IACR Membership Meeting
Eurocrypt 2012, Cambridge, UK

Bart Preneel

presidentHEREATiacr.org

http://www.iacr.org

Agenda

- About IACR & Your Board
- Membership & Elections
- Financial Report
- Conferences & Workshops
- IACR Fellows
- Publications
- Current Board Activities
- Open Discussion

About IACR

- Non-profit organisation registered in the USA

- The Association's purposes are "to advance the theory and practice of cryptology and related fields, and to promote the interests of its members with respect thereto, and to serve the public welfare"

Delivering

- Eurocrypt, Crypto, Asiacrypt
- FSE, PKC, CHES, TCC
- Journal of Cryptology and newsletter
- IACR archive of past proceedings
  - http://www.iacr.org/archive
- ePrint server
  - http://eprint.iacr.org/

About IACR

- Run by a Board of Directors
  - 4 elected Officers
  - 9 elected Directors
  - 6 General Chairs
- Supported by
  - JoC editor in Chief, Membership Secretary, Archivist, Database Administrator
  - Representatives of Asiacrypt, PKC, FSE, CHES & TCC Steering Committees

Your Board ('12)

OFFICERS

- Bart Preneel
- Christian Cachin
- Martijn Stam
- Greg Rose

DIRECTORS

- Josh Benaloh
- Tom Berson
- Shai Halevi
- Matsuru Matsui
- David Naccache
- Christof Paar
- David Pointcheval
- Nigel Smart
- Serge Vaudenay

Your Board ('12)

APPOINTEES

- Matt Franklin
- abhi shelat
- Kevin McCurley
- Hilarie Orman
- Christopher Wolf

GENERAL CHAIRS

- (Nigel Smart)
- Lisa Yiqun Lin
- Xuejia Lai
- Aggelos Kiayias
- Helena Handschuh
- Satyanarayana V. Lokam

STEERING COMMITTEE REPRESENTATIVES

- Tsutomu Matsumoto
- Jean-Jacques Quisquater
- (Bart Preneel)
- (David Pointcheval)
- Ivan Damgård

Membership

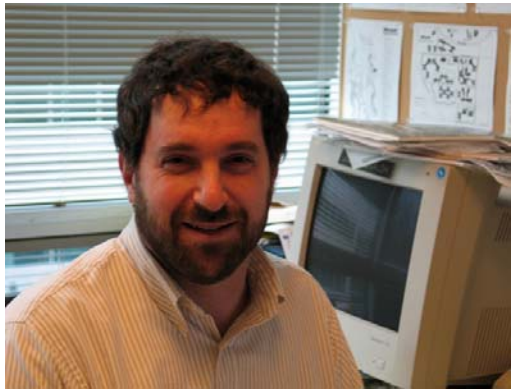
- By attending this conference, you will become a member of IACR for 2013
- If you attended one of our conferences or workshops last year, you are already a member for 2012

IACR Election

- There is an election for Board members every year in the Fall
  - in 2013 the terms of 3 elected Directors expire
  - we are actively seeking interested members to join the Board
  - please contact any Board member (or a member of the 2013 Election Committee) if you would like to know more, or are interested in standing for election

