# International Association for Cryptologic Research

Christian Cachin
President, IACR

CRYPTO 2016

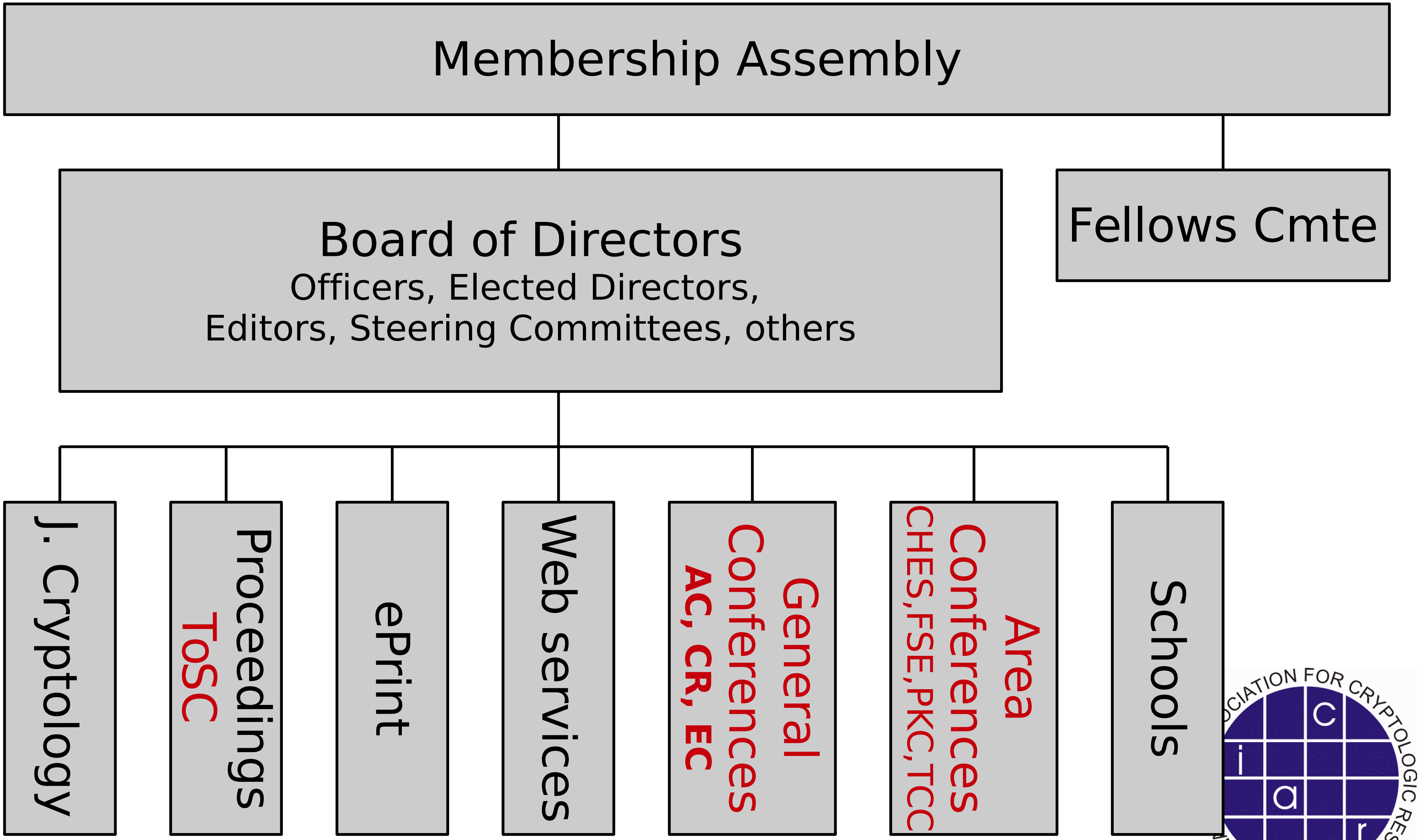
# Membership meeting

- About IACR
  - Publications
  - Conferences
  - Cryptology
- Financial report
- Membership report
- Online services
- Publications
- 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)

# One picture



Membership Assembly

Board of Directors
Officers, Elected Directors,
Editors, Steering Committees, others

