International Association for Cryptologic Research

Michel Abdalla
IACR President

Crypto 2021

Membership meeting agenda

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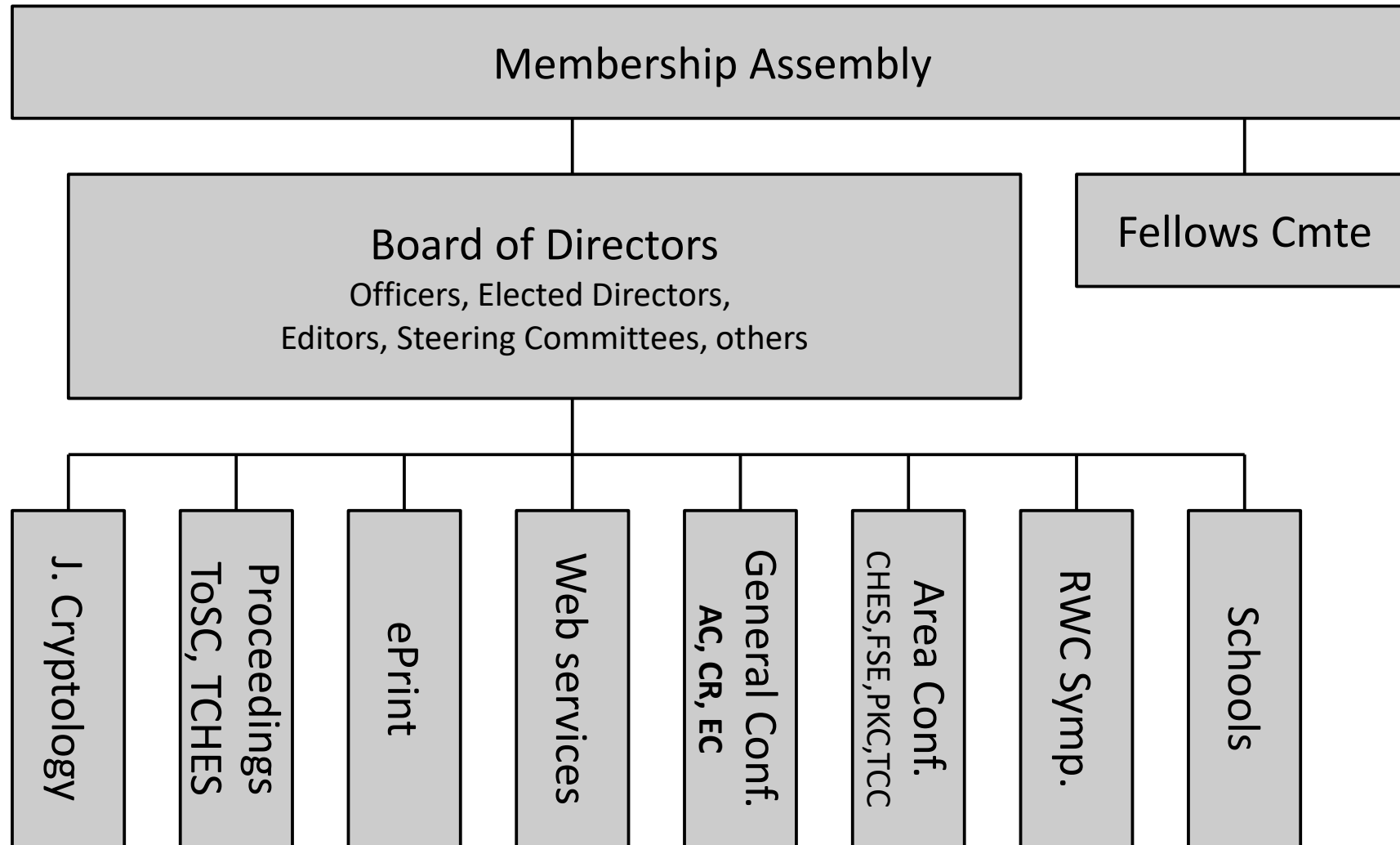- Open discussion
- Future events

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

- Everyone attending an IACR event becomes a member in the next calendar year
  - By attending Crypto 2021, you are a member of the IACR for 2022