IACR Election Committee 2012

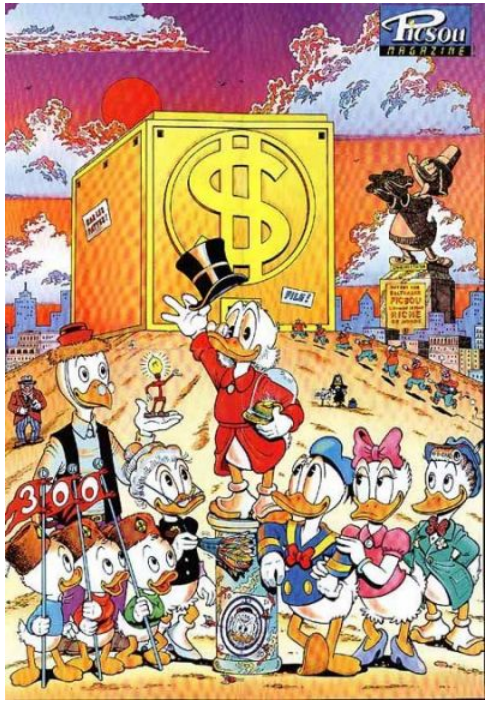
Josh Benaloh



David Pointcheval

Greg Rose

IACR Financial Report 2011



Greg Rose

treasurer@iacr.org

Financial Summary - 2011

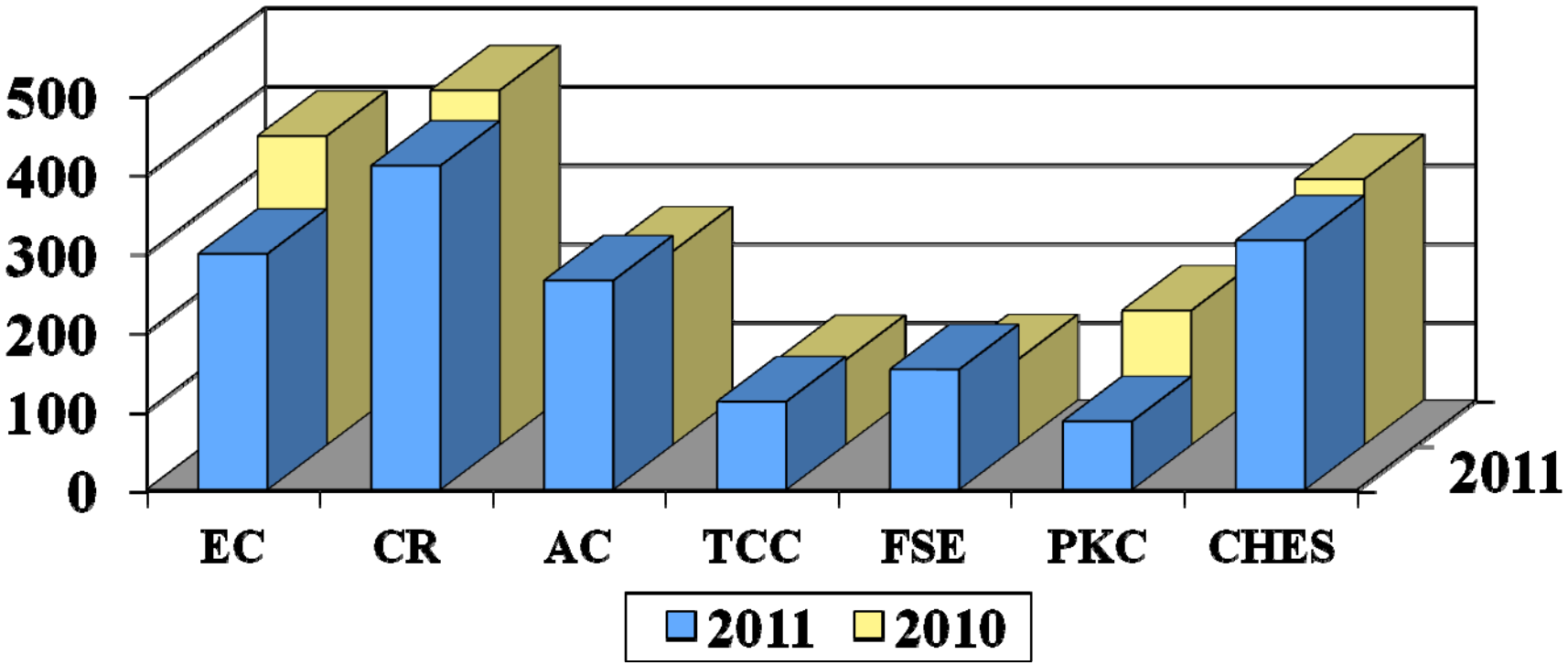
- US economy recovering a little, European not so much.
- Financial support from sponsoring organisations increasing greatly, maybe due to recruiting?

- Attendance at our events down a little overall
  - PKC(87), TCC(112),
  - FSE(153), CHES(317)
  - Crypto (412)
  - Eurocrypt (300), Asiacrypt (266)