Fellows Cmte

J. Cryptology

Proceedings
ToSC

ePrint

Web services

General
Conferences
**AC, CR, EC**

Area
Conferences
CHES,FSE,PKC,TCC

Schools

# Membership

- Everyone attending an IACR event becomes a member in next calendar year
- Become a member online
- Membership fee of $50 ($25 students)

# Board of Directors

- 4 Officers
- 9 elected Directors
- Appointed Directors
  - Includes General Chairs of EC/CR/AC conferences
- Observers
  - Representing Steering Committees of area-confs. (CHES, FSE, PKC, TCC)

- www.iacr.org/bod.html

- In-person meetings at Eurocrypt and Crypto

# Board meeting at CRYPTO

- Reviewed past and planned future operations
- Discussed video recording
- Selected Tal Rabin as GC of CRYPTO 2018
- Selected Mitsuru Matsui as 2018 IACR Distinguished Lecturer
- Selected a Program Co-Chair of EC 2018-19
- Approved CHES 2017 and TCC 2017

# 2016 Elections

- An important election year
  - www.iacr.org/elections/2016/
- 4 Officer positions
  - President, vice president, secretary, treasurer
- 3 Director positions
  - Paar, Pointcheval, Preneel
- Schedule
  - Aug-Sep 24: Nomination phase (to Nigel Smart)
  - Oct-Nov: Online election using Helios
- Committee
  - **Nigel Smart**, Masayuki Abe, Michel Abdalla

# Financial report

# Journal of Cryptology

Journal of CRYPTOLOGY

Volume 27 Number 2
April 2014

Springer

Available online

- Current editor in Chief
  - Ivan Damgård
- Read online
  - www.iacr.org/services/springer.php
- Paper delivery is opt-in for $20 extra
  - Change that in your membership data online
- Online submission reviewing system

# New Editor in Chief for JoC

- Kenny Paterson has been appointed recently

- 2017-2019
- Transition initiated from Ivan Damgård

# IACR Transactions on Symmetric Cryptology (ToSC)

- New publication, replacing Proceedings of FSE
- Journal with rapid and strict review schedule
- Online only, published by Bochum Univ. library
- **Gold open access**
- Publication in ToSC gives presentation at FSE
  - Conference-journal hybrid (PVLDB, PoPETS …)

# ToSC operation

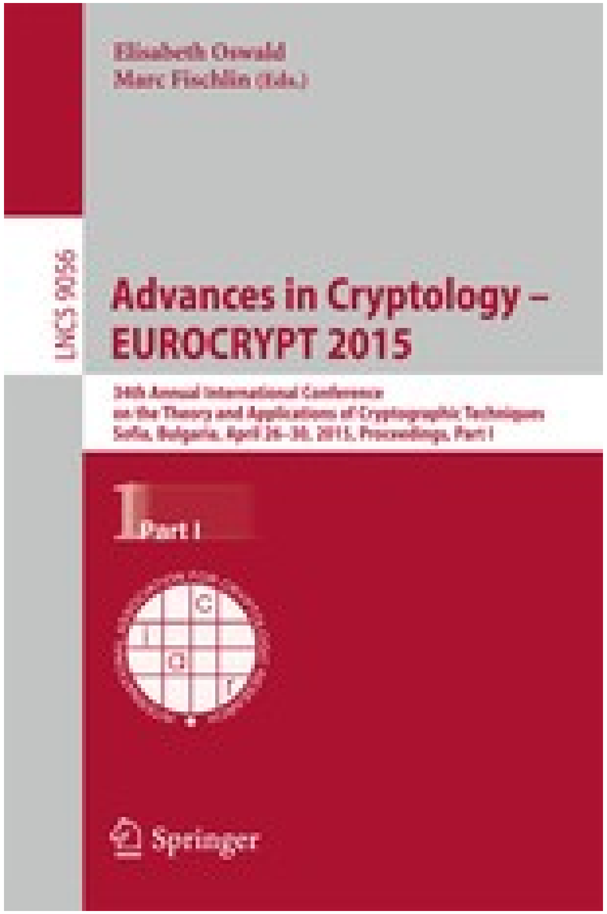
- Editors in Chief for 2016
  - María Naya-Plasencia & Bart Preneel

- Schedule
  - 4 submission deadlines/year and 4 review periods

  - Decision after approx. 2 months
    - Accept
    - Conditional accept
    - Major revision (→ must resubmit after 3 or 6 months; decision will be accept or reject, not another revision)
    - Reject (a different paper can be submitted later)

  - Papers accepted by January 20xx must be presented at FSE 20xx

# Conference proceedings



Elisabeth Oswald
Marc Fischlin (Eds.)

