

International Association for Cryptologic Research

Christian Cachin
President, IACR

Eurocrypt 2019



Membership meeting

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

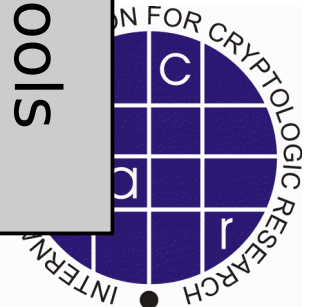
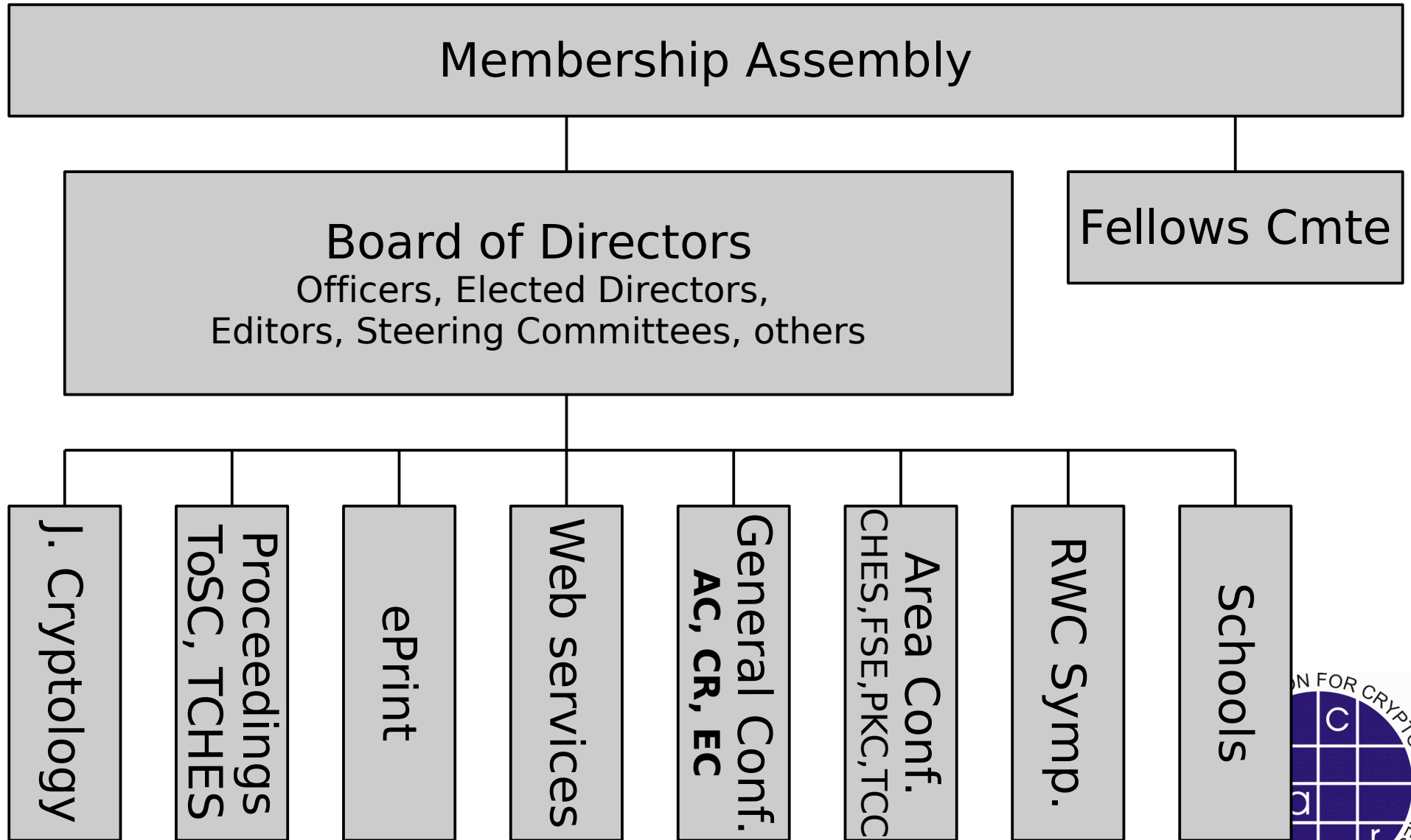


