International Association for Cryptologic Research

Michel Abdalla
IACR President

Eurocrypt 2020

Membership meeting agenda

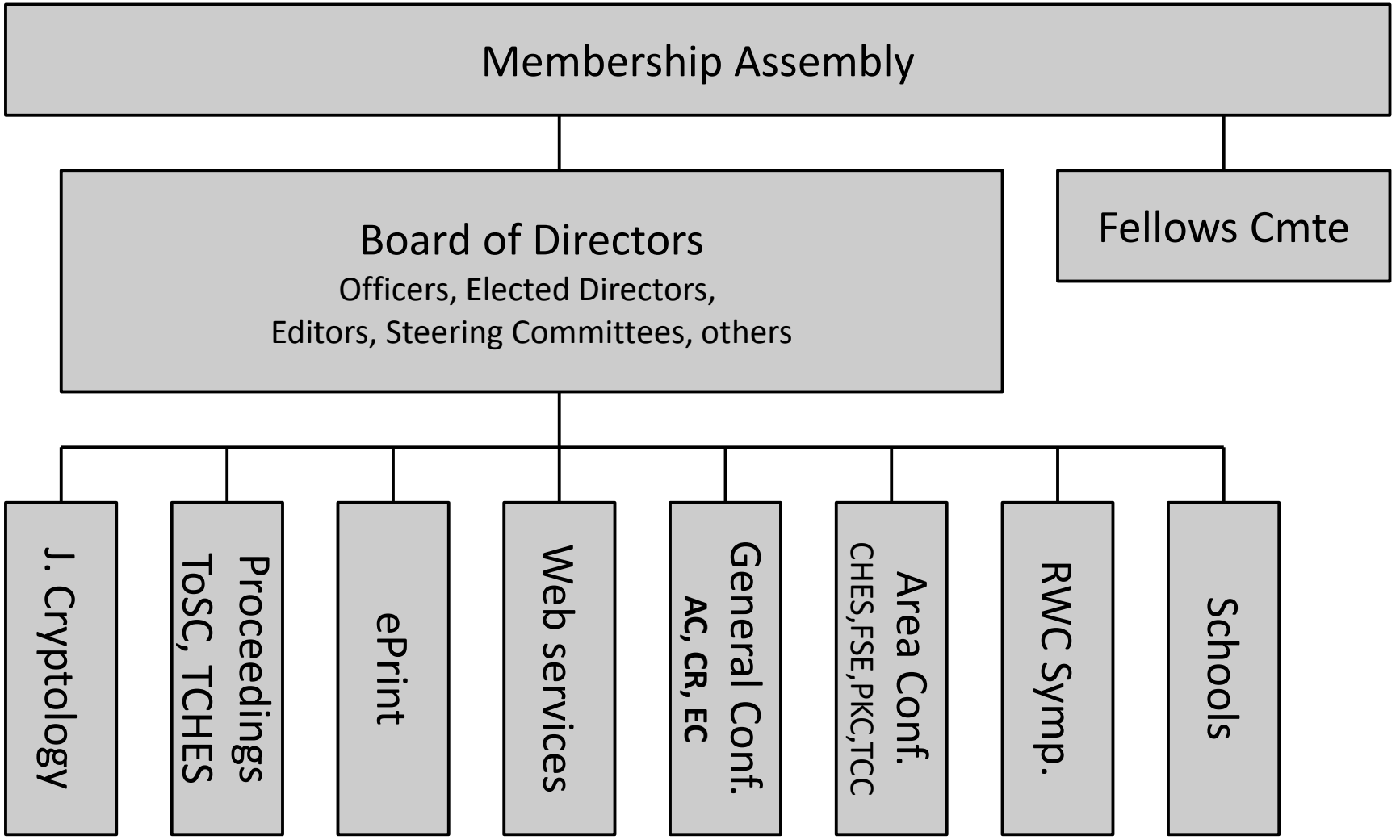
- About IACR
  - Publications
  - Conferences
  - Journal of Cryptology
- Financial report
- Membership report
- Online services
- Recent developments
- Open discussion
- Future events

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/

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

Membership

- Everyone attending an IACR event becomes a member in the next calendar year
  - By attending Eurocrypt 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

- Each year you elect 3 Directors
  - 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)
Tancrède 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

