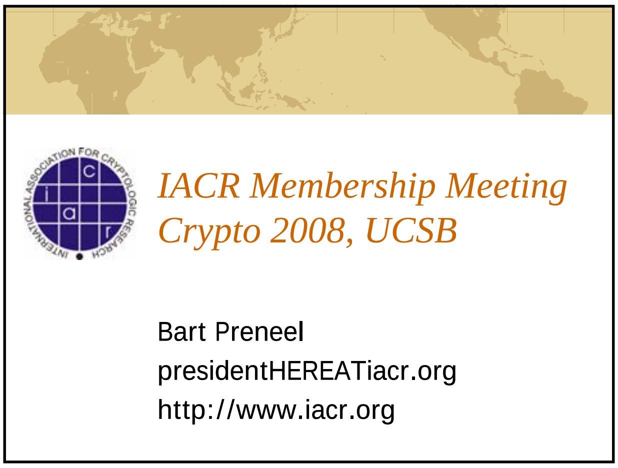
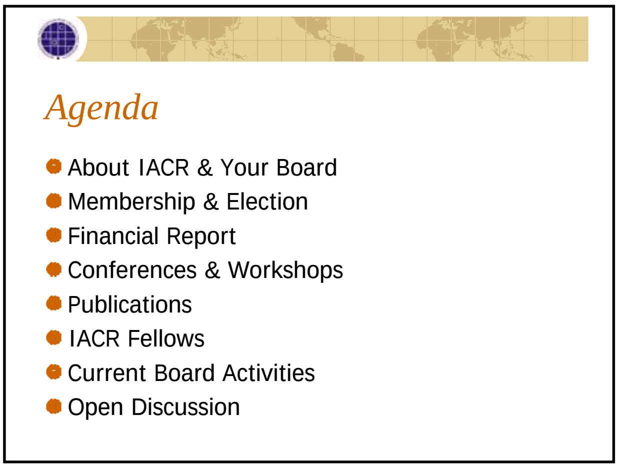


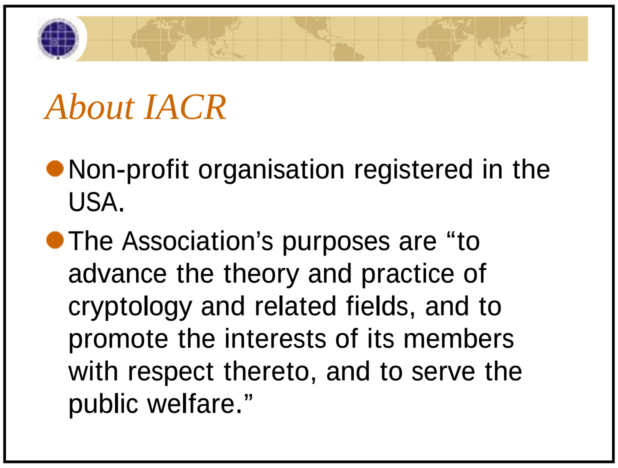
IACR Membership Meeting Crypto 2008, UCSB

