International Association for Cryptologic Research

Christian Cachin
President, IACR

Asiacrypt 2016

Program Chairs' Report

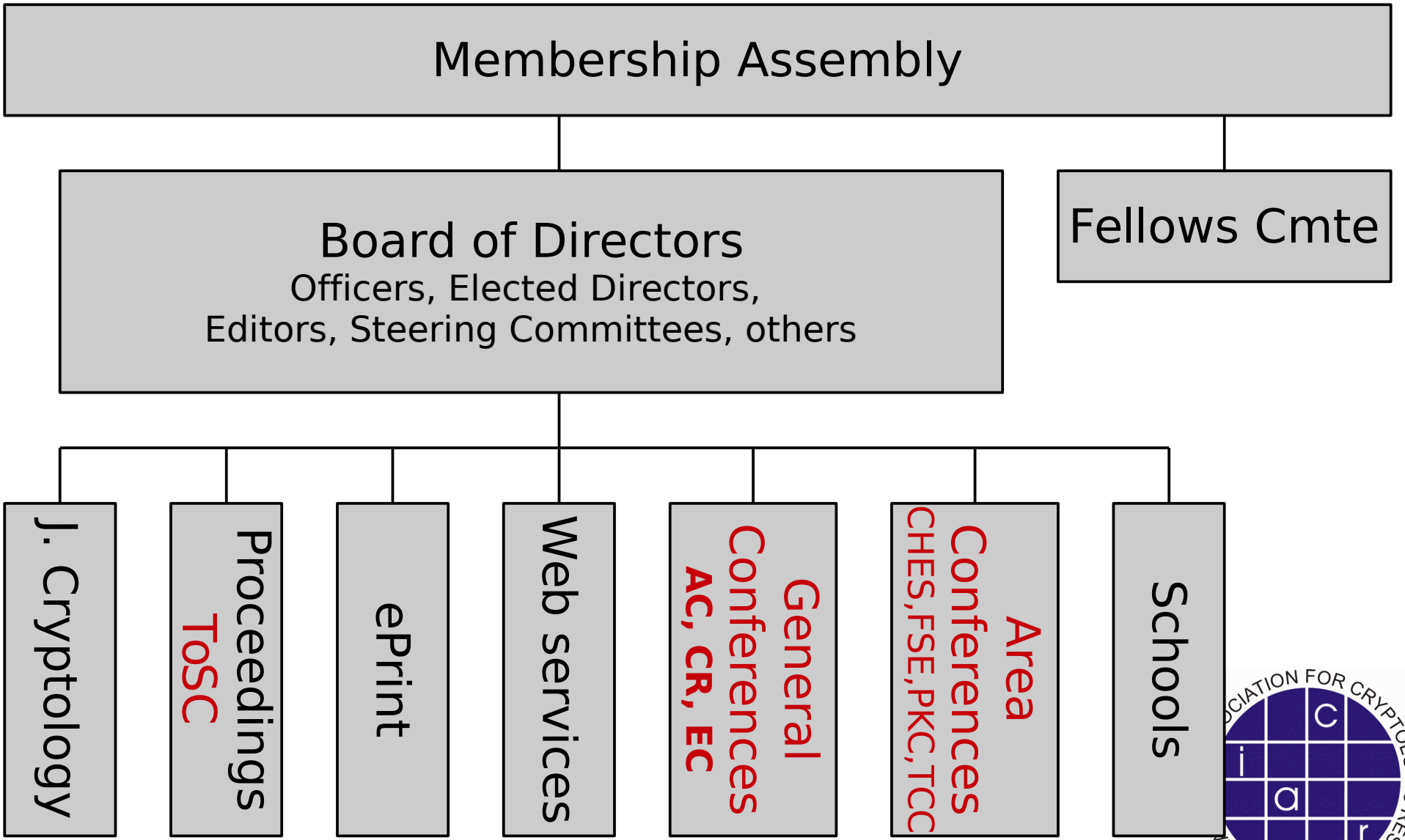
Membership meeting

- 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
- Membership fee of $50 ($25 students)
- Become a member online
- If you don't attend a conference in a calendar year, renew your membership online 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)

- www.iacr.org/bod.html

- In-person meetings at Eurocrypt and Crypto

Recent actvities of the Board

- Past and planned future operations
- Video recording
- Selected Tal Rabin as GC of CRYPTO 2018
- Selected Mitsuru Matsui as 2018 IACR Distinguished Lecturer
- Selected Vincent Rijmen as PC of EC 2018-19
- Approved CHES 2017, CHES 2018, TCC 2017 and two IACR schools

2016 Elections

- "Big" election
  - www.iacr.org/elections/2016/
- 4 Officer positions
  - President: Christian Cachin
  - Vice president: Greg Rose
  - Secretary: Joppe Bos
  - Treasurer: Brian LaMacchia
- 3 Director positions
  - Bart Preneel
  - Shai Halevi
  - Francois-Xavier Standaert

