IACR Membership Meeting Eurocrypt 2011, Tallinn

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 (’11)

OFFICERS

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

DIRECTORS

- Josh Benaloh
- Tom Berson
- Stuart Haber
- Antoine Joux
- Matsuru Matsui
- David Naccache
- Christof Paar
- David Pointcheval
- Serge Vaudenay

Your Board ('11)

APPOINTEES

- Matt Franklin
- Shai Halevi
- Kevin McCurley
- Hilarie Orman
- Christopher Wolf

GENERAL CHAIRS

- Helger Lipmaa
- Tom Shrimpton
- Hyoung-Joong Kim
- Nigel Smart
- Lisa Yiqun Lin
- Xuejia Lai

STEERING COMMITTEE REPRESENTATIVES

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

Thanks to ex-Officers

- Ed Dawson
- Tom Shrimpton (Crypto’11 general chair)
- Helena Handschuh

Membership

- By attending this conference, you will become a member of IACR for 2012
- If you attended one of our conferences or workshops last year, you are already a member for 2011

IACR Election

- There is an election for Board members every year in the Fall
  - In 2011 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 2011 Election Committee) if you would like to know more, or are interested in standing for election

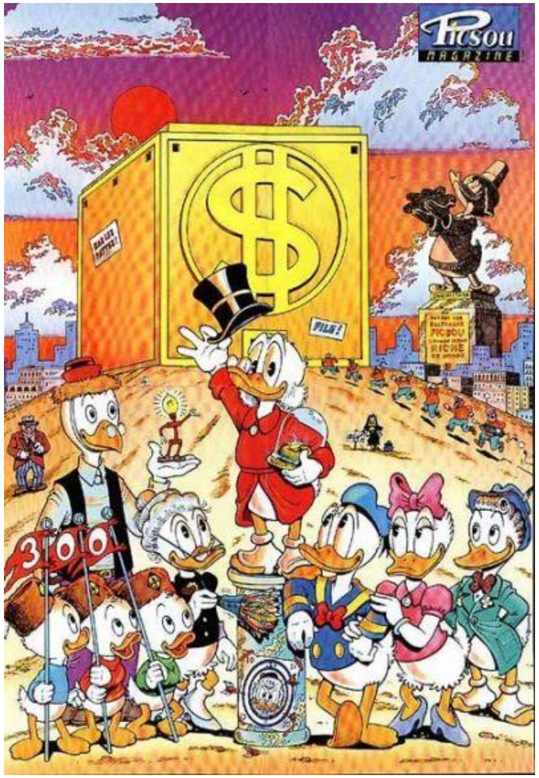
IACR Election Committee 2011

Greg Rose

Martijn Stam

Serge Vaudenay

IACR Financial Report Y2010



Greg Rose

treasurer@iacr.org

Thanks!

To Helena Handschuh

- great work for previous 9 years
- organized handover
- continues to help me

Financial Summary - 2010

- Strong financial support from several sponsoring organisations in spite of economic downturn
- Attendance at our events did really well
  - PKC (171) more than doubled
  - TCC (108),
  - FSE (109) down
  - CHES (338)
  - Crypto (451) up more than 100,
  - Eurocrypt (393)
  - Asiacrypt (246)

2011 Highlights

- Commit to run our events successfully
- Conference registration waivers for student speakers (Marconi grant)
- Other sponsorship
- Target break-even budgets

