IACR Membership Meeting
Crypto 2010, UCSB

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 Archive
  - 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 ('10)

OFFICERS

- Bart Preneel *
- Ed Dawson *
- Tom Shrimpton *
- Helena Handschuh *

DIRECTORS

- Josh Benaloh
- Tom Berson
- Christian Cachin *
- Stuart Haber
- Antoine Joux
- Tsutomu Matsumoto *
- David Naccache
- David Pointcheval *
- Serge Vaudenay

Your Board ('10)

APPOINTEES

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

GENERAL CHAIRS

- Olivier Billet *
- Zulfikar Ramzan *
- San Ling *
- Helger Lipmaa
- (Tom Shrimpton)
- Hyoung-Joong Kim

STEERING COMMITTEE REPRESENTATIVES

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

Membership

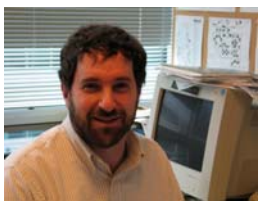
- By attending this conference, you will become a member of IACR for 2011
- If you attended one of our conferences or workshops last year, you are already a member for 2010

IACR Election

- There is an election for Board members every year in the Fall
  - In 2010 the terms of 4 officers and 3 elected Directors expire
  - We are actively seeking interested members to join the Board
  - Please contact any Board member or a member of the Election Committee if you would like to know more, or are interested in standing for election

IACR Election Committee 2010

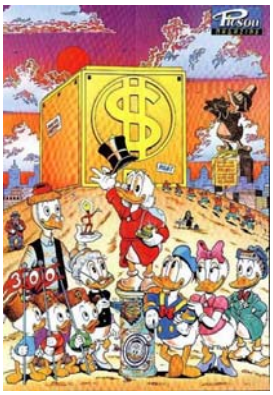
Josh Benaloh
(chair)



Jean-Jacques
Quisquater

Serge Vaudenay
(returning officer)

IACR Financial Report Y2009



Helena Handschuh
treasurer@iacr.org

Financial Summary - 2009

- Not-for-profit organisation; 501(c)(3) status since 1987
- Strong financial support from several sponsoring organisations throughout the year
- Attendance at our events did really well
  - PKC(76), TCC(108),
  - FSE(220), CHES(312)
  - Crypto (353),
  - Eurocrypt, (438), Asiacrypt (303)
- The euro has been fluctuating a lot again. 1.5 to 1.25 dollars per euro
- IACR levels out these currency fluctuations
- Extremely low administration overhead : < 2%
- ***Strong financial position for IACR***

2010 Highlights

- Commit to run our events **successfully** despite economic downturn
- Target **break-even** budgets (not for profit)
- Keep minimal overhead - less than 2%

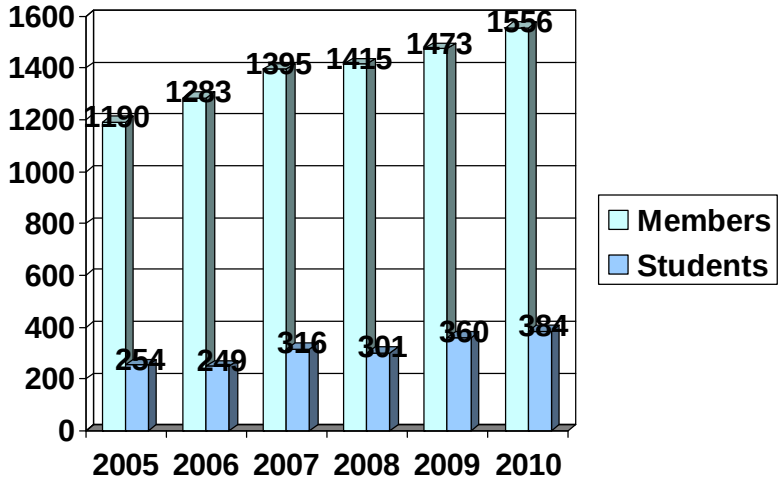
- Marconi grant allocated to
  - IACR Conference registration fee waivers for **student speakers**
- Reduced membership fee for 2012 (starting at FSE2011).
  - **$88/44 reduced to $70/35**