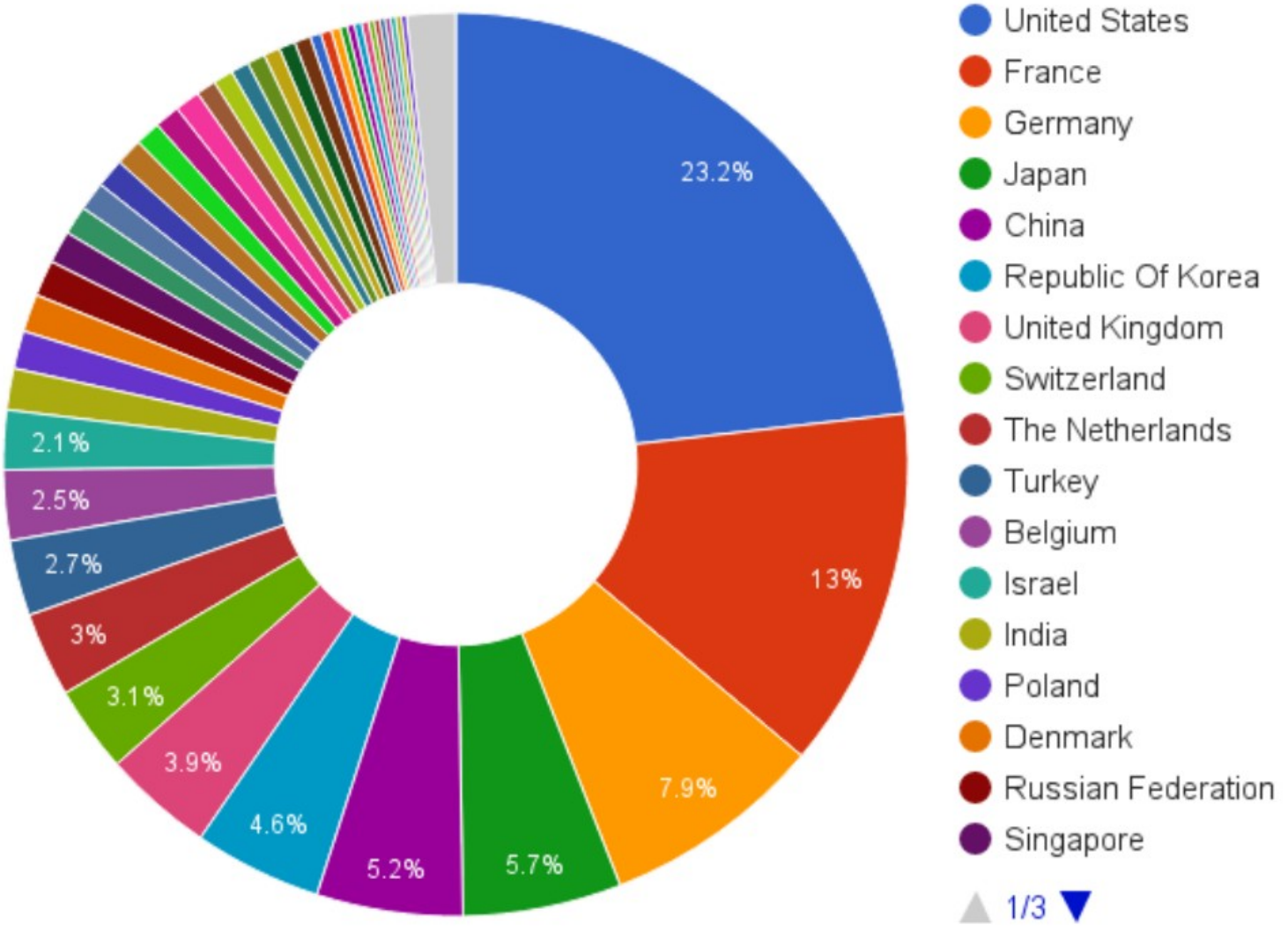
Finanical summary

- Low overhead, less than 2% for administration
- Sufficient reserves, log($) ≈ 21
  - Cryptography Research Fund (donation) allows substantial sponsorship
    - Registration waivers for all student speakers
    - Support for IACR schools
- Keep membership fee of $50 / $25

Membership summary

- 1552 members (1176 regular / 376 students)
- Increased from last year...
  - 1469 members in 2015

