International Association for Cryptologic Research

Christian Cachin
President, IACR

EUROCRYPT 2016

Membership meeting

- About IACR
  - Publications
  - Conferences
  - Cryptology Schools
- Online services

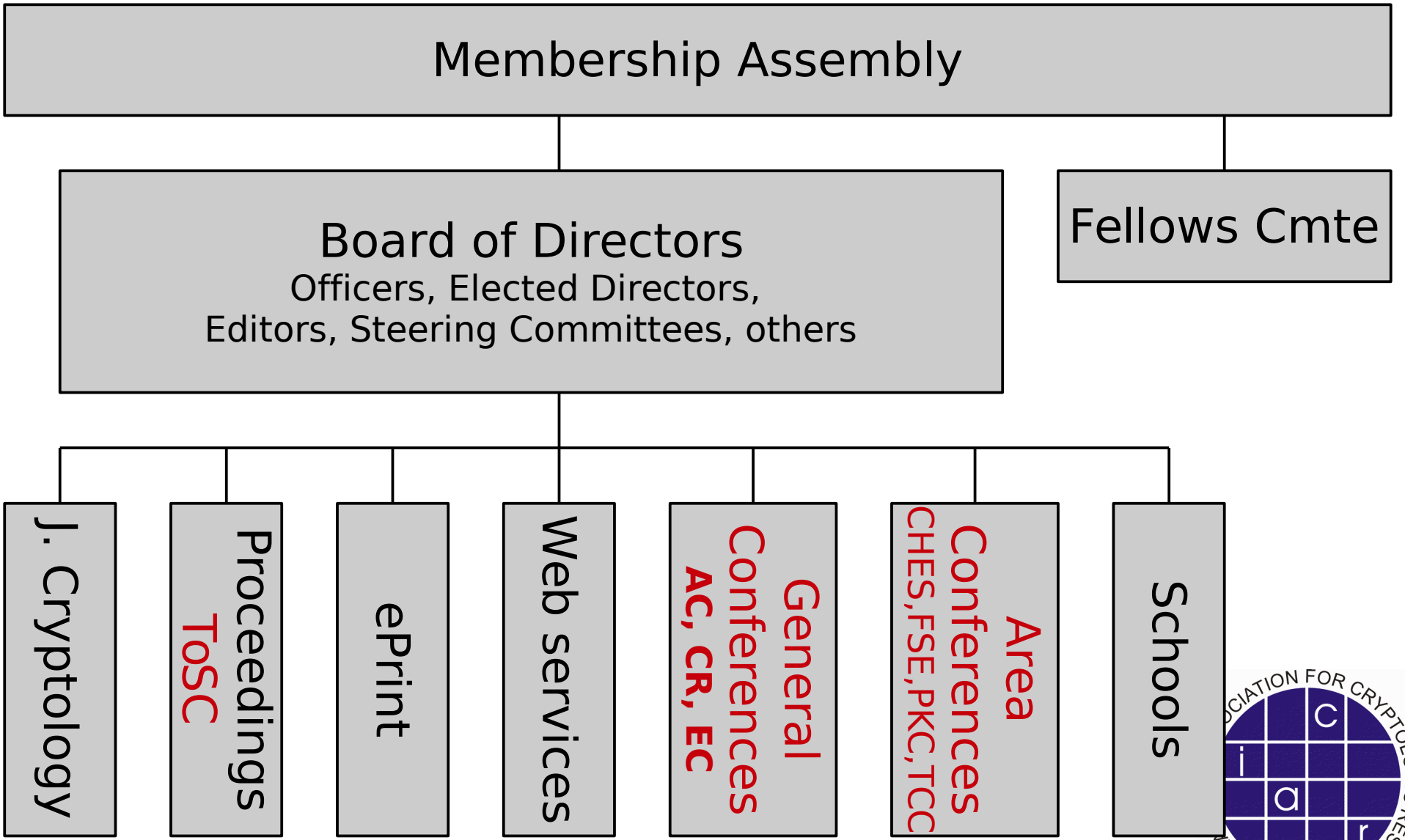
- Financial report

- 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

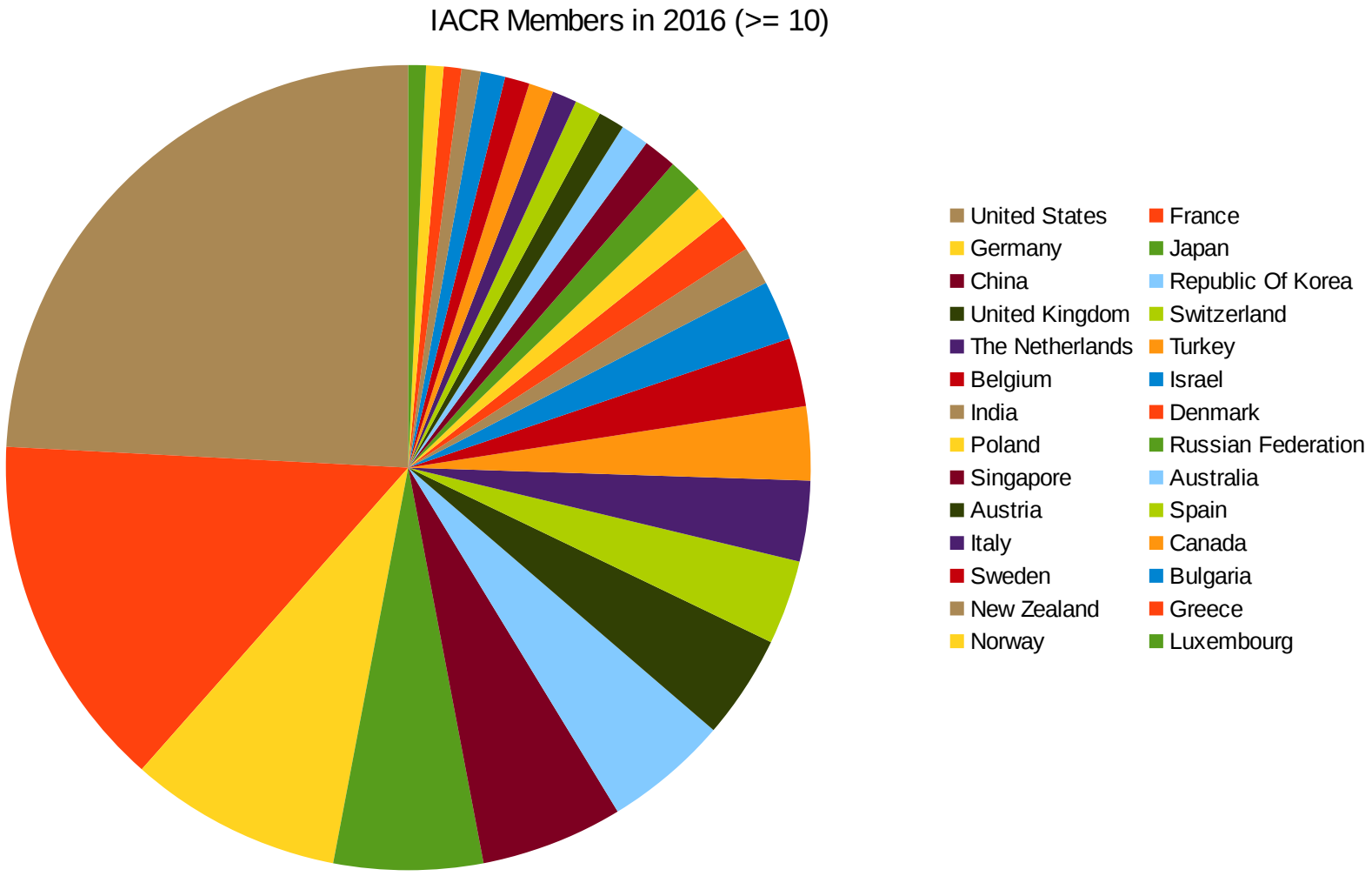
Membership

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

Member statistics

Current total 1526

Member statistics



Board of Directors

- 4 Officers
- 9 elected Directors
- Appointed Directors and observers

- www.iacr.org/bod.html

- Election of 3 Director positions every year
  - 2016 election in October/November
    - www.iacr.org/elections/2016/