- Extremely low administration overhead : < 2%

- ***Strong financial position for IACR***

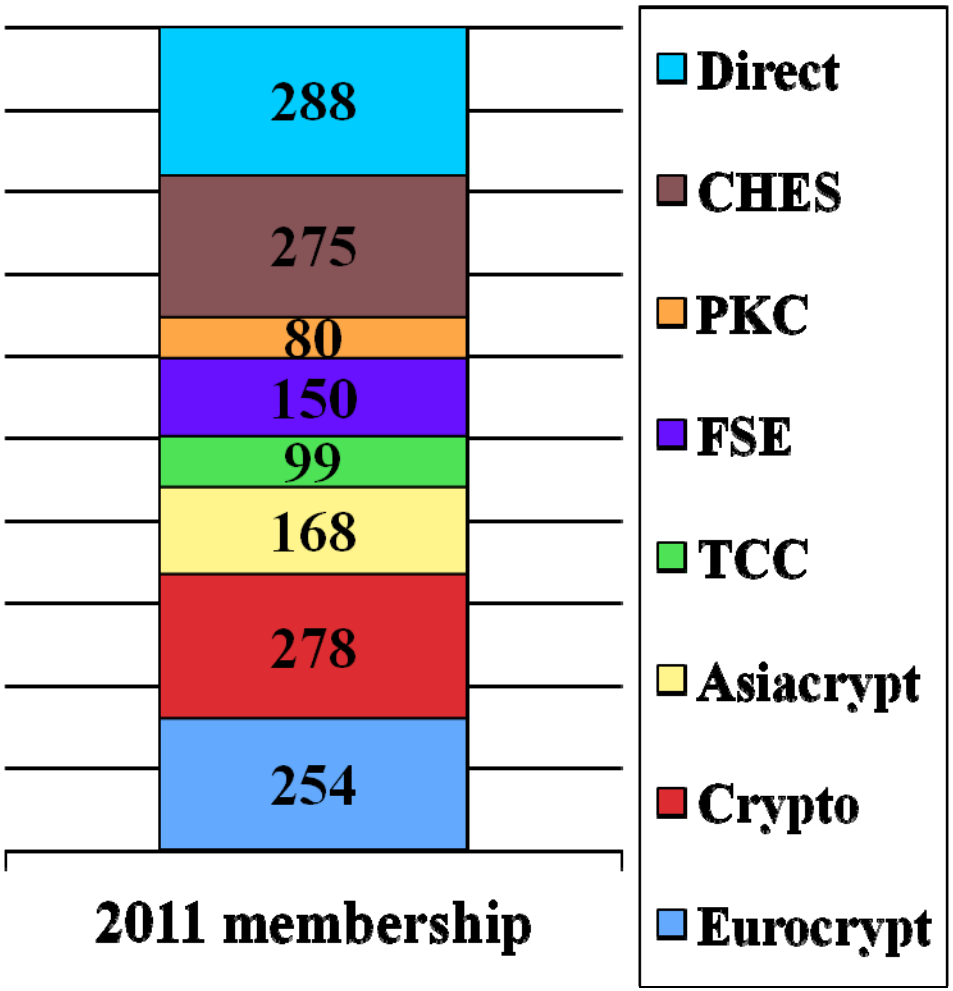
2010/2011 Conferences and Workshops



PKC: Paris more popular than Taormina? 2010 unusual

2010: Crypto and CHES co-located

2011 Membership



2012 Membership fees collected in 2011:

- Conferences and Workshops
- Directly through IACR
- US$ 70/35

2012 Highlights

- Conference registration waivers for student speakers
- Marconi grant will run out but sponsorships increasing
- Target break-even (or slight loss) budgets
- Keep minimal overhead - less than 2%
- Membership fee US$ 70/35