Bart Preneel
presidentHEREATiacr.org
http://www.iacr.org



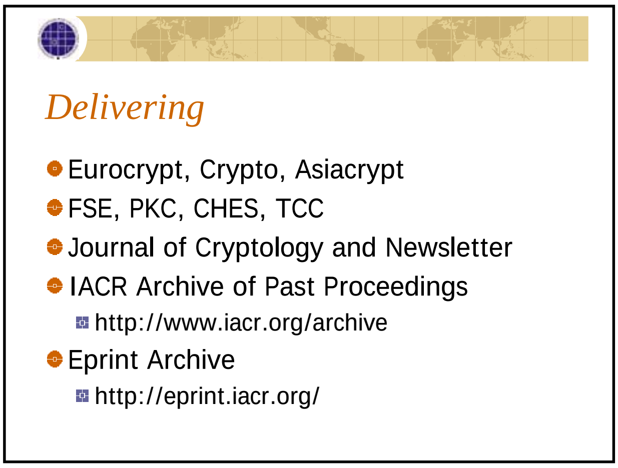
Agenda

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



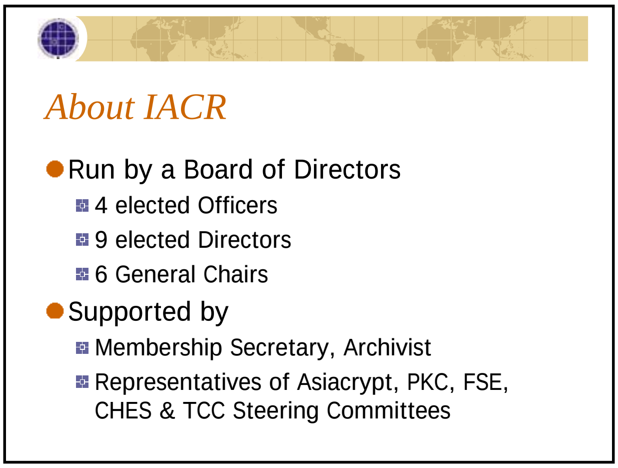
About IACR

- 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."



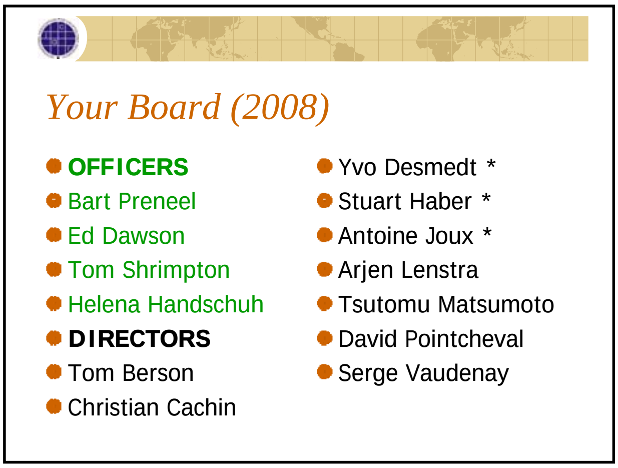
Delivering

- 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
  - Membership Secretary, Archivist
  - Representatives of Asiacrypt, PKC, FSE, CHES & TCC Steering Committees



Your Board (2008)

- **OFFICERS**
- Bart Preneel
- Ed Dawson
- Tom Shrimpton
- Helena Handschuh
- **DIRECTORS**
- Tom Berson
- Christian Cachin
- Yvo Desmedt *
- Stuart Haber *
- Antoine Joux *
- Arjen Lenstra
- Tsutomu Matsumoto
- David Pointcheval
- Serge Vaudenay

Your Board (2008)

- **APPOINTEES**
- Shai Halevi
- James Hughes
- Ueli Maurer

- **GENERAL CHAIRS**
- Murat Apohan *
- Susan Langford *
- Lynn Batten *
- Alexander May
- John Black
- Eiji Okamoto

Membership

- By attending this conference, you will become a member of IACR for 2009
- If you attended one of our conferences or workshops last year, you are already a member for 2008

IACR Election

- There is an election for Board members every year in the Fall
  - 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

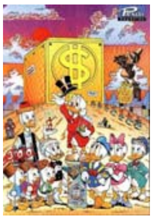
IACR Election Committee

Christian Cachin
(returning officer)

Jim Hughes
(chair)