LNCS 9056

Advances in Cryptology –
EUROCRYPT 2015

34th Annual International Conference
on the Theory and Applications of Cryptographic Techniques
Sofia, Bulgaria, April 26–30, 2015, Proceedings, Part I

Part I

Springer

- ASIACRYPT
- CRYPTO
- EUROCRYPT
- CHES
- ~~FSE~~
- PKC
- TCC

- Online for members
  - www.iacr.org/proceedings
- Online for all (> 4yr)
  - link.springer.com

# Cryptology schools

- IACR reviews proposals and supports some schools each year
  - Educational, typically 1-week, learning required (Summer/Winter/Spring/Fall school)
  - Financial support for speakers etc. and publicity
- Next proposals are due August 31 (extended)
  - Committee chaired by Michel Abdalla
  - www.iacr.org/schools/

# 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 – 2016

- Ed Dawson
- Shai Halevi
- Victor Shoup
- Nigel P. Smart

Nominations for 2017 Fellows due by 31 Dec.

Information will be on website later in the year
www.iacr.org/fellows/

# Membership report

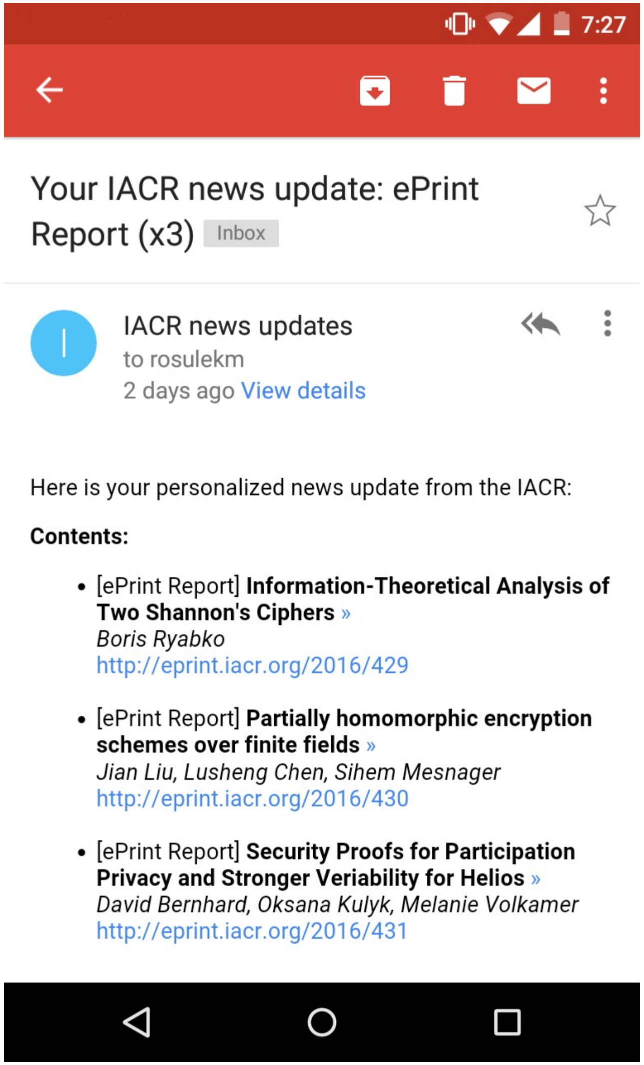
# Online services

**iacr.org**
**ia.cr**

# 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/theiacr
  - Weibo: weibo.com/iacr
  - Email: iacr.org/news/subscribe