- 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/2021/

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 (2021-2023)

Marc Fischlin (2020-2021)

Nadia Heninger (2019-2021)

Tancrède 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)

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

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
- 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
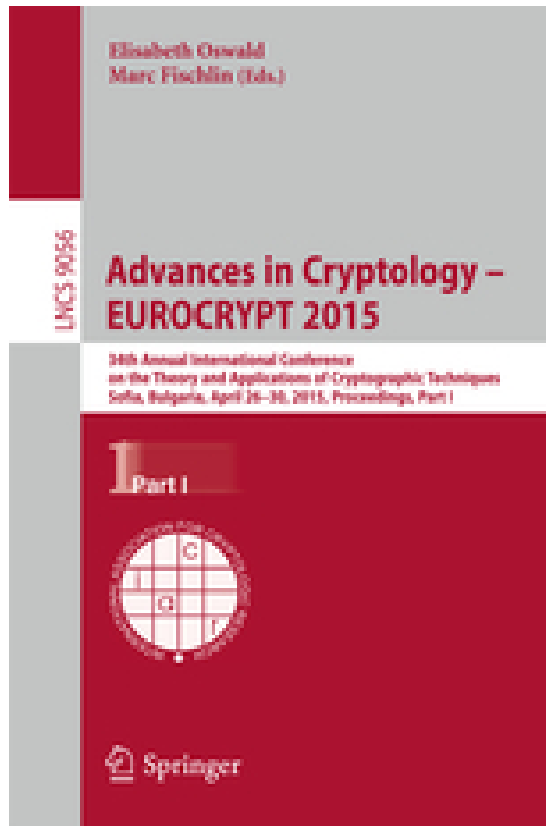
- ASIACRYPT
- CRYPTO
- EUROCRYPT
- PKC
- TCC

- 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 December 31
  - 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.

2021, Asiacrypt – Andrew Yao

2022, Eurocrypt – Ingrid Verbauwhede

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/

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

Online services

iacr.org
ia.cr

Thanks to the team!

- Foteini Baldimtsi
  - Communications Secretary
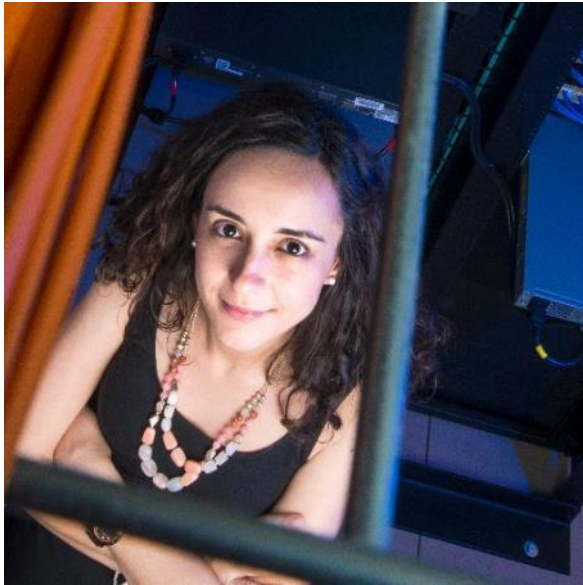
- Yu Yu
  - Webmaster

International Association for Cryptologic Research

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

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.
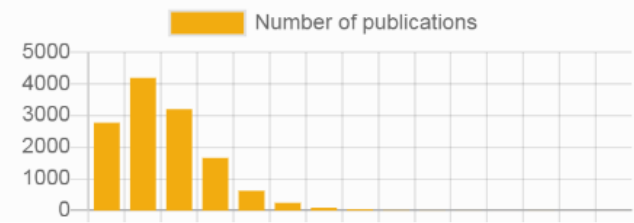
Number of publications

5000
4000
3000
2000
1000
0

International Association for Cryptologic Research

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 ▼

Crypto 2021

⚠ Due to the COVID-19 pandemic, Crypto 2021 will be held virtually. Please note that the dates of the conference have changed to August 16-20 2021.

Register now   **Join the conference**   **Crypto 2021 swag**

Crypto 2021 will take place virtually on August 16-20 2021. Crypto 2021 is organized by the International Association for Cryptologic Research (IACR).