David Pointcheval

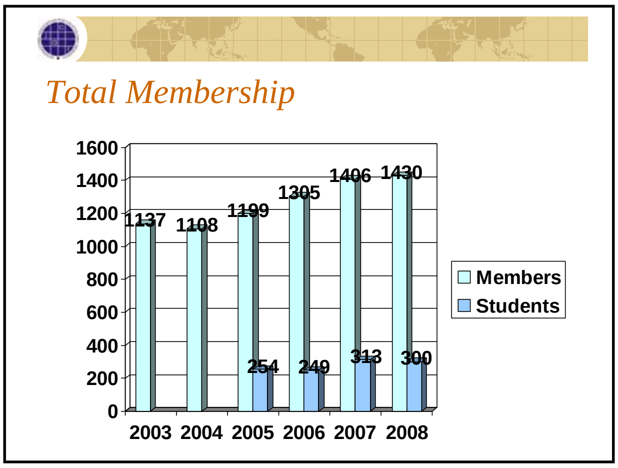
IACR Financial Report Y2007



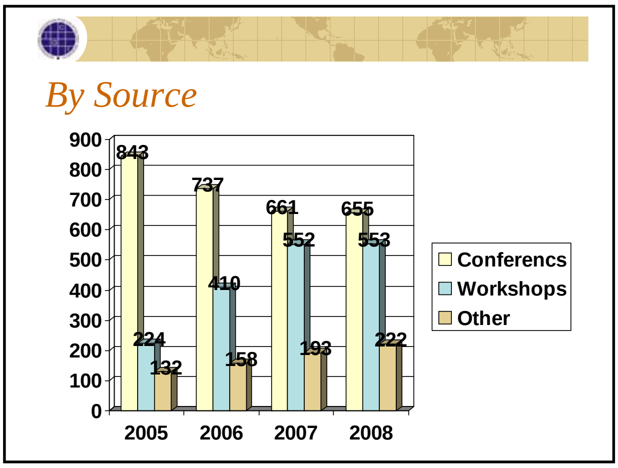
Helena Handschuh
treasurerHEREATiacr.org

IACR Membership Secretary

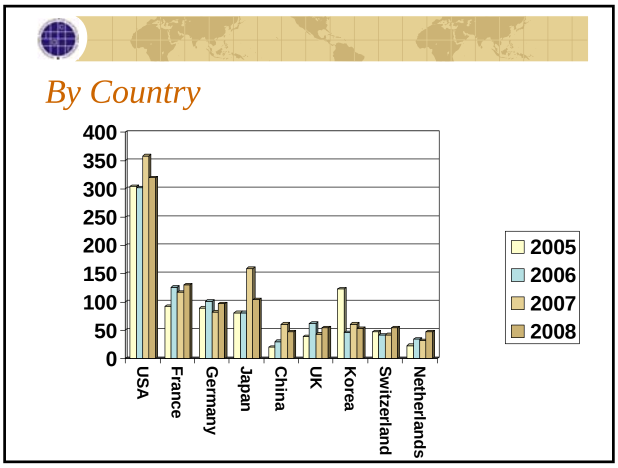
Shai Halevi
iacrmemHEREATiacr.org



Total Membership

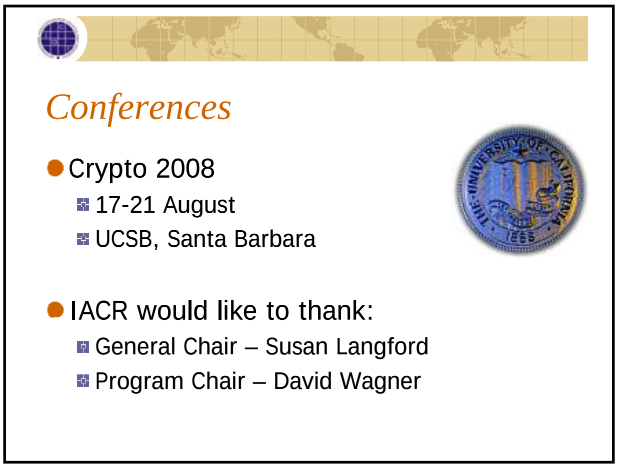


By Source



By Country

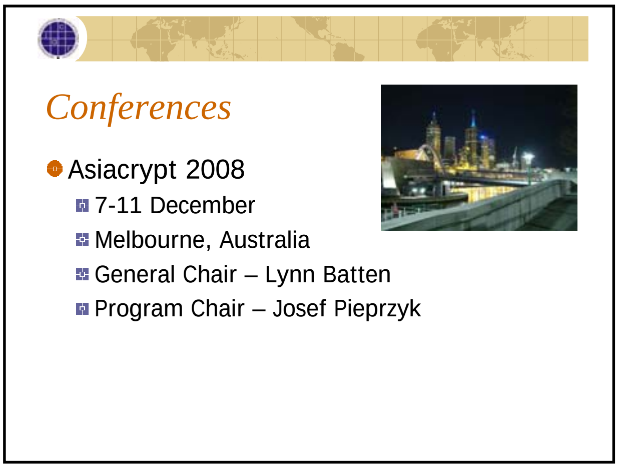
Conferences & Workshops



Conferences

- Crypto 2008
  - 17-21 August
  - UCSB, Santa Barbara
- IACR would like to thank:
  - General Chair – Susan Langford
  - Program Chair – David Wagner