Questions for the Treasurer

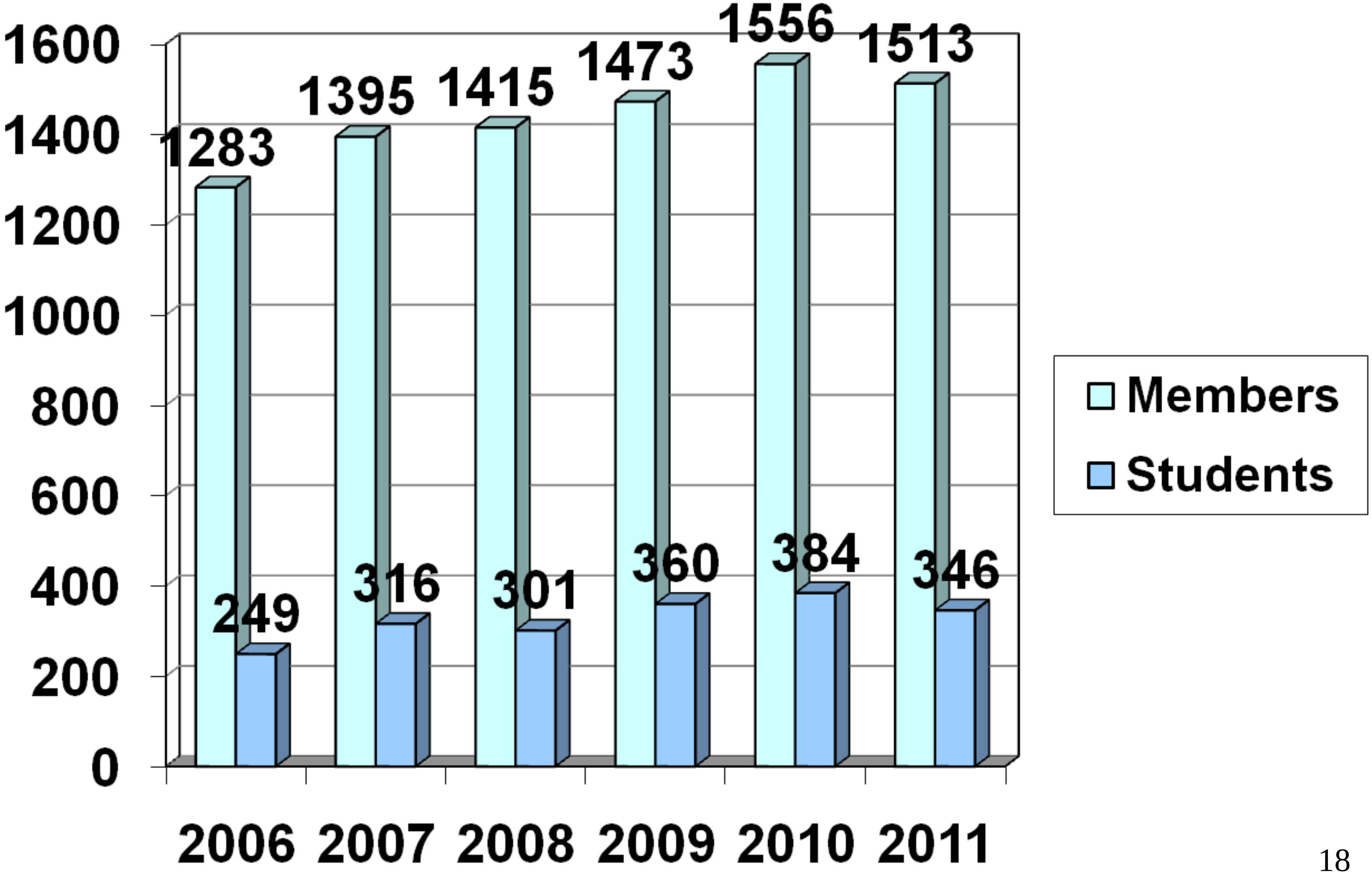
IACR Membership

May 2011

Shai Halevi

iacrmemHEREATiacr.org

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

Planned for 2012-2013

- server upgrade
- software upgrade

Springer Access for Regional Associations

- Implemented a system for CACR members to get tokens for the IACR reading room at Springer
  - Works fine from our side
  - Springer's side under test
- Can be used also for CRSI
  - Waiting for membership list

Chinese Association for Cryptologic Research

Cryptology Research Society of India

Conferences & Workshops

2011 Conferences

- Eurocrypt 2011: 15-19 May, Tallinn, Estonia
  - Helger Lipmaa/Kenny Paterson
- Crypto 2011: 19-23 Aug., UCSB, Santa Barbara
  - Tom Shrimpton/Phil Rogaway
  - **IACR Distinguished Lecture: Ron Rivest**
- Asiacrypt 2011: 4-8 Dec., Seoul, Korea
  - Hyoung-Joong Kim/Dong Hoon Lee+Xiaoyun Wang