IACR Membership

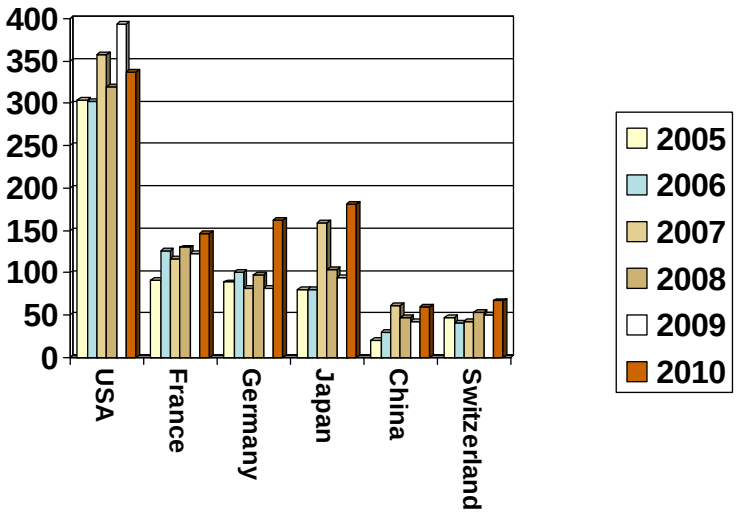
Summer 2010

Shai Halevi
iacrmemHEREATiacr.org

Total Membership



By Country



On-Line services

- Same as last few years
  - Membership/Conference registration
  - Submission/Review for conferences
  - ePrint
  - CryptoDB
  - Mailing lists
- All on the same server

Minor changes to membership/confreg systems

- New address format for sending the journal
  - At Springer's request
- Better handling of fraudulent registrations
- Dealing with VAT, currency issues
  - More details needed on receipts
- Multi-event discount for CRYPTO/CHES '10
- ...

"PCI Compliance"

- Becoming a little more work now
  - Need to make small changes to our system
  - Must fill out a compliance questionnaire annually
- Still doable on volunteer time
  - But the trend is toward more work
  - Eventually may need to pay someone to do it

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
  - Flaky from Springer's side
    - Not clear why, hopefully it will be fixed
- Can be used also for CRSI
  - If they ever get back to me

Chinese Association for Cryptologic Research

Cryptology Research Society of India

Conferences & Workshops

2012 Conferences

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

2010-2011 Conferences

- Asiacrypt 2010: 5-9 Dec., Singapore
  - Ling San/Masayuki Abe
- Eurocrypt 2011: 15-19 May, Tallinn, Estonia
  - Helger Lipmaa/Kenny Paterson+David Pointcheval
- Crypto 2011: 14-18 Aug., UCSB, Santa Barbara
  - Tom Shrimpton/Phil Rogaway+Rei Safavi-Naini
  - **IACR Distinguished Lecture: Ron Rivest**
- Asiacrypt 2011: 4-8 Dec., Seoul, Korea
  - Hyoung-Joong Kim/Dong Hoon Lee+Xiaoyun Wang

2011 Workshops

- FSE: 14-16 Feb., Lyngby, Denmark
  - Lars Knudsen+Gregor Leander/Antoine Joux
- PKC: 6-9 March, Taormina, Italy
  - Nelly Fazio+Antonio Nicolosi/Rosario Gennaro
- TCC: 27-30 March, Providence, RI, USA
  - Anna Lysyanskaya/Yuval Ishai
- CHES: 26-29 Sept., Tokyo, Japan
  - Akashi Satoh/Bart Preneel + Tsuyoshi Takagi

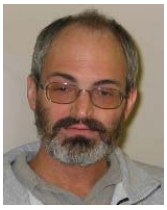
Conferences and Workshops

- Now hearing proposals for 2013 conferences and 2012 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
- Expansion planned: PhD thesis,...
- Submit to newsletterHEREATiacr.org

IACR Fellows

Current IACR Fellows

- Tom Berson
- G. Robert Jr. Blakley
- Gilles Brassard
- David Chaum
- Don Coppersmith
- 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
- Michael O. Rabin
- Ron Rivest
- Adi Shamir
- Gustavus (Gus) Simmons
- Jacques Stern

New IACR Fellows in 2010

- Andrew Clark
- Ivan Damgård
- Yvo Desmedt
- Jean-Jacques Quisquater
- Andrew Yao

Procedures

- Candidates, nominators, and endorsers must be IACR members. Verify membership by corresponding with iacrmemHEREATiacr.org
- Deadline: December 31, 2010
- Instructions: http://www.iacr.org/fellows/
- Submit to fellowsHEREATiacr.org
- Selection-committee members:
  - 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 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]