Important Dates

24 Feb 2021	Submission deadline at 21:00 UTC
20 Mar 2021	Workshop proposal submission deadline at 23:59 UTC
1 April 2021	Workshop proposal notification of decision
16 Apr 2021	First round paper notifications
23 Apr 2021	Paper rebuttals due

Website Updates

14 Aug 2021	Rump session page added
12 July 2021	Registration has opened
7 July 2021	Conference dates have changed to 16-20 August 2021
4 July 2021	Tentative program is online
23 Apr 2021	Switch to a virtual conference

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
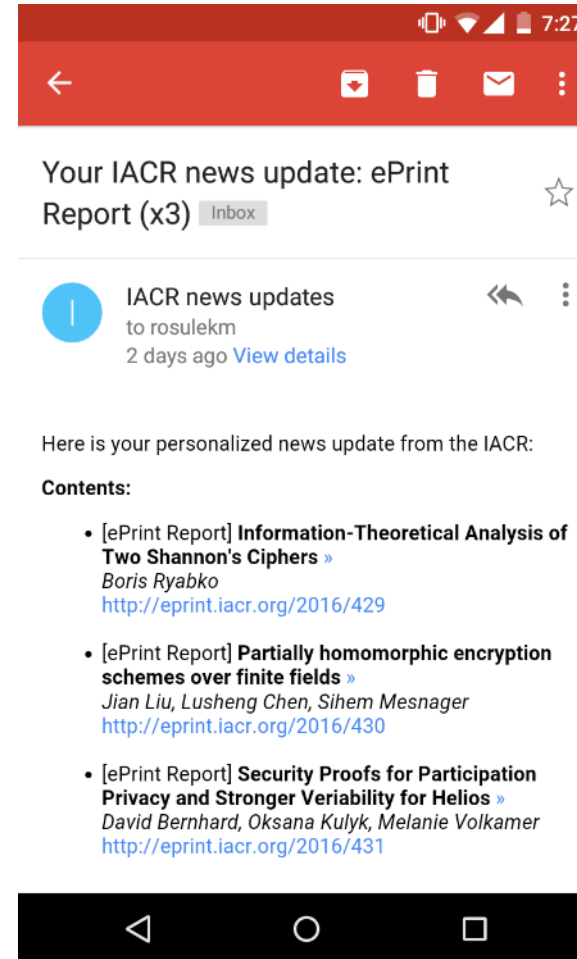
IACR publications portal

- 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

Current topics

Recent work in the Board

- Find details online: iacr.org/docs/minutes/

- COVID-19 Impact

- Hybrid conference implementation

- 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

COVID-19 impact on IACR conferences

- Conferences were converted to an all-digital format
    - Eurocrypt 2020 (May 11-15, 2020)
    - …
    - Asiacrypt 2020 (December 7-11, 2020)
    - RWC 2021 (January 11-14, 2021)
    …
    - Crypto 2021

- No FSE 2021

- Eurocrypt 2021
    - Postponed to October
    - First IACR hybrid conference

- Unchanged for now: TCC 2021, Asiacrypt 2021, RWC 2022

- Affiliated workshops were also 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
  - Small group video conferencing via the conference portal

- 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 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, 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, 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.

- CHES 2021, 12 – 15 Sept, Online
  - Liji Wu, Guoqiang Bai, Zhe Liu, Junfeng Fan (GC)
  - Elke De Mulder & Peter Schwabe (TCHES EiC)

- TCC 2021, 15 – 19 Nov, Raleigh (US)
  - Alessandra Scafuro (GC)
  - Kobbi Nissim & Brent Waters (PC)

- RWC 2022, 10 – 12 Jan, Amsterdam (The Netherlands)
  - Lejla Batina, Joan Daemen, Peter Schwabe (GC)
  - Dan Boneh, Helena Handschuh (PC)

Future Area Conf. & Symp.

- 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)

- CHES 2022, Sept, Beijing, China
  - Liji Wu, Guoqiang Bai, Zhe Liu, Junfeng Fan (GC)
  - Sonia Belaïd & Thomas Eisenbarth (TCHES EiC)

Thank you for your attention!