  - 4 Officers
  - 3 Directors

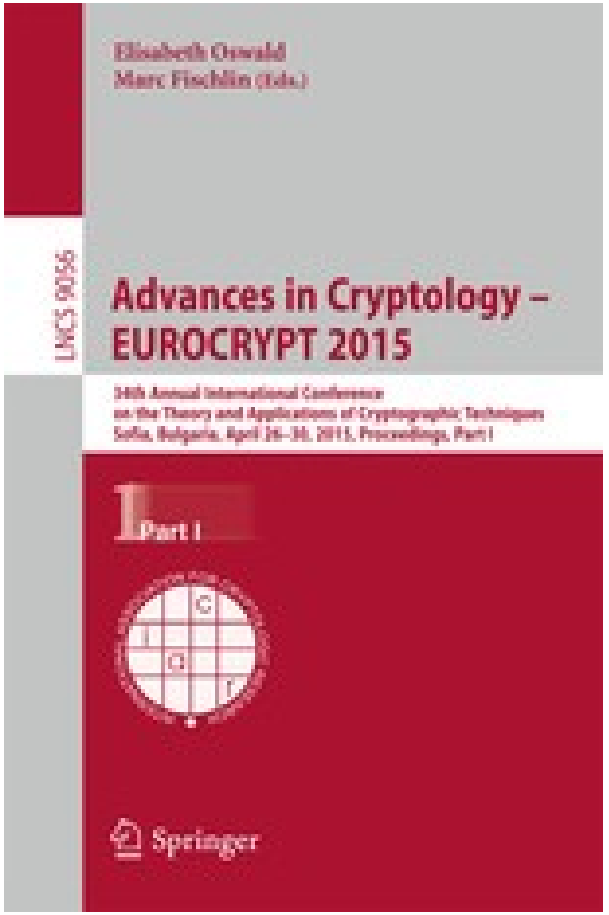
Journal of Cryptology

- 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

Search for new Editor in Chief

- Ivan Damgård will step down as EiC of Journal of Cryptology by Dec 2016
- Search process for new EiC initiated
- Committee
  - Christian Cachin
  - Ivan Damgård
  - Phillip Rogaway

Proceedings



- ASIACRYPT
- CRYPTO
- EUROCRYPT
- CHES
- FSE → ToSC
- 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 June 30
  - 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/

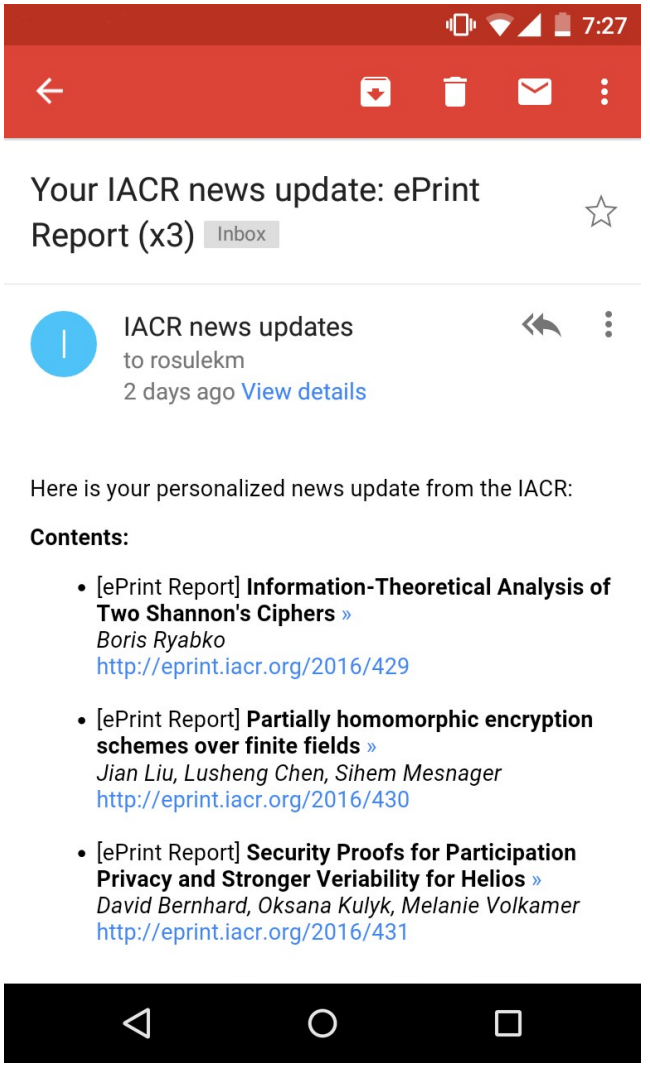
Online services

iacr.org

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 4 years: Springer version, open access