2012 Conferences

- Eurocrypt: 15-19 April, Cambridge, UK
  - Nigel Smart
  - David Pointcheval + Thomas Johansson
- Crypto: 19-23 Aug., UCSB, Santa Barbara, USA
  - Lisa Yiqun Lin
  - Rei Safavi-Naini + NN
- Asiacrypt: 2-6 December, Beijing, China
  - Xuejia Lai
  - Xiaoyun Wang + NN
  - **IACR Distinguished Lecture: Dan Boneh**

2013 Conferences

- Eurocrypt: April-May, Athens, Greece
  - Aggelos Kiayias
  - Thomas Johansson + NN
- Crypto: 19-23 Aug., UCSB, Santa Barbara
  - NN
- Asiacrypt: tbd

2011-2012 Workshops

- CHES’11: 28 Sept. – 1 Oct, Nara, Japan
  - Akashi Satoh
  - Bart Preneel + Tsuyoshi Takagi
- PKC’12: 7-9 March, Japan, tbc
- TCC’12: 18-21 March, Taormina, Italy
  - Nelly Fazio + Rosario Gennaro
  - tbd
- FSE’12: Washington DC, USA –March/April 2012
  - co-located with NIST SHA-3 workshop

Conferences and Workshops

- Now hearing proposals for 2014 conferences and 2013 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 this field
  - Published by Springer-Verlag and mailed to all IACR members
- Please submit your best papers for publication
- We have an increased page budget this year and expect to be publishing more papers
- We are seeking to include more papers in Applied Cryptology

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**
- 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
- Arjen K. Lenstra
- James L. Massey
- Ueli Maurer
- Kevin McCurley
- Ralph Merkle
- Silvio Micali
- Moni Naor
- Jean-Jacques Quisquater
- Michael O. Rabin
- Ron Rivest
- Adi Shamir
- Gustavus (Gus) Simmons
- Jacques Stern
- Andy Yao