Questions for the Treasurer

IACR Membership

2012

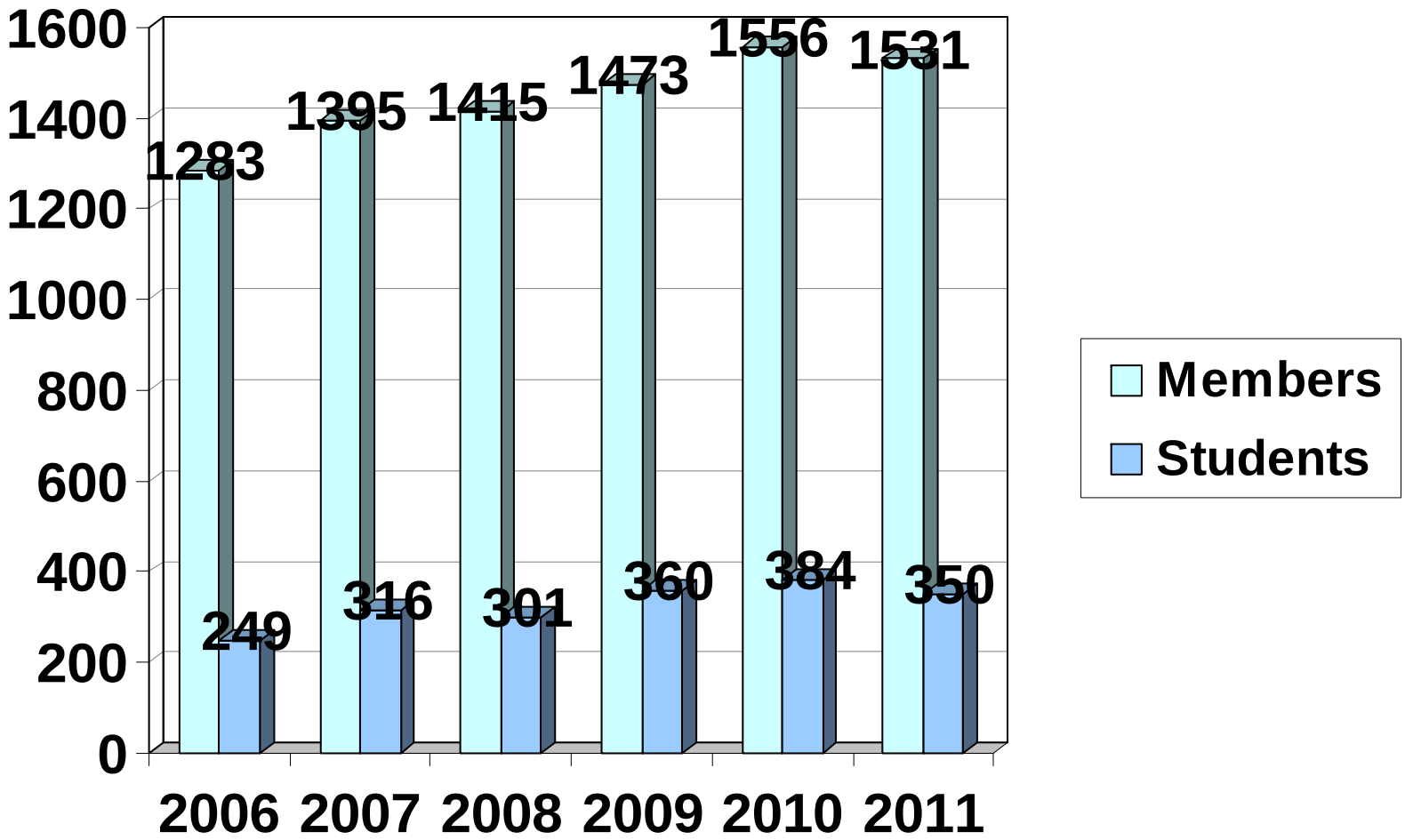
abhi shelat

iacrmemHEREATiacr.org

Thanks to Shai Halevi

- 6 years of dedicated service as membership secretary (2006-2011)

Total Membership



On-Line services

- All on the same server
  - www.iacr.org
  - ePrint
  - newsletter, mailing lists
  - membership/conference registration
  - submission/review for conferences
  - CryptoDB, archive
- Machine upgrade needed