IACR

- **International Association for Cryptologic Research**
 - Purpose is to further research in cryptology and related fields
 - 1983
 - Incorporated as non-profit organization in Nevada (US)
- For all information – iacr.org/docs/



One picture



Membership

- Everyone attending an IACR event becomes a member in **next calendar year**
- 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
 - This year also 4 Officers
 - iacr.org/elections/2019/



Officers

Christian Cachin, President (2017-2019)

Greg Rose, Vice President (2017-2019)

Brian LaMacchia, Treasurer (2017-2019)

Joppe Bos, Secretary (2017-2019)

Directors

Michel Abdalla, Director (2019-2021)

Masayuki Abe, Director (2018-2020)

Shai Halevi, Director (2017-2019)

Nadia Heninger, Director (2019-2021)

Tancredi Lepoint, Director (2018-2020)

Anna Lysyanskaya, Director (2019-2021)

Bart Preneel, Director (2017-2019)

Francois-Xavier Standaert, Director (2017-2019)

Moti Yung, Director (2018-2020)

Other Board Members

Lejla Batina, Eurocrypt 2020 General Chair (2019-2020)

Marc Fischlin, Eurocrypt 2019 General Chair (2018-2019)

Kwangjo Kim, Asiacrypt 2020 General Chair (2019-2020)

Mitsuru Matsui, Asiacrypt 2019 General Chair (2018-2019)

Kenny Paterson, Editor-in-Chief, Journal of Cryptology (2017-2019)

Leo Reyzin, Crypto 2020 General Chair (2019-2020)

Mike Rosulek, Communications Secretary (2017-2020)

Douglas Stebila, Membership Secretary (2017-2020)

Muthu Venkatasubramaniam, Crypto 2019 General Chair (2018-2019)



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 are 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**

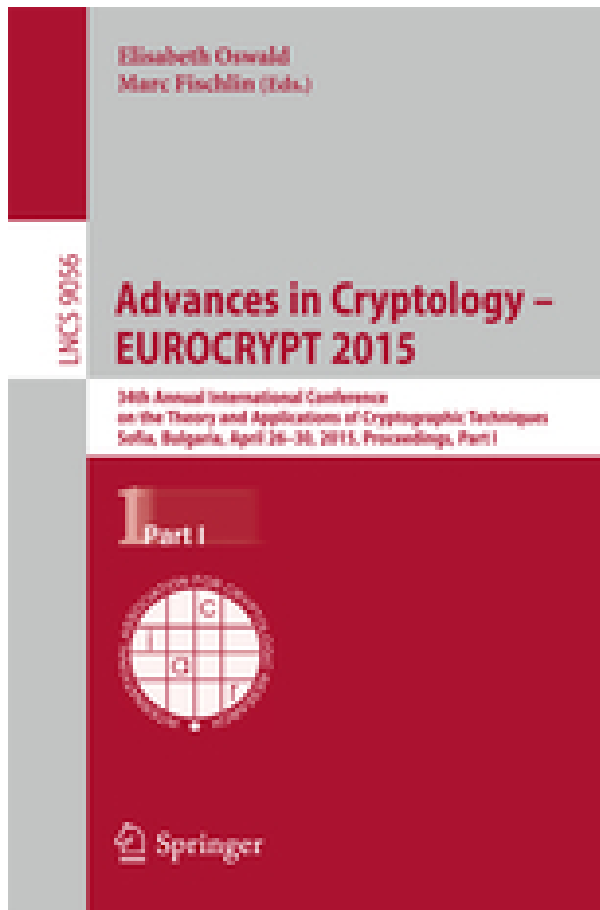


IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)

- CHES-TCHES are 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
 - Online for all (≥ 3 yr)
 - link.springer.com



Cryptology ePrint Archive

- eprint.iacr.org
- More than 1000 pre-prints per year
- ~~Sasha Boldyreva & Tancreède Lepoint~~, editors
→ Joppe Bos



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
 - Euclidean lattices: theory and applications, July 15-July 19, Kaliningrad, Russia
- **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.