Your IACR news update: ePrint Report (x3) Inbox

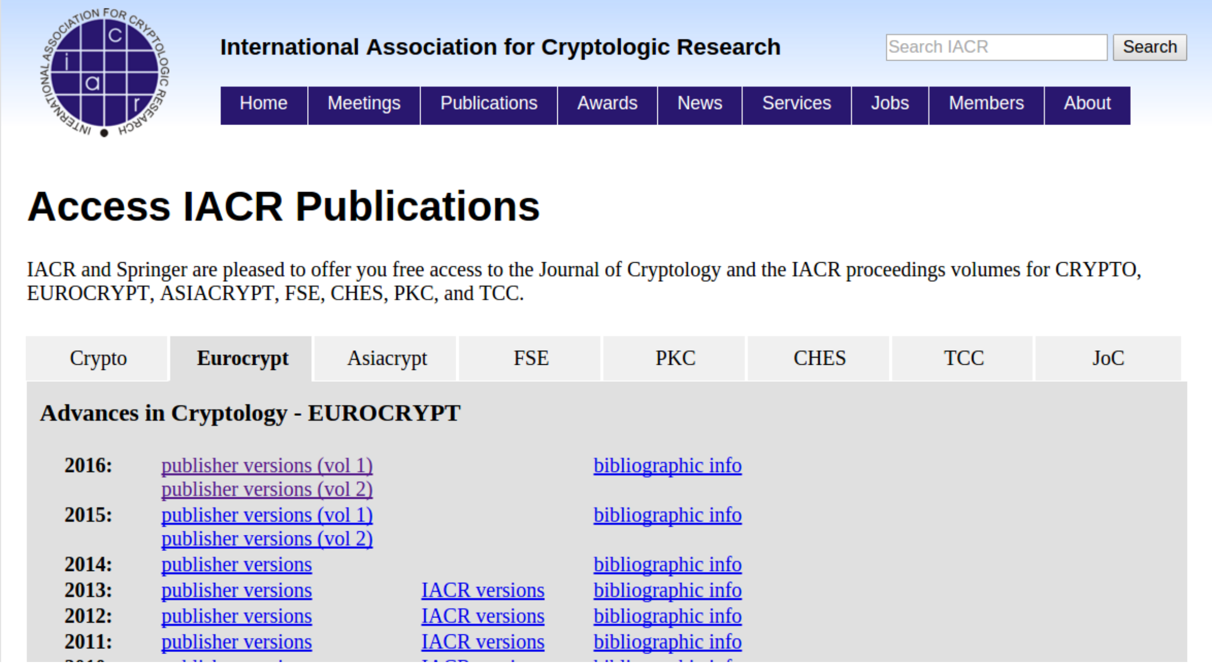
IACR news updates
to rosulekm
2 days ago View details

Here is your personalized news update from the IACR:

**Contents:**

- [ePrint Report] **Information-Theoretical Analysis of Two Shannon's Ciphers** »
  *Boris Ryabko*
  http://eprint.iacr.org/2016/429
- [ePrint Report] **Partially homomorphic encryption schemes over finite fields** »
  *Jian Liu, Lusheng Chen, Sihem Mesnager*
  http://eprint.iacr.org/2016/430
- [ePrint Report] **Security Proofs for Participation Privacy and Stronger Veriability for Helios** »
  *David Bernhard, Oksana Kulyk, Melanie Volkamer*
  http://eprint.iacr.org/2016/431

# IACR publications portal



International Association for Cryptologic Research

## 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.

**Advances in Cryptology - EUROCRYPT**

| | | | |
|---|---|---|---|
| **2016:** | publisher versions (vol 1)<br>publisher versions (vol 2) | | bibliographic info |
| **2015:** | publisher versions (vol 1)<br>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: Springer version, IACR members only
  after 2 years: “IACR version”, public access
  after 3-4 years: Springer version, open access

# All online services

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

# Cryptography Research Fund for Students

- With donation from CRI, IACR has created Cryptography Research Fund for Students
- Sponsors student participation at IACR events
  - Waive registration fee for student speakers at EUROCRYPT, CRYPTO, ASIACRYPT, CHES, FSE, TCC and PKC
  - Support for Cryptology Schools
  - More ideas are welcome

# Cryptology ePrint Archive

**eprint.iacr.org**

# Cryptology ePrint Archive

- eprint.iacr.org
- More than 1000 pre-prints per year
- Sasha Boldyreva & Tancrède Lepoint, editors

# Reminders & good practice

- Abstracts should be self-contained
- Abstracts will be copied without context
  - No references to document
  - No citations like [12], use Cachin et al. 2012
- Do not cut&paste your abstract from PDF
- Do not cut&paste your abstract from LaTeX
- LaTeX math commands are fine (MathJax)
  - All other LaTeX is an error

# All final versions of papers must be submitted to eprint

- IACR copyright asks you to upload final version of paper to eprint

- Upload is automated — if you do not specify the eprint reference for a camera-ready version, then it is automatically uploaded eprint!