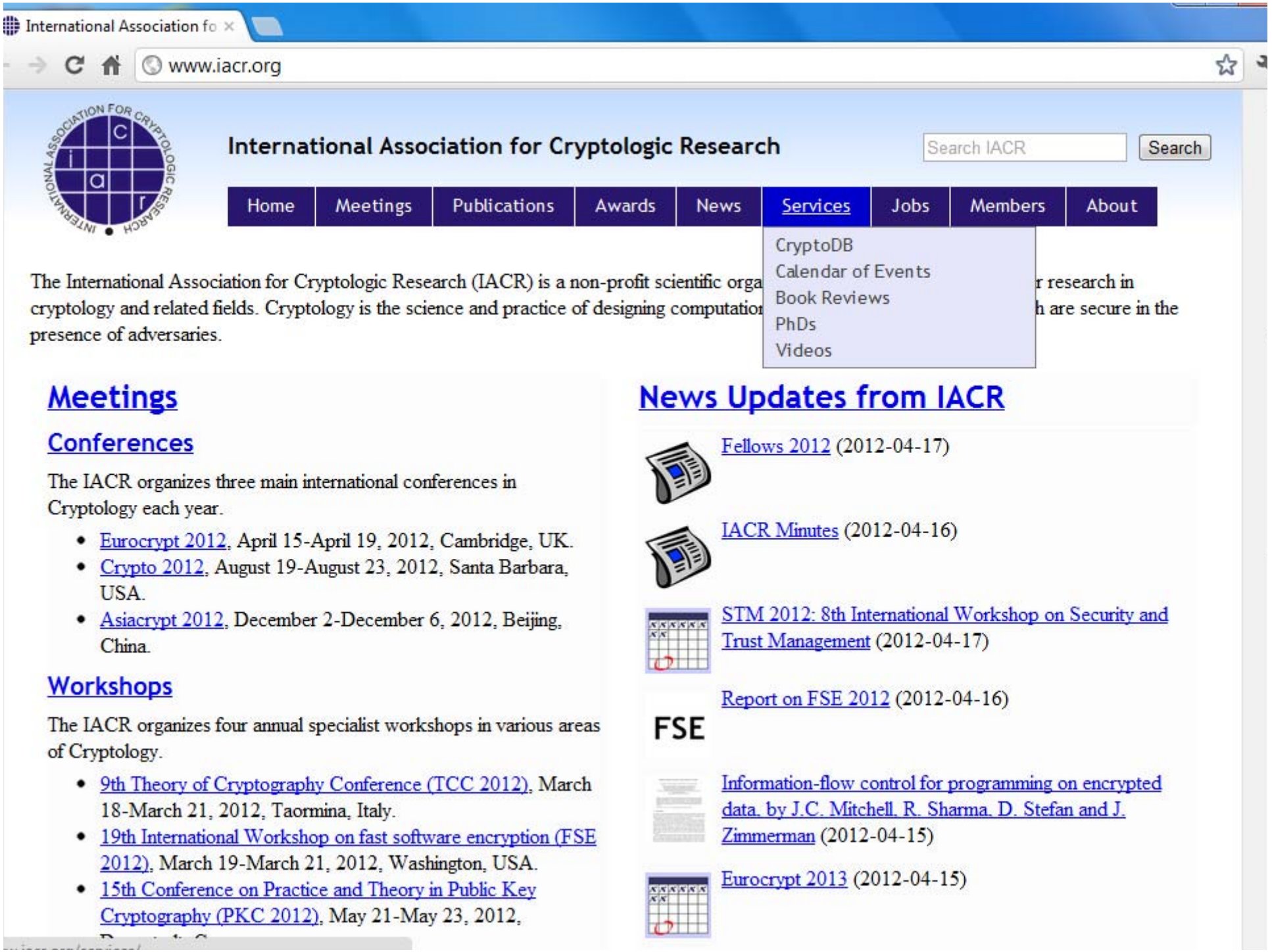
Website update 2012

Kevin McCurley

Christian Cachin

Nigel Smart

Christopher Wolf


International Association fo
www.iacr.org
International Association for Cryptologic Research
Search IACR
Search
Home
Meetings
Publications
Awards
News
Services
Jobs
Members
About
CryptoDB
Calendar of Events
Book Reviews
PhDs
Videos
The International Association for Cryptologic Research (IACR) is a non-profit scientific orga
r research in
cryptology and related fields. Cryptology is the science and practice of designing computatio
h are secure in the
presence of adversaries.
Meetings
Conferences
The IACR organizes three main international conferences in Cryptology each year.
Eurocrypt 2012, April 15-April 19, 2012, Cambridge, UK.
Crypto 2012, August 19-August 23, 2012, Santa Barbara, USA.
Asiacrypt 2012, December 2-December 6, 2012, Beijing, China.
Workshops
The IACR organizes four annual specialist workshops in various areas of Cryptology.
9th Theory of Cryptography Conference (TCC 2012), March 18-March 21, 2012, Taormina, Italy.
19th International Workshop on fast software encryption (FSE 2012), March 19-March 21, 2012, Washington, USA.
15th Conference on Practice and Theory in Public Key Cryptography (PKC 2012), May 21-May 23, 2012,
News Updates from IACR
Fellows 2012 (2012-04-17)
IACR Minutes (2012-04-16)
STM 2012: 8th International Workshop on Security and Trust Management (2012-04-17)
Report on FSE 2012 (2012-04-16)
FSE
Information-flow control for programming on encrypted data, by J.C. Mitchell, R. Sharma, D. Stefan and J. Zimmerman (2012-04-15)
Eurocrypt 2013 (2012-04-15)

Conferences & Workshops

Eurocrypt 2012 – Cambridge, UK

- General chair: Nigel Smart
- Program co-chairs:
  - David Pointcheval
  - Thomas Johansson

2012-2013 Conferences

- Crypto'12: 19-23 Aug., UCSB, Santa Barbara, USA
  - Yiqun Lisa Yin/Rei Safavi-Naini + Ran Canetti
- Asiacrypt'12: 2-6 Dec., Beijing, China
  - Xuejia Lai/Xiaoyun Wang + Kazue Sako
  - **IACR Distinguished Lecture: Dan Boneh**
- Eurocrypt'13: 26-30 May, Athens, Greece
  - Aggelos Kiayias/Thomas Johansson + Phong Nguyen
  - **IACR Distinguished Lecture: Eli Biham**
- Crypto'13: 18-22 Aug., UCSB, Santa Barbara, USA
  - Helena Handschuh/Ran Canetti + Juan Garay
- Asiacrypt'13: 1-5 Dec., Bangalore, India
  - Satyanarayana V. Lokam/Kazue Sako + Palash Sarkar

2014 Conferences

- Eurocrypt: 4-8 May, Copenhagen, Denmark
  - Lars R. Knudsen + Gregor Leander/Phong Nguyen + NN
- Crypto: *17-21 Aug* (tbc), UCSB, Santa Barbara
  - **IACR Distinguished Lecture: tbc**
- Asiacrypt: *7-11 Dec* (tbc), Kaohsiung, Taiwan
  - D. J. Guan/Palash Sarkar + NN