2019, Eurocrypt – **Cynthia Dwork**

2020, Crypto – **Silvio Micali**



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 – 2019

- Jonathan Katz
- Kaoru Kurosawa
- Daniele Micciancio
- Vincent Rijmen
- Amit Sahai
- Xiaoyun Wang

Nominations for 2020 Fellows are due by
November 2019 !

Information will be 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 2019

- Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data
 - Yevgeniy Dodis, Leonid Reyzin, Adam D. Smith
 - Eurocrypt 2004
- Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions
 - Antoine Joux
 - Crypto 2004
- How Far Can We Go Beyond Linear Cryptanalysis?
 - Thomas Baignères, Pascal Junod, Serge Vaudenay
 - Asiacrypt 2004
- <https://iacr.org/testoftime/>



Financial report

- Brian LaMacchia



Membership report

- Douglas Stebila



Online services

iacr.org
ia.cr

~~Mike Rosulek~~ & Yu Yu



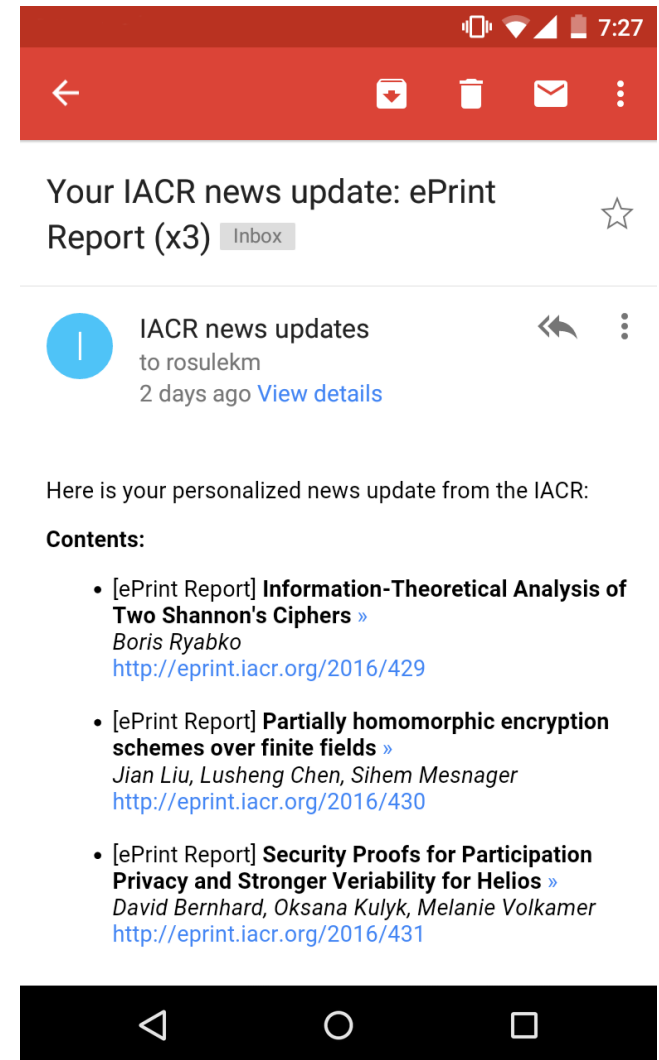
All online services

- 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



International Association for Cryptologic Research

Search IACR Search

Home Meetings Publications Awards News Services Jobs Members About

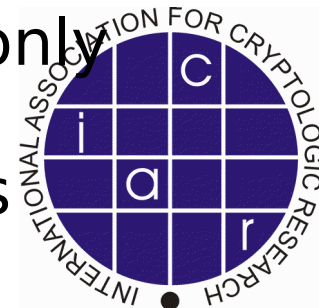
Access IACR Publications

IACR and Springer are pleased to offer you free access to the Journal of Cryptology and the IACR proceedings volumes for CRYPTO, EUROCRYPT, ASIACRYPT, FSE, CHES, PKC, and TCC.