New IACR Fellows in 2011

- David Kahn
- Charles Rackoff
- Richard Schroeppel
- Scott Vanstone

Procedures

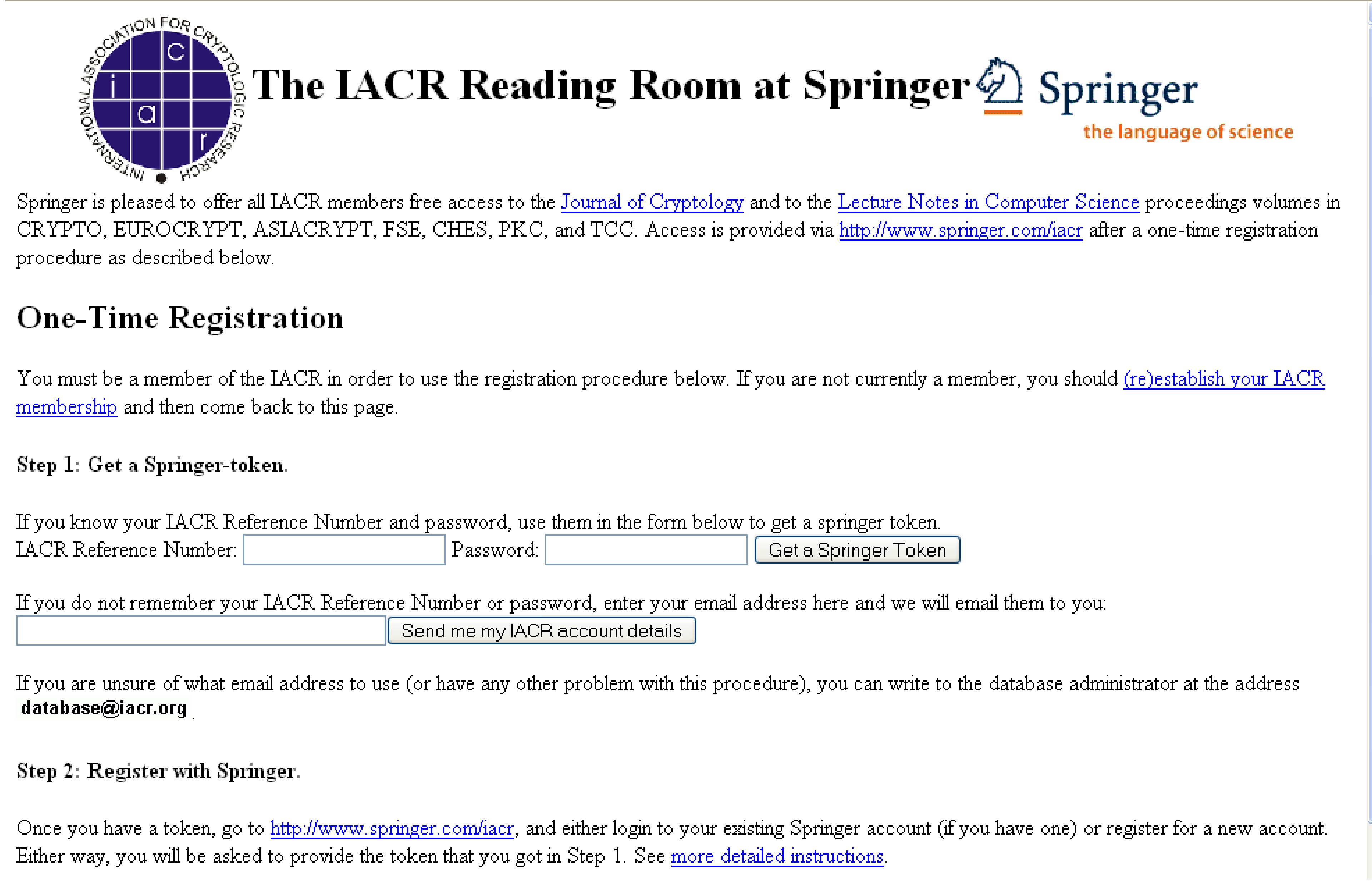
- Candidates, nominators, and endorsers must be IACR members. Verify membership by corresponding with iacrmemHEREATiacr.org
- Deadline: December 31, 2011
- Instructions: http://www.iacr.org/fellows/
- Submit to fellowsHEREATiacr.org
- Selection-committee members (to be updated):
  - Arjen Lenstra, Ueli Maurer, Tatsuaki Okamoto, Ron Rivest (Chair), Moti Yung

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 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.