THE UNIVERSITY OF CALIFORNIA
1868



Conferences

- Asiacrypt 2008
  - 7-11 December
  - Melbourne, Australia
  - General Chair – Lynn Batten
  - Program Chair – Josef Pieprzyk

Conferences

- Eurocrypt 2009
  - 26-30 April
  - Cologne (Köln), Germany
  - General Chair – Alexander May
  - Program Chair – Antoine Joux

Conferences

- Crypto 2009
  - 16-20 August
  - UCSB, Santa Barbara
  - General Chair – John Black
  - Program Chair – Shai Halevi

Conferences

- Asiacrypt 2009
  - 6-10 December
  - Tokyo, Japan
  - General Chair – Eiji Okamoto
  - Program Chair – Mitsuru Matsui
  - Distinguished Lecture – Tatsuaki Okamoto

Conferences

- Eurocrypt 2010
  - 30 May – 3 June
  - Nice, France
  - General Co-Chairs – Olivier Billet and Matt Robshaw
  - Program Chair – tbc
  - Distinguished Lecture – Moti Yung

Conferences

- Crypto 2010
  - 15-19 August
  - UCSB, Santa Barbara
  - General Chair – Zulfikar Ramzan
  - Program Chair – Tal Rabin
  - (Tentative: CHES 2010 at UCSB from 18-20 August)

Conferences

- Asiacrypt 2010
  - 5-9 December
  - Singapore, Marine Bay Sands
  - General Chair – Ling San
  - Program Chair – Masayuki Abe

Workshops

- FSE 2009
  - 22-25 February
  - Leuven, Belgium
  - General Chair – Bart Preneel
  - Program Chair – Orr Dunkelman

Workshops

- TCC 2009
  - 15-17 March
  - San Francisco, USA
  - General Chair – Dan Boneh
  - Program Chair – Omer Reingold

Workshops

- PKC 2009
  - 18-20 March
  - Irvine, California
  - General Chair – Stanislaw Jarecki
  - Program Co-Chairs – Gene Tsudik and Stanislaw Jarecki

Workshops

- CHES 2009
  - 6-9 September
  - Lausanne, Switzerland
  - General Chair – Marcelo Kaihara
  - Program Chairs – Christophe Clavier and Kris Gaj

Conferences and Workshops

- Now hearing proposals for 2011 conferences and 2010 workshops
- Details on how to submit a proposal on www.iacr.org
- Or see a member of the Board

Journal of Cryptology

Editor in Chief – Ueli Maurer
maurerHEREATinf.ethz.ch

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

Journal of Cryptology

- Matt Franklin, U.C. Davis has been appointed as next Editor in Chief

IACR Newsletter

Editor – Jim Hughes

newsletterHEREATiacr.org

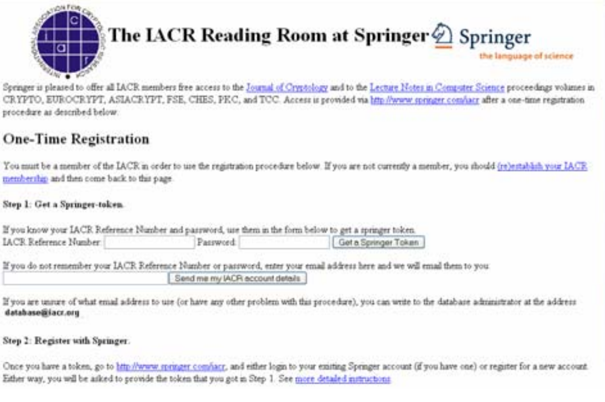
IACR Newsletter/Website

- Available on http://www.iacr.org/newsletter
- Contents
  - Calendar of events
  - Job opportunities
  - Publication announcements etc.
- Submit to newsletterHEREATiacr.org

Springer Online 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: **https://secure.iacr.org/membership/members/springer.html**



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:

