parallel co-chair  
Starting 2020-21

# COVID-19 impact on IACR conferences

- Several conferences were converted to an all-digital format
  - Eurocrypt 2020 (May 11-15, 2020)
  - PKC 2020 (June 1-4, 2020)
  - CRYPTO 2020 (August 17-21, 2020)
  - CHES 2020 (September 14-18, 2020)
  - TCC 2020 (November 15-19, 2020)
- FSE 2020 was postponed to November 8-12, 2020
- Changes to future Eurocrypt editions
  - Eurocrypt 2021 moved to Zagreb, Croatia
  - Eurocrypt 2022 moved to Trondheim, Norway
- Unchanged for now: Asiacrypt 2020, RWC 2021
- Associated workshops for Eurocrypt 2020 were cancelled



# 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 using Jitsi on [conf.iacr.org](https://conf.iacr.org)
- Use of Zoom and YouTube
  - **Does NOT constitute an endorsement** of these technologies by the IACR
  - Attendees are not required to install Zoom software to attend a webinar
- 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

- Original proposal submitted to the board
  - Paulo Barreto
  - Seny Kamara
  - Elisabeth Oswald
  - Michael Naehrig
  - Tom Ristenpart
  - Nigel Smart
- Complement to Journal of Cryptology
- Implementation details still under discussion



# Open discussion





# Upcoming events



# Future General Conferences

- Crypto 2020, 17 – 21 Aug, Online
  - Leo Reyzin (GC)
  - Daniele Micciancio & Tom Ristenpart (PC)
- Asiacrypt 2020, 6 – 10 Dec, Daejeon (KR)
  - Kwangjo Kim (GC)
  - Shiho Moriai & Wang Huaxiong (PC)



# Future General Conferences

- Eurocrypt 2021, 2 – 6 May, Zagreb (Croatia)
  - Lejla Batina & Stjepan Picek (GC)
  - Anne Canteaut & François-Xavier Standaert (PC)
- Crypto 2021, 15 – 19 Aug, UCSB, Santa Barbara (US)
  - Vladimir Kolesnikov (GC)
  - Tal Malkin & Chris Peikert (PC)
- Asiacrypt 2021, 5 – 9 Dec, Singapore
  - 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, early Dec
  - NN (GC)
  - Shweta Agrawal & Dongdai Lin (PC)



# Future Area Conf. & Symp.

- PKC 2020, 1 – 4 Jun, Online
  - Petros Wallden & Markulf Kohlweiss & Viassilis Zikas (GC)
  - Aggelos Kiayias (PC)
- CHES 2020, 14 – 18 Sept, Online
  - Chitchanok Chuengsatiansup, Yuval Yarom (GC)
  - Amir Moradi & Mehdi Tibouchi (TCHES EiC)
- FSE 2020, 8 – 12 Nov, Athens (GR)
  - Christina Boura (GC)
  - Gaëtan Leurent & Yu Sasaki (ToSC EiC)



# Future Area Conf. & Symp.

- TCC 2020, 15 – 19 Nov, Online
  - Alessandra Scafuro (GC)
  - Rafael Pass & Krzysztof Pietrzak (PC)
- RWC 2021, 11 – 13 Jan, Amsterdam (The Netherlands)
  - Lejla Batina, Joan Daemen, Peter Schwabe (GC)
  - Tom Shrimpton, Kenny Paterson (PC)
- CHES 2021, 12 – 15 Sept, Beijing (China)
  - Liji Wu, Guoqiang Bai, Zhe Liu, Junfeng Fan (GC)
  - Elke De Mulder & Peter Schwabe (TCHES EiC)



**Thank you for your attention!**