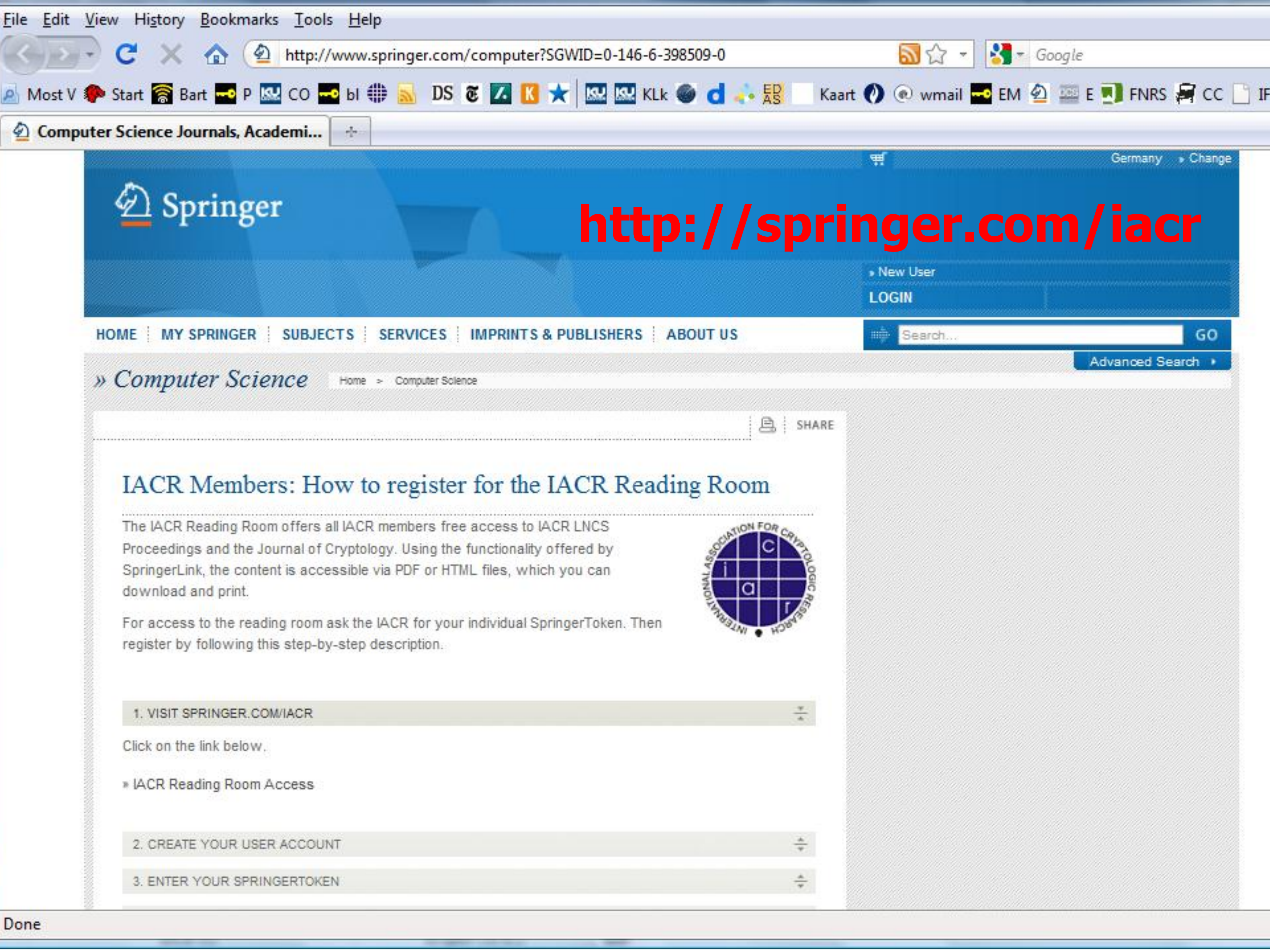
If you know your IACR Reference Number and password, use them in the form below to get a springer token.
IACR Reference Number: Password:

If you do not remember your IACR Reference Number or password, enter your email address here and we will email them to you:

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
Most V Start Bart P CO bl DS KLk Kaart wmail EM E FNRS CC IF
Computer Science Journals, Academi...
Germany
» Change
Springer
» New User
LOGIN
HOME MY SPRINGER SUBJECTS SERVICES IMPRINTS & PUBLISHERS ABOUT US
Search...
GO
Advanced Search
» Computer Science
Home > Computer Science
SHARE
INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
Done

http://springer.com/iacr

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.