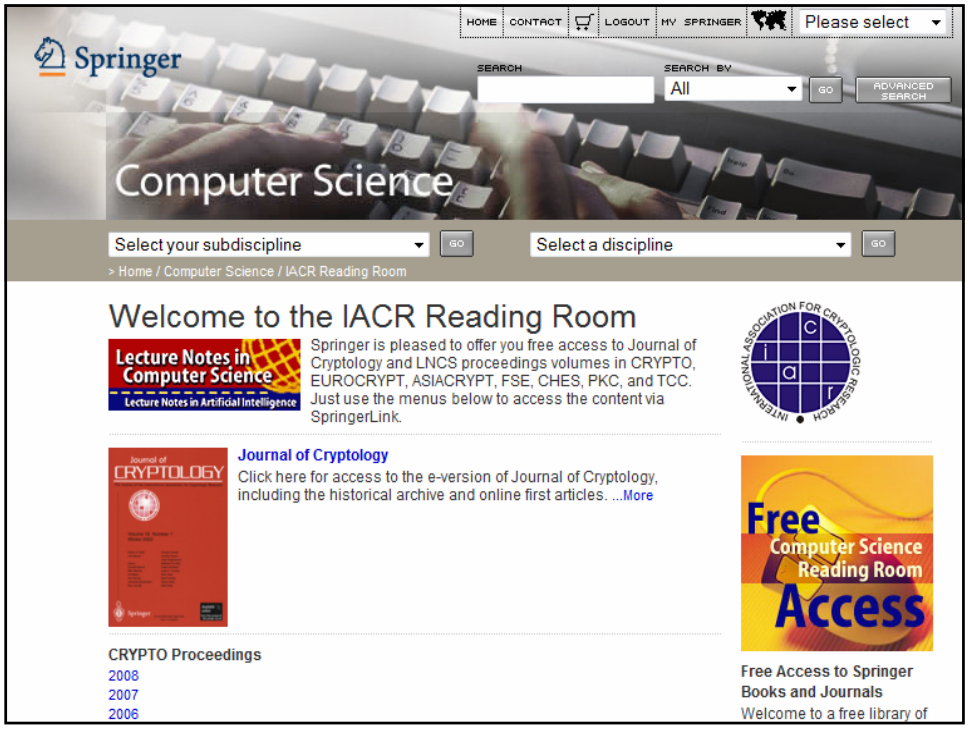
If you do not remember your IACR Reference Number or password, enter your email address here and we will email them to you:
[ ] [Send me my IACR account details]

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.


HOME HELP LOGIN MY SPRINGER Please select
Springer
SEARCH
SEARCH BY
All
GO
ADVANCED SEARCH
Registration
Select a discipline
> Home
Are you already a springer.com user?
If you would like to access this restricted area, please log in first. To benefit from this exclusive offer, you will have to enter your SpringerToken for: IACR Reading Room.
Please log in with your existing user name/email address and password. Be aware that the password is case sensitive and must not contain any spaces.
User name / Email address
Password (5-10 characters)
Forgot your password? Forgot your user name?
SUBMIT
Are you new to springer.com?
If you want to sign in, you'll need to register first. Registration is fast and free.
CONTINUE
Changing Account Data
Click here to find out how to change your e-mail address, password, user name, personal profile or method of payment. ...More!
Both User Name AND Password Forgotten?
If you have forgotten both your user name AND your password, please click here. ...More!
SpringerAlerts
Be the first to know: Register here for the Springer e-mail newsletter providing you with customized information on the latest books in your field. ...More!
http://springer.com/iacr


HOME CONTACT LOGOUT MY SPRINGER Please select
Springer
SEARCH
SEARCH BY
All
GO
ADVANCED SEARCH
Computer Science
Select your subdiscipline
Select a discipline
> Home / Computer Science / IACR Reading Room
Welcome to the IACR Reading Room
Lecture Notes in Computer Science
Lecture Notes in Artificial Intelligence
Springer is pleased to offer you free access to Journal of Cryptology and LNCS proceedings volumes in CRYPTO, EUROCRYPT, ASIACRYPT, FSE, CHES, PKC, and TCC. Just use the menus below to access the content via SpringerLink.
Journal of Cryptology
Click here for access to the e-version of Journal of Cryptology, including the historical archive and online first articles. ...More
CRYPTO Proceedings
2008
2007
2006
Free Computer Science Reading Room Access
Free Access to Springer Books and Journals
Welcome to a free library of

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-PKC 2008
    - formatting is slightly different (but exactly the same content)
- Future options (under consideration)
  - paper version optional
  - open access with Springer Verlag or with other organization (e.g. Usenix)

Current Board Activities

Current Board Activities: E-voting for IACR

- 2008: call for remote voting systems with presentations at Crypto
- 2008: modification of IACR Bylaws to allow for electronic voting (after approval by Membership)
- 2009: after evaluation Helios and Punchscan were invited to present to the Board and to organize a demo election
- Winter 2010: demo election with Helios
  - 379 cast votes, out of the 1542 eligible voters
- Summer 2010: issues identified during demo resolved
- Thanks to
  - Ben Adida, Olivier de Marneffe, Olivier Pereira
  - Yvo Desmedt
  - Josh Benaloh, Stuart Haber, Shai Halevi

Current Board Activities: E-voting for IACR

The Board recommends that the IACR membership approve the following:

- The IACR adopts the Helios remote e-voting system for future IACR elections (including 2010). At the same time, the IACR clearly publishes a statement that its use of this system does not constitute an endorsement of this or other remote-voting systems for public-sector elections.

Current Board Activities

- Flagship conference: rolling program chairs (junior and senior year) from 2011 onwards
- Towards open access publications
  - Offer on-line publications to a broader community
- Co-location of workshops/conferences to reduce travel overhead
- Ethical guidelines for authors and reviewers

Open Discussion