2012-2013 Workshops

- PKC'12: 21-23 May, Darmstadt, Germany
  - Johannes Buchmann + Mark Manulis/Marc Fischlin
- CHES'12: 9-12 Sept, Leuven, Belgium
  - Lejla Batina + Ingrid Verbauwhede/Emmanuel Prouff + Patrick Schaumont
- PKC'13, 27 Feb–1 March, Nara, Japan
  - Goichiro Hanaoka/Kaoru Kurosawa
- TCC'13: 3-6 March, Tokyo, Japan
  - Masayuki Abe + Tatsuaki Okamoto/Amit Sahai
- FSE'13: 10-13 March, Singapore
  - Jian Guo + Thomas Peyrin/Shiho Moriai
- CHES'13: 9-12 Aug, UCSB
  - Thomas Eisenbarth + Çetin Koç/Guido Bertoni + Jean-Sébastien Coron

Conferences and Workshops

- Now hearing proposals for 2015 conferences and 2014 workshops
- Details on how to submit a proposal on www.iacr.org
- Or see a member of the Board/Steering Committee

In particular: candidates for Crypto general chair

Journal of Cryptology

Editor in Chief – Matt Franklin
franklinHEREATcs.ucdavis.edu

Journal of Cryptology

- The premier Journal in cryptology
  - published by Springer-Verlag
  - available in reading room and via postal mail to IACR members (unless you opt-out)
- Overall health very good
- Submission pipeline steady and sustainable
- Send me your ideas for new special issues
  - practical topics especially welcome

IACR Newsletter

Editor – Christopher Wolf
newsletterHEREATiacr.org

IACR Newsletter/Website

- available on http://www.iacr.org/newsletter
- contents
  - calendar of events
  - job opportunities
  - publication announcements
  - book reviews
  - **PhD database**
- via web but also
  - **twitter (http://twitter.com/#!/iacr_news)**
  - **RSS**
  - **email subscription**

- Submit to newsletterHEREATiacr.org

IACR Fellows

Current IACR Fellows

- Tom Berson
- G. Robert Jr. Blakley
- Gilles Brassard
- David Chaum
- Andrew Clark
- Don Coppersmith
- Ivan Damgård
- Yvo Desmedt
- Whitfield Diffie
- Oded Goldreich
- Shafi Goldwasser
- Martin Hellman
- Hideki Imai
- David Kahn
- Arjen K. Lenstra
- James L. Massey
- Ueli Maurer
- Kevin McCurley
- Ralph Merkle
- Silvio Micali
- Moni Naor
- Jean-Jacques Quisquater
- Michael O. Rabin
- Charles Rackoff
- Ron Rivest
- Richard Schroeppel
- Adi Shamir
- Gustavus (Gus) Simmons
- Jacques Stern
- Scott Vanstone
- Andrew Yao

New IACR Fellows in 2012

- Mihir Bellare
- Eli Biham
- Manuel Blum
- Andrew Odlyzko
- Phil Rogaway
- Claus Schnorr
- Jennifer Seberry

Procedures

- Candidates, nominators, and endorsers must be IACR members. Verify membership by corresponding with iacrmemHEREATiacr.org
- Deadline: December 31, 2012
- Instructions: http://www.iacr.org/fellows/
- Submit to fellowsHEREATiacr.org
- Selection-committee members (to be updated):
  - Arjen Lenstra (chair), Ueli Maurer, Kevin McCurley, Ron Rivest, Phil Rogaway

Publications

Springer-Verlag

- Publisher of IACR's conference and workshop proceedings in the LNCS series and the Journal of Cryptology
- IACR reading room: all IACR Members have FREE electronic access to ALL past proceedings of our conferences & workshops and to J. Cryptology

- **http://springer.com/iacr**
- Access token: **http://www.iacr.org**

The IACR Reading Room at Springer

Springer
the language of science

Springer is pleased to offer all IACR members free access to the Journal of Cryptology and to the Lecture Notes in Computer Science proceedings volumes in CRYPTO, EUROCRYPT, ASIACRYPT, FSE, CHES, PKC, and TCC. Access is provided via http://www.springer.com/iacr after a one-time registration procedure as described below.

One-Time Registration

You must be a member of the IACR in order to use the registration procedure below. If you are not currently a member, you should (re)establish your IACR membership and then come back to this page.

Step 1: Get a Springer-token.