- Current editor in Chief
  - Kenny Paterson
- Read online
  - iacr.org/publications/access.php
- Paper delivery is opt-in for $40 extra
  - When you pay yearly membership

https://iacr.org/jofc/

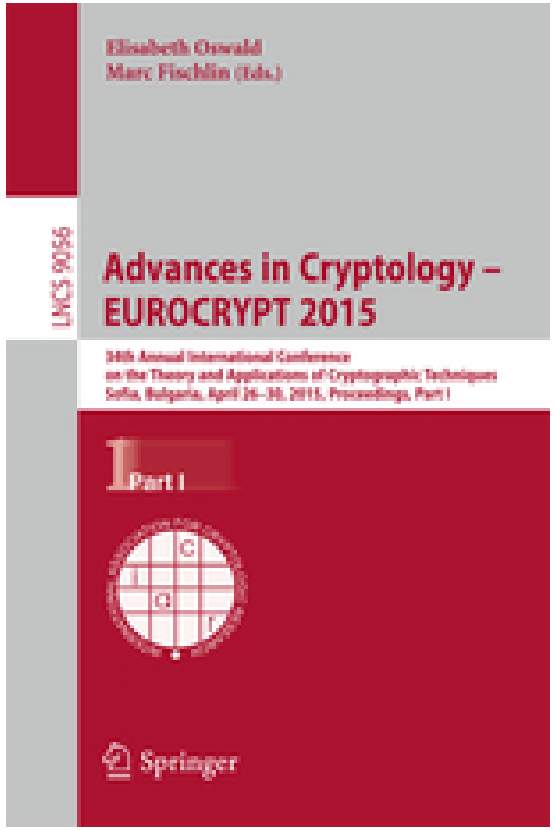
IACR Transactions on Symmetric Cryptology (ToSC)

- 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
- **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
- **Gold open access**

Conference proceedings



- ASIACRYPT
- CRYPTO
- EUROCRYPT
- PKC
- TCC

- Online for members
  - www.iacr.org/proceedings
- Gold open-acccess ≥ 3yr
  - link.springer.com

Cryptology ePrint Archive

- eprint.iacr.org

- Preprints, full versions, corrected versions, revised versions ...
  - Record is 124 revisions, then withdrawn

- 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 (UK)
  - Encrypted Search (Morocco)
  - Theory and Practice of Multi-Party Computation (Denmark)

- 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.

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/

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

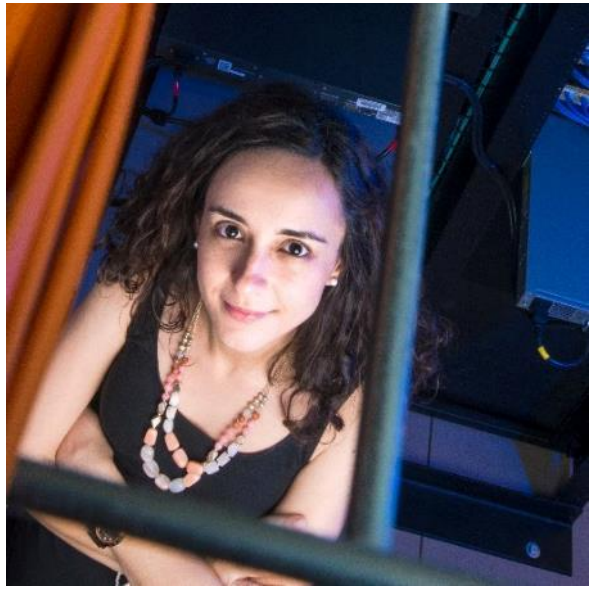
Online services

iacr.org

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

ePrint Report

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

ePrint Report

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

IACR

Open Positions in Cryptology

Submit a job

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

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

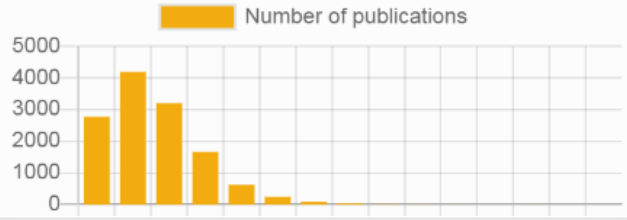
General ▾ Publications ▾ People ▾

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


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, Abdelrahaman Aly, Nigel P. Smart
Report
nonly
fied a
the
Expand

Thanks (2) to the team!