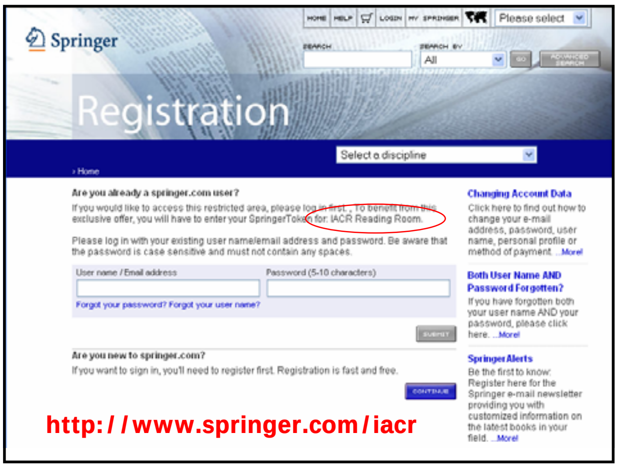
If you do not remember your IACR Reference Number or password, enter your email address here and we will email them to you:

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

https://secure.iacr.org/membership/members/springer.html



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)

Are you new to springer.com?

If you want to sign in, you'll need to register first. Registration is fast and free.

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!

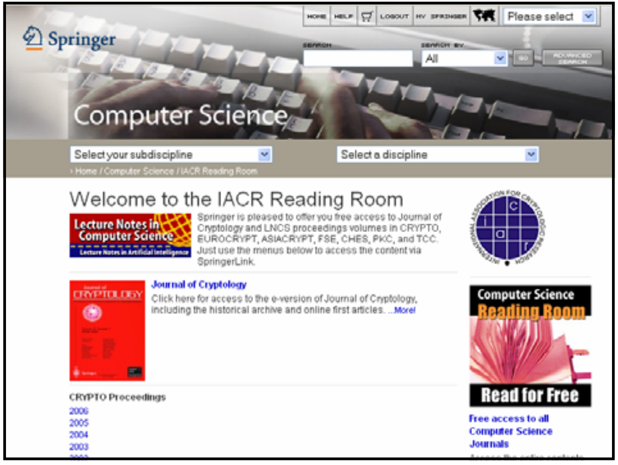
Both User Name AND Password Forgotten?

If you have forgotten both your user name AND your password, please click here. ...More!

Springer Alerts

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://www.springer.com/iacr



Springer
HOME
HELP
LOGOUT
MY SPRINGER
Please select
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
2006
2005
2004
2003

Free access to all Computer Science Journals

IACR statement on its conference publications in Lecture Notes in Computer Science

[...]

Until 2006, LNCS was included in Thomson's ISI (International Science Citation Index); however, Thomson has recently decided to move LNCS from ISI to ISI Proceedings. This implies a.o. that LNCS no longer receives an impact factor and that citations to and from LNCS articles are no longer counted the same way as before. Unfortunately, for some funding agencies this implies that the status of LNCS publications has been devalued.

The IACR regrets this move and wants to emphasize that this modification of status has no impact whatsoever on the *scientific* value of the proceedings of our conferences. The program committees of the IACR conferences consist of the best researchers in the field; they perform high quality reviews and select only 15-25% of the submissions based on scientific quality. The IACR maintains that the articles published at its conferences belong to the top quality research in the area of cryptology that is competitive in scientific quality and impact with the results that are published in ISI journals.

IACR Fellows

Current IACR Fellows

- Tom Berson
- Gilles Brassard
- David Chaum
- Don Coppersmith
- Whitfield Diffie
- Shafi Goldwasser
- Martin Hellman
- Hideki Imai
- Kevin McCurley
- Silvio Micali
- Ron Rivest
- Adi Shamir
- Gustavus (Gus) Simmons
- Jacques Stern

New Fellows IACR in 2008

- Ueli Maurer
- Ralph Merkle
- Moni Naor

Procedures

- Candidates, nominators, and endorsers must be IACR members. Verify membership by corresponding with iacrmemHEREATiacr.org
- Deadline: December 31, 2008
- Instructions: http://www.iacr.org/fellows/
- Selection-committee members: Cynthia Dwork, Hugo Krawczyk, Tatsuaki Okamoto, Michael Wiener, Moti Yung

Current Board Activities

Current Board Activities (1/2)

- Expanding the materials available in our own archive (where IACR has the copyright) http://www.iacr.org/archive
  - Currently up to Crypto 2006

Current Board Activities (2/2)

- E-voting for IACR?
- Waiver of registration fee for students who present a paper at IACR flagship conferences (Marconi foundation)
- Expand service to members of national associations for cryptologic research
- Co-location of workshops/conferences to reduce travel

Open Discussion