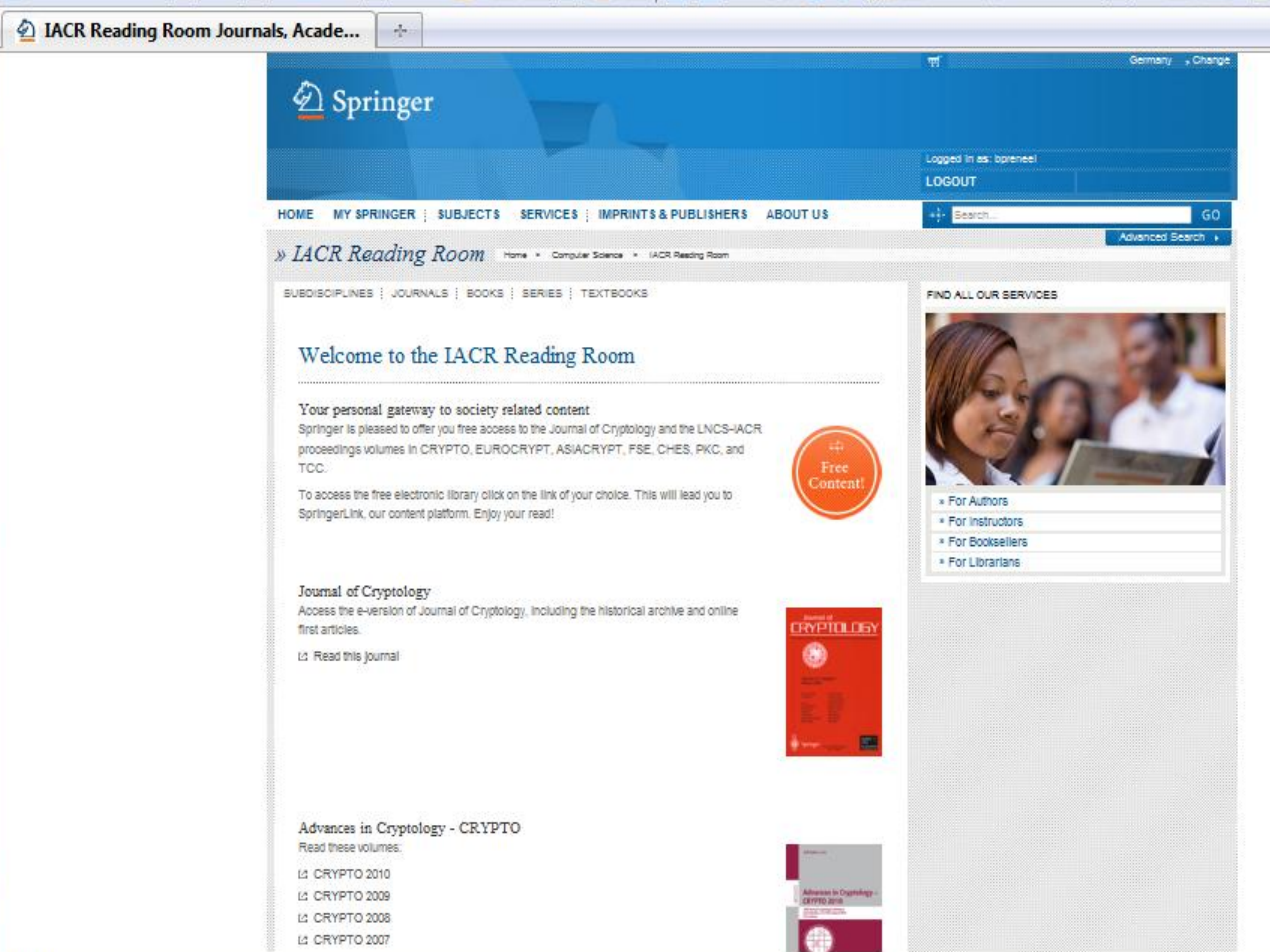
1. VISIT SPRINGER.COM/IACR

Click on the link below.

» IACR Reading Room Access

2. CREATE YOUR USER ACCOUNT

3. ENTER YOUR SPRINGERTOKEN



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!

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

IACR Publications

- Today
  - access to IACR members in IACR reading room at Springer (few weeks-months after conference)
  - open access of conference proceedings after 2 years at http://www.iacr.org/archive
    - currently Eurocrypt 2000- Asiacrypt 2008
    - formatting is slightly different (but exactly the same content)

Current Board Activities

Current Board Activities: e-publishing

- opt out for paper copy of Journal of Cryptology (will result in reduced membership fee in future)
- opt out for paper copy of proceedings – default would be online access or USB stick (reduced registration fee)
- open access with Springer Verlag or with other organization (e.g. Usenix)
- DVD with all IACR publications

Current Board Activities: e-voting

- Helios: participation in 2010 from 20% to 30%

- 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 year)
- Ethical guidelines for authors and reviewers
- Co-location of workshops/conferences to reduce travel overhead (under discussion)
  - FSE/PKC/TCC co-locate with Eurocrypt every 3rd year
  - CHES co-locate with Crypto every 3rd year

Current Board Activities

- Questionnaire for Eurocrypt 2012 college accommodation in Cambridge
  - 70 £ per night (≈ 80 EUR)
  - needs to be pre-booked (not refundable)

Open Discussion