Crypto	Eurocrypt	Asiacrypt	FSE	PKC	CHES	TCC	JoC
Advances in Cryptology - EUROCRYPT							
2016:	publisher versions (vol 1) publisher versions (vol 2)			bibliographic info			
2015:	publisher versions (vol 1) publisher versions (vol 2)			bibliographic info			
2014:	publisher versions			bibliographic info			
2013:	publisher versions	IACR versions		bibliographic info			
2012:	publisher versions	IACR versions		bibliographic info			
2011:	publisher versions	IACR versions		bibliographic info			

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



Website redesign

- Uniform conference websites
 - Operational since a few years
- Main website in responsive design
 - Currently underway
- Thanks to Kevin McCurley





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

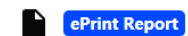


Multi-signatures enable a group of signers to jointly generate a short and efficiently verifiable signature on a common message. They are commonly used in proof-of-stake and permissioned blockchains, where reaching consensus usually involves a committee of nodes signing the next block. Adaptive corruptions, 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

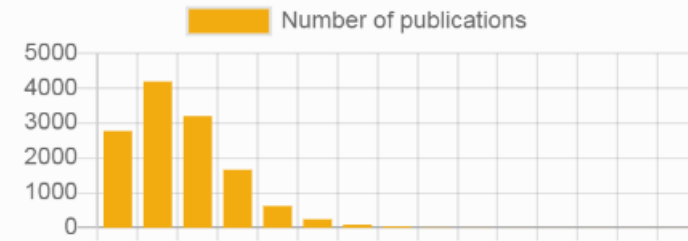
General ▾ Publications ▾ People ▾

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, Ventsislav 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

Expand ▾



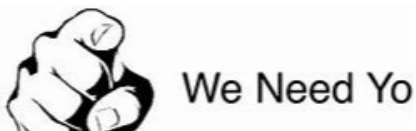
Your IACR



WE NEED YOU!



WE WANT YOU



WE NEED YOU TO MAKE IT HAPPEN



Current topics



Recent work of the Board

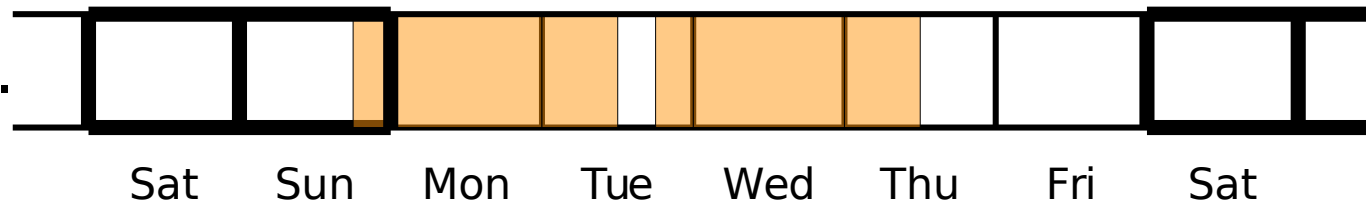
- Find details online
 - iacr.org/docs/minutes/
- Workshops are now an integral part of General Conferences (Asiacrypt, Crypto, Eurocrypt)
- Worried about growing difficulties with visas and problems with international exchange
- Nominations for 2019 election open



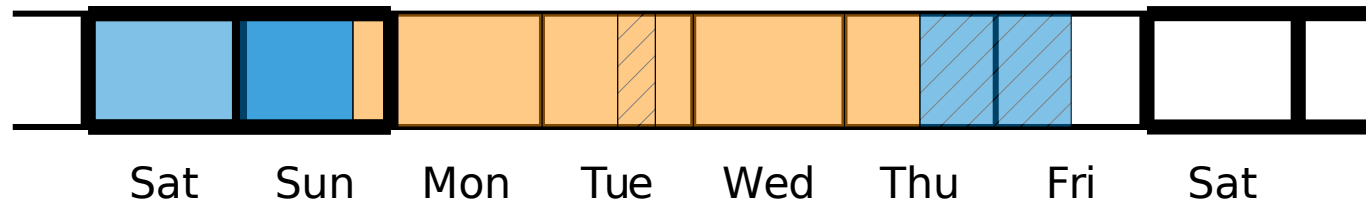
Adjusting to growth

Should we rethink the schedule of AC/EC/CR?