- Prone to errors — likely a duplicate/bad/wrong version
  - If you resubmit the final version this does not update the eprint version
  - Any bugs are your responsibility to fix

- => Submit to eprint before you submit the final version to program chair

# Video recordings

# Videos & presentations

- Parallel sessions make it more important to have recordings
- Publication on Youtube channel
  - Thanks to Kevin McCurley for many hours of work!
- IACR consent & copyright form asks for permission to release
  - Video recording of talk (voice vs. full video)
  - Presentation material (static PDF)
- Board suggests that recording and publication of video and presentation be made mandatory

# Video editor needed

- Help all General Chairs with format
- Process recordings
- Publish on current channel
- Archive for future use
- Please come talk to me (president@iacr.org)

# Open discussion

# Upcoming events

# Cryptology Schools 2016

- Computational Algebraic Number Theory School (with ECC 2016)
  - ecc2016.yasar.edu.tr/school.html
  - Izmir (TR), 1-7 Sep, 2016

- IACR-SEAMS School "Cryptography: Foundations and New Directions"
  - viasm.edu.vn/en/hdkh/cryptoschool2016
  - Hanoi, Vietnam, 27 Nov-4 Dec, 2016

- School on Randomness in Cryptography
  - eventum.upf.edu/go/school_randomness_cryptography
  - Barcelona (ES), 14-18 Nov, 2016

# Future General Conferences

- Asiacrypt 2016, 4-8 Dec, Hanoi (Vietnam)
  - Phan Duong Hieu & Ngo Bao Chau (GC)
  - Jung Hee Cheon & Tsuyoshi Takagi (PC)
  - www.asiacrypt2016.com
- Eurocrypt 2017, 30 Apr-4 May, Paris (France)
  - Michel Abdalla (GC)
  - Jean-Sébastien Coron & Jesper Buus Nielsen (PC)
  - eurocrypt2017.di.ens.fr

# Future General Conferences

- Crypto 2017, 20-24 Aug (tent.), UCSB, Santa Barbara
  - Steve Myers (GC)
  - Jonathan Katz & Hovav Shacham (PC)
  - IACR Distinguished Lecture by Shafi Goldwasser

- Asiacrypt 2017, 3-7 Dec, Hong Kong (HK)
  - Duncan Wong & SM Yiu (GC)
  - Tsuyoshi Takagi & Thomas Peyrin (PC)

- Eurocrypt 2018, 29 Apr-3 May, Tel Aviv (IL)
  - Orr Dunkelman (GC)
  - Jesper Buus Nielsen & NN (PC)

# Future General Conferences

- Crypto 2018, 19-23 Aug (tent.), UCSB, Santa Barbara
  - Tal Rabin (GC)
  - Hovav Shacham & NN (PC)

- Asiacrypt 2018, 2-6 Dec, Brisbane (AU)
  - Josef Pieprzyk (GC)
  - Thomas Peyrin & NN (PC)
  - IACR Distinguished Lecture by Mitsuru Matsui

- Eurocrypt 2019, Apr/May, Darmstadt (DE)
  - Marc Fischlin (GC)
  - NN & NN (PC)

# Future Area Conferences

- TCC 2016-B, 1-3 Nov. Beijing (CN)
  - Dongdai Lin (GC)
  - Martin Hirt & Adam Smith (PC)
- FSE 2017, March 5-8, Tokyo (JP)
  - Tetsu Iwata & Shiho Moriai (GC)
  - María Naya-Plasencia & Bart Preneel (TOSC EIC)
- PKC 2017, March 28-31, Amsterdam (NL)
  - Marc Stevens (GC)
  - Serge Fehr (PC)

# Future Area Conferences

- CHES 2017, 25-28 Sep, Taipei (TW)
  - Bo-Yin Yang & Chen-Mou Cheng (GC)
  - Naofumi Homma & Wieland Fischer (PC)

- TCC 2017, 13-15 Nov, JHU/Baltimore (US)
  - Abhishek Jain (GC)
  - Yael Kalai & Leonid Reyzin (PC)

# Next Event: Goleta Beach