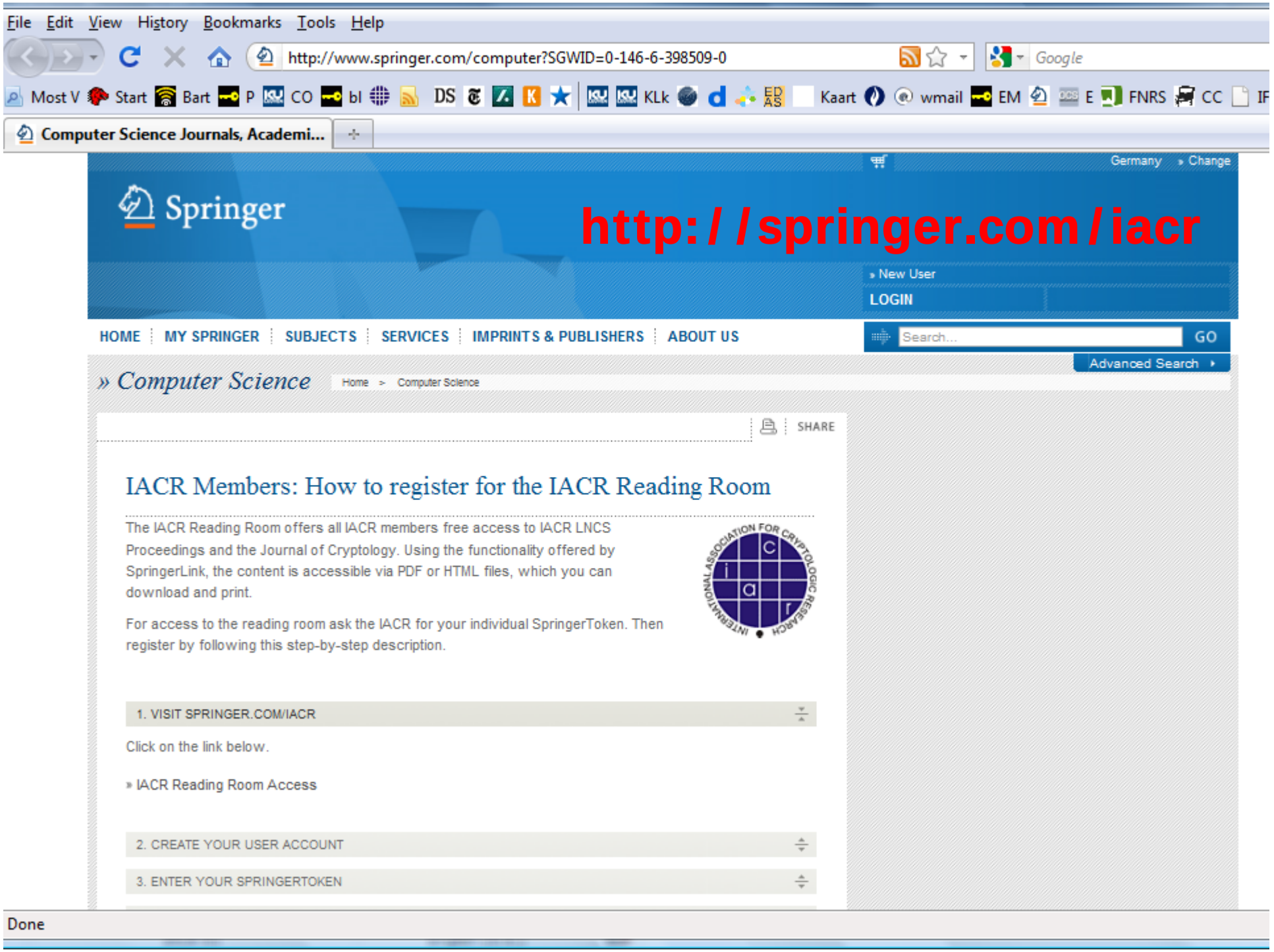
If you know your IACR Reference Number and password, use them in the form below to get a springer token.
IACR Reference Number: [ ] Password: [ ] Get a Springer Token

If you do not remember your IACR Reference Number or password, enter your email address here and we will email them to you:
[ ] Send me my IACR account details

If you are unsure of what email address to use (or have any other problem with this procedure), you can write to the database administrator at the address **database@iacr.org** .

Step 2: Register with Springer.

Once you have a token, go to http://www.springer.com/iacr, and either login to your existing Springer account (if you have one) or register for a new account. Either way, you will be asked to provide the token that you got in Step 1. See more detailed instructions.


File Edit View History Bookmarks Tools Help
http://www.springer.com/computer?SGWID=0-146-6-398509-0
Google
Computer Science Journals, Academi...
Springer
http://springer.com/iacr
Germany » Change
» New User
LOGIN
HOME | MY SPRINGER | SUBJECTS | SERVICES | IMPRINTS & PUBLISHERS | ABOUT US
Search...
GO
Advanced Search
» Computer Science
Home > Computer Science
SHARE
IACR Members: How to register for the IACR Reading Room
The IACR Reading Room offers all IACR members free access to IACR LNCS Proceedings and the Journal of Cryptology. Using the functionality offered by SpringerLink, the content is accessible via PDF or HTML files, which you can download and print.
For access to the reading room ask the IACR for your individual SpringerToken. Then register by following this step-by-step description.
1. VISIT SPRINGER.COM/IACR
Click on the link below.
» IACR Reading Room Access
2. CREATE YOUR USER ACCOUNT
3. ENTER YOUR SPRINGERTOKEN
Done

IACR Reading Room Journals, Acade...