- Kay McKelly

- Kevin McCurley

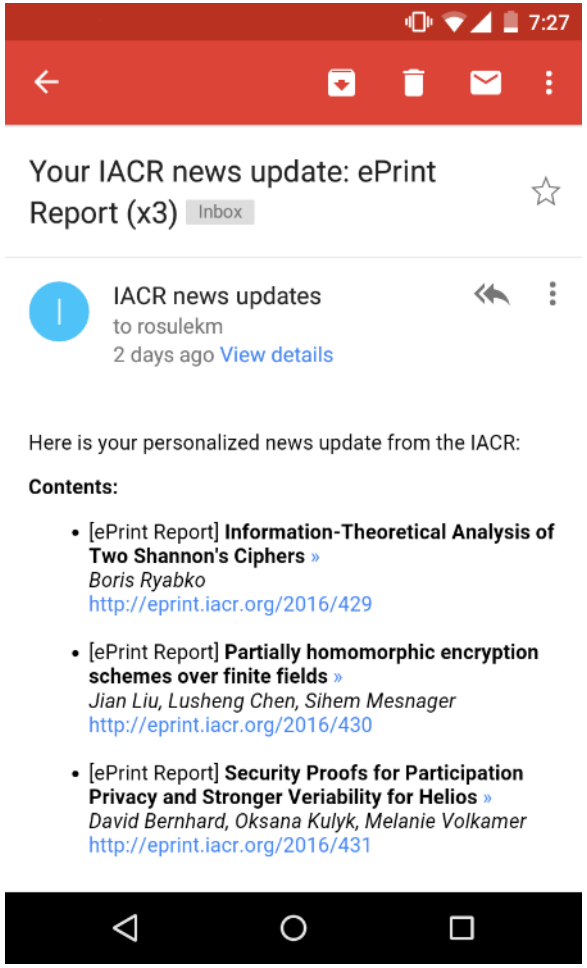
All online services

- 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
  - Twitter: twitter.com/iacr_news
  - Weibo: weibo.com/iacr
  - Email: iacr.org/news



IACR publications portal

- 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

Your IACR


We Need YOU
WE NEED YOU
WE NEED YOU
WE NEED YOU
We need YOU!
WE NEED YOU!
YOU
WE WANT YOU
WE NEED YOU To join OUR TEAM
WE NEED YOU!
WE NEED YOU!
WE NEED YOU
WE NEED YOU
We need you
WE NEED YOU!
WE NEED YOU
WE WANT YOU!
WE WANT YOU
We NEED you!
We Need You!!!
WE NEED YOU
WE NEED YOU!
WE NEED YOU!
We Need Yo
WE NEED YOU
We Need You!

Current topics

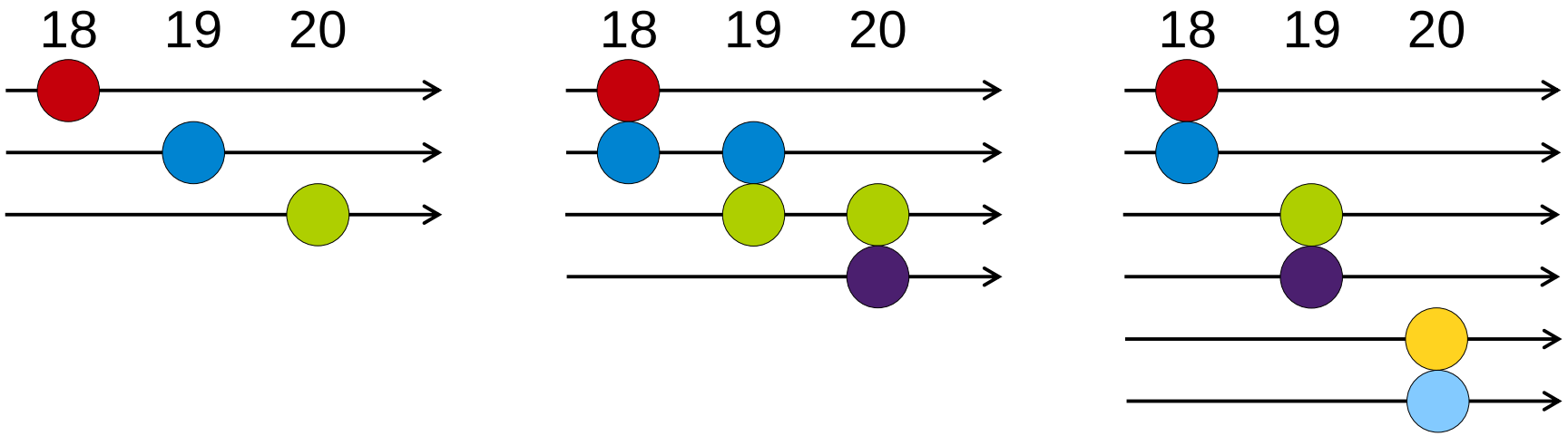
Recent work in the Board

- Find details online: iacr.org/docs/minutes/
- COVID-19 Impact
- Virtual conference implementation
- Parallel co-chairs
- Workshops are now an integral part of Asiacrypt, Crypto, and Eurocrypt
- J. of Cryptology will switch to the “continuous article publishing” model in 2021
- Growing difficulties with visas and problems with international exchange

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 (dates to be decided)
- 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: TCC 2020, 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
  - Small group video conferencing using Jitsi on 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

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)
  - NN & NN (PC)

- Crypto 2022, 14 – 18 Aug, UCSB, Santa Barbara (US)
  - NN (GC)
  - NN & NN (PC)

- Asiacrypt 2022, early Dec
  - NN (GC)
  - NN & NN (PC)

Future Area Conf. & Symp.

- PKC 2020, 1 – 4 Jun, Online
  - Petros Wallden & Markulf Kohlweiss & Viassilis Zikas (GC)
  - Aggelos Kiayias (PC)

- CHES 2020, 14 – 17 Sept, Online
  - Liji Wu, Guoqiang Bai, Zhe Liu, Junfeng Fan (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, 16 – 19 Nov, Durham, NC (US)
  - 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)

Thank you for your attention!