All online services

- Cryptology ePrint Archive
  - Sasha Boldyreva & Nigel Smart, editors
- Access to Springer proceedings & IACR versions
- Open positions in cryptology
- Calendar of events
- Museum of historic papers
- CryptoDB: bibliography database
- Petitions
- PhD genealogy 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

- More than 1000 pre-prints per year
- Sasha Boldyreva & Nigel Smart (editors)

Reminders & good practice

- Abstracts should be self-contained
- Abstracts are 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
  - 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

Financial report

Publications

Publications and Open Access

- Green-OA
  - Authors may publish their versions of a paper freely online (home page, eprint repositories), access to main publication is limited
  - LNCS proceedings, when ≤ 4 years after release
  - Journal of Cryptology
- Gold-OA
  - Main publication is accessible freely (online)
  - LNCS proceedings, when ≥ 4 years after release
  - IACR Transactions on Symmetric Cryptology

IACR Transactions on Symmetric Cryptology (ToSC)

- New publication, replacing Proceedings of FSE
- Journal with rapid and strict review schedule
- Gold open access
- Publication in ToSC gives presentation at FSE
  - Conference-journal hybrid
  - Similar to PVLDB, PoPETS ...

FSE proceedings → ToSC

- ToSC will only be published online
- 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

ToSC mechanics

- Editorial board of ToSC replaces FSE program committee
  - Program Chair → Editor in Chief
  - María Naya-Plasencia & Bart Preneel
- RUB library operates ToSC at no cost to IACR
  - RUB library already publishes OA journals
- Open-source journal publishing platform
- Authors must strictly adhere to format and schedule

Open discussion

Upcoming events

Cryptology Schools 2016

- Blockchain Technologies: from cryptographic e-cash to modern cryptocurrency
  - Corfu (GR), 30 May-2 June, 2016
  - bitcoinschool.gr

- IACR-SEAMS School on Cryptography
  - viasm.edu.vn/en/hdkh/cryptoschool2016
  - Hanoi, Vietnam, 24 Nov-2 Dec, 2016

- School on Randomness in Cryptography
  - M. Barbosa, J.P. Degabriele, P. Farshim
  - Barcelona (ES), 14-17 Nov, 2016

Cryptology Schools 2016

- ECC2016 Computational Algebraic Number Theory School
  - Izmir (TR), 1-4 Sep, 2016
  - ecc2016.yasar.edu.tr/school.html

Future General Conferences

- Crypto 2016, 14-18 Aug, UCSB, Santa Barbara
  - Brian LaMacchia (GC)
  - Matt Robshaw and Jonathan Katz (PC)
  - iacr.org/conferences/crypto2016/
- 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 & NN (PC)
  - IACR Distinguished Lecture by Shafi Goldwasser
- Asiacrypt 2017, 3-7 Dec, Hong Kong (HK)
  - Duncan Wong & SM Yiu (GC)
  - Tsuyoshi Takagi & NN (PC)

Future General Conferences

- Eurocrypt 2018, 29 Apr-3 May, Tel Aviv (IL)
  - Orr Dunkelman (GC)
  - NN & NN (PC)
- Asiacrypt 2018, 2-6 Dec, Brisbane (AU)
  - Josef Pieprzyk (GC)
  - NN & NN (PC)
- Eurocrypt 2019, Apr/May, Darmstadt (DE)
  - Marc Fischlin (GC)
  - NN & NN (PC)

Future Area Conferences

- CHES 2016, 16-19 Aug., UCSB, Santa Barbara
  - Cetin Kaya Koc & Erkay Savas (GC)
  - Benedikt Gierlichs & Axel Poschmann (PC)
- TCC 2016-B, 1-3 Nov. Beijing (CN)
  - Dongdai Lin (GC)
  - Martin Hirt & Adam Smith (PC)
- PKC 2017, March 28-31, Amsterdam (NL)
  - Marc Stevens (GC)
  - Serge Fehr (PC)