Springer

Germany › Change

Logged in as: bpreneel

LOGOUT

HOME | MY SPRINGER | SUBJECTS | SERVICES | IMPRINTS & PUBLISHERS | ABOUT US

Search... GO

Advanced Search

» IACR Reading Room

Home › Computer Science › IACR Reading Room

SUBDISCIPLINES | JOURNALS | BOOKS | SERIES | TEXTBOOKS

Welcome to the IACR Reading Room

Your personal gateway to society related content

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

To access the free electronic library click on the link of your choice. This will lead you to SpringerLink, our content platform. Enjoy your read!

Free Content!

Journal of Cryptology

Access the e-version of Journal of Cryptology, including the historical archive and online first articles.

Read this journal

Advances in Cryptology - CRYPTO

Read these volumes:

- CRYPTO 2010
- CRYPTO 2009
- CRYPTO 2008
- CRYPTO 2007

FIND ALL OUR SERVICES

- For Authors
- For Instructors
- For Booksellers
- For Librarians

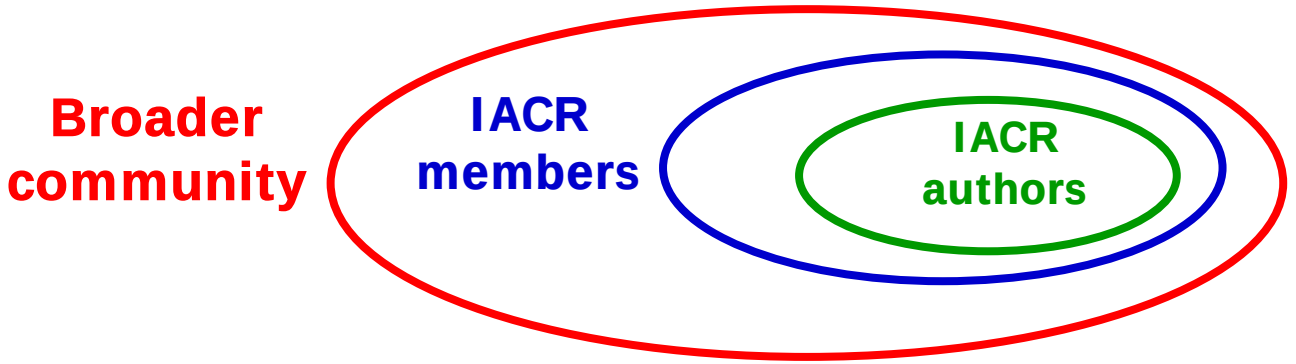
IACR Publications

- springer.com/iacr access to IACR members in IACR reading room after conference + JoC
- iacr.org/archive open access of author version of conference proceedings after 2 years
  - currently Eurocrypt 2000 - Asiacrypt 2009
  - formatting is slightly different: pagination and references (but text is the same)
  - managed by Hilarie Orman (IACR archivist)

Current Board Activities

E-publishing goals

- Distribution and archival
- Scientific credit
  - competitive review or multi-round in-depth review
  - formal publisher
  - indexing/citations in ISI (LNCS was removed in 2004), Google Scholar, Microsoft Academic Search, Scopus, DBLP,...
  - download count (single source)



Current Board Activities: e-publishing

Opt-In for paper

- Proceedings: currently opt-in
- Journal of Cryptology: currently opt-out
  - plan to switch to opt-in 1-2 years (40$ cost)

Current Board Activities: e-publishing

Open access for proceedings

- Proceedings papers immediately and freely available for everyone (for both IACR members and IACR non-members)
- Open access is not free: cost for verification, collecting meta-data, enhancing references

- Cost of current non open access model (paper): 100 K$ per year (250 papers)
- Discussions with several publishers and other scientific organizations
- Perfect solution may not be possible

Current Board Activities: e-voting

- Helios: participation up from 20% to 30% (2010) and **41.8%** (2011)

- Switch to approval voting
  - previous: vote for 1, 2, 3 out of n candidates
  - new: vote for 1, 2, 3, 4, ..., n-1,n candidates
- Integrity/verifiability could be strengthened if the public audit file would list who has voted (now only a list of pseudonyms)

Current Board Activities

- **Flagship conference**
  - rolling program chairs: (junior and senior) program co-chair
  - increase number of accepted papers (accommodate this with shorter talks, more half-days, longer days, parallel sessions)
- **Ethical guidelines for authors and reviewers**
  - submission to conference and journal in parallel **only** with explicit permission from pc chair and journal editor
  - http://www.iacr.org/docs/
- **Co-location of workshops/conferences to reduce travel overhead (tentative)**
  - FSE/PKC/TCC co-locate with Eurocrypt every 3rd year?
  - CHES co-locate with Crypto every 3rd year
- **Recording of talks – only with presenter's permission**

Open Discussion