Membership By Country



Journal of Cryptology

- 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 from Ivan Damgård

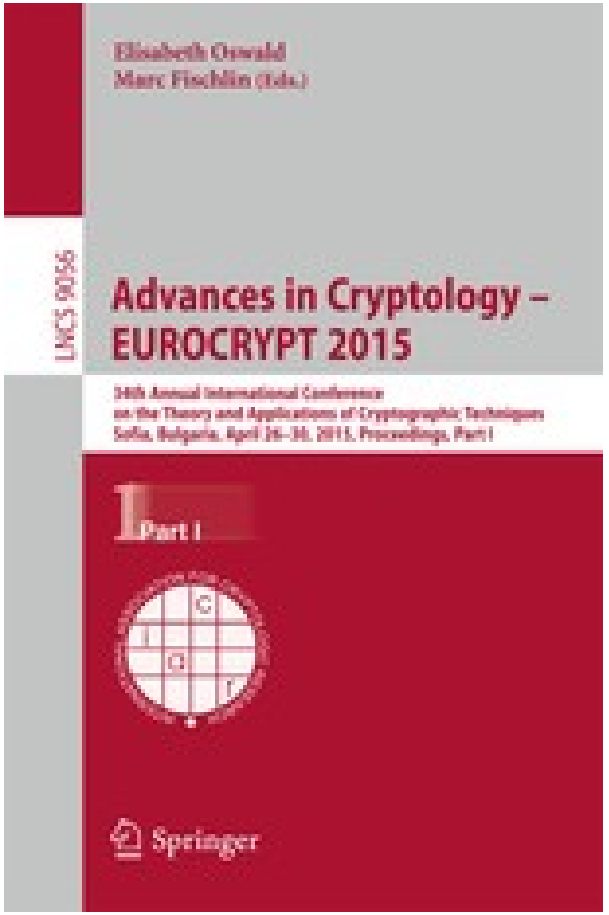
IACR Transactions on Symmetric Cryptology (ToSC)

- 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



- 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 December 31
  - 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.

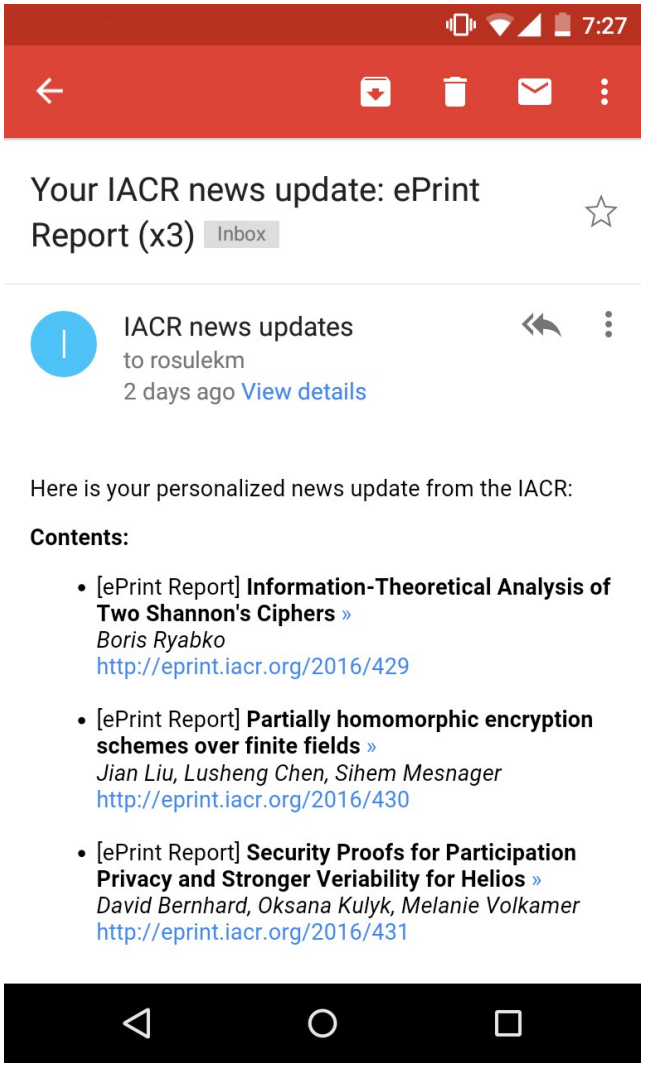
Information will be on website later in the year
www.iacr.org/fellows/

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



IACR publications portal

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 2017

- School on Security and Correctness in the Internet of Things
  - Graz (AT), spring 2017
  - Stefan Mangard, Graz University of Technology
- Advanced School on Cryptology and Information Security in Latin America (ASCcrypto)
  - September 17-19, 2017, la Havana, Cuba
  - Daniel J. Bernstein and Francisco Rodriguez-Henriquez

Future General Conferences

Eurocrypt 2017, 30 Apr-4 May, Paris (France)

- Michel Abdalla (GC)
- Jean-Sébastien Coron & Jesper Buus Nielsen (PC)
- eurocrypt2017.di.ens.fr

- Crypto 2017, 20-24 Aug, UCSB, Santa Barbara
  - Steve Myers (GC)
  - Jonathan Katz & Hovav Shacham (PC)
  - IACR Distinguished Lecture by Shafi Goldwasser
  - www.iacr.org/conferences/crypto2017/

Future General Conferences

- 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 & Vincent Rijmen (PC)

Future General Conferences

- Crypto 2018, 19-23 Aug, 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)
  - Vincent Rijmen & NN (PC)

Future Area Conferences

- 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)
- 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)

Thank you!


INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
c
i
a
r