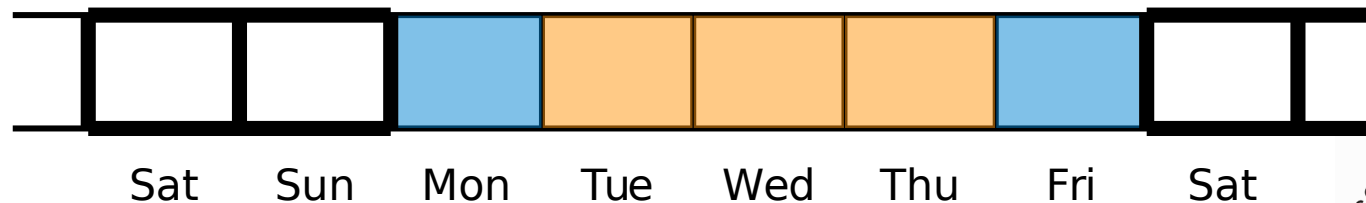
Since 1981...



Today



Alternative?



Open discussion



Upcoming events



Future General Conferences

- Crypto 2019, late Aug, UCSB, Santa Barbara
 - Muthu Venkitasubramaniam (GC)
 - Sasha Boldyreva & Daniele Micciancio (PC)
- Asiacrypt 2019, 8-12 Dec, Kobe (JP)
 - Mitsuru Matsui (GC)
 - Steven Galbraith & Shiho Moriai (PC)



Future General Conferences

- Eurocrypt 2020, 10-14 May, Zagreb (Croatia)
 - Lejla Batina & Stjepan Picek (GC)
 - Yuval Ishai & Anne Canteaut (PC)
- Crypto 2020, late Aug, UCSB, Santa Barbara
 - Leo Reyzin (GC)
 - Daniele Micciancio & NN (PC)
- Asiacrypt 2020, 6-10 Dec, Daejeon (KR)
 - Kwangjo Kim (GC)
 - Shiho Moriai & **Wang Huaxiong** (PC)



Future General Conferences

- Eurocrypt 2021, Apr/May, Trondheim (Norway)
 - Colin Boyd (GC)
 - Anne Canteaut & NN (PC)
- Crypto 2021, late Aug, UCSB, Santa Barbara
 - NN
- Asiacrypt 2021, 5-9 Dec., Singapore
 - Guo Jian (GC)
 - Wang Huaxiong & NN (PC)



Future Area Conf. & Symp.

- CHES 2019, 24-28 Aug, Atlanta (US)
 - Vincent Mooney, Patrick Schaumont, Yunsu Fei (GC)
 - Jorge Guajardo & Pierre-Alain Fouque (TCHES EiC)
- TCC 2019, 1-5 Dec, Nuremberg (DE)
 - Dominique Schröder (GC)
 - Alon Rosen & Dennis Hofheinz (PC)

* * *

- RWC 2020, 8-10 Jan, New York (US)
 - Tom Ristenpart (local organizer)
 - Aggelos Kiayias (PC)



Future Area Conf. & Symp.

- FSE 2020, 22-26 Mar, Athens (GR)
 - Christina Boura (GC)
 - Gaëtan Leurent & Yu Sasaki (ToSC EiC)
- PKC 2020, 27-30 Apr, Edinburgh (UK)
 - Petros Wallden & Markulf Kohlweiss & Viassilis Zikas (GC)
 - Aggelos Kiayias (PC)
- TCC 2020, 16-19 Nov, Durham, NC (US)
 - Alessandra Scafuro (GC)
 - Rafael Pass & Krzysztof Pietrzak (PC)

