IACR
International Association for Cryptologic Research

http://www.iacr.org

Bart Preneel

president@iacr.org

About IACR

- Non-profit organisation registered in the USA.
  - “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.”
- Elected Board of Directors
  - volunteers
  - annual elections
- Representatives of Asiacrypt, PKC, FSE, CHES & TCC Steering Committees

Delivering

- Eurocrypt, Crypto, Asiacrypt
- FSE, PKC, CHES, TCC
- Journal of Cryptology and Newsletter
- IACR Reading room at Springer Verlag
- IACR Archive of Past Proceedings (2 years after publication)
  - http://www.iacr.org/archive
- Eprint Archive
  - http://eprint.iacr.org/
- Fellows program

Your Board ('13)

OFFICERS

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

DIRECTORS

- Michel Abdalla
- Josh Benaloh
- Tom Berson
- Shai Halevi
- Anna Lysyanskaya
- Matsuru Matsui
- Christof Paar
- David Pointcheval
- Nigel Smart

Your Board ('13)

APPOINTEES

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

GENERAL CHAIRS

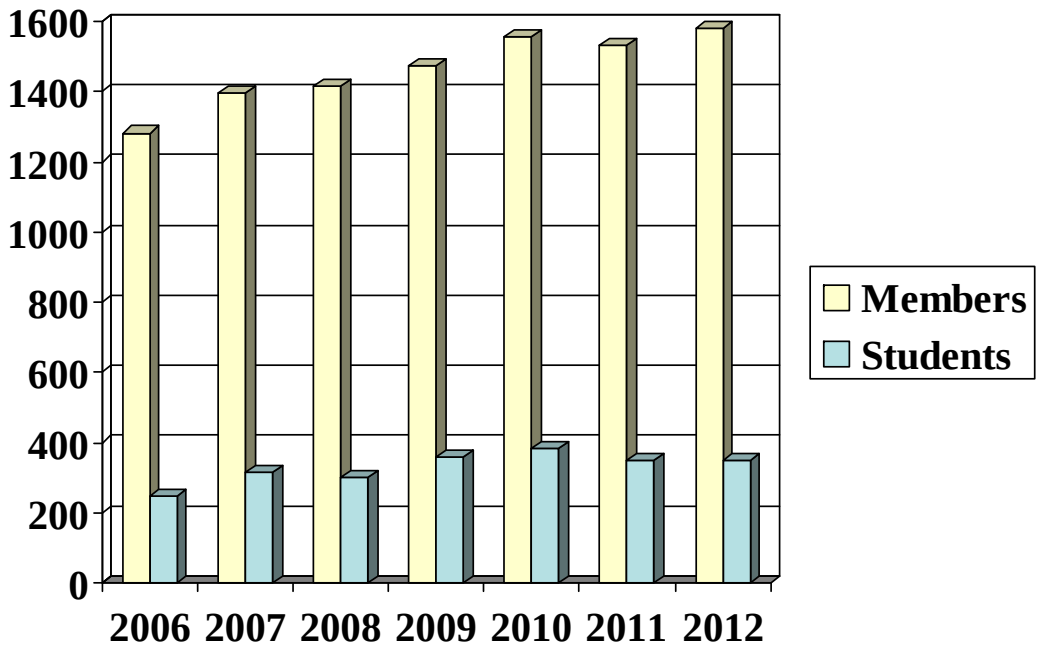
- Aggelos Kiayias
- Helena Handschuh
- Satyanarayana V. Lokam
- Gregor Leander
- Alexandra Boldyreva
- D.J. Guan

STEERING COMMITTEE REPRESENTATIVES

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

Total Membership

- By attending this workshop, you will become a member of IACR for 2014
- If you attended one of our conferences or workshops last year, you are already a member for 2013



FSE Steering committee

- Anne Canteaut, France (2011-2014)
- Thomas Johansson, Sweden (2013-2016)
- Antoine Joux, France (2010-2013)
- Shiho Moriai, Japan (2013-2016)
- Kaisa Nyberg, Finland (2012-2015)
- Bart Preneel, Belgium, IACR contact (1993-2016)
- Vincent Rijmen, Belgium, chair (2010-2013)
- Matt Robshaw, USA (2010-2013)

FSE 2013

FSE'13: 10-13 March, Singapore

- general co-chairs: Jian Guo and Thomas Peyrin
- program chair: Shiho Moriai

FSE 2014 - tentative

FSE'14: 2-5 March, London, UK

- general and program co-chairs:
  Carlos Cid, Christian Rechberger

Springer-Verlag

- IACR reading room: all IACR Members have FREE electronic access to ALL past LNCS proceedings of our conferences & workshops and to J. Cryptology at Springer-Verlag

  http://springer.com/iacr

- Get an access token:
  http://www.iacr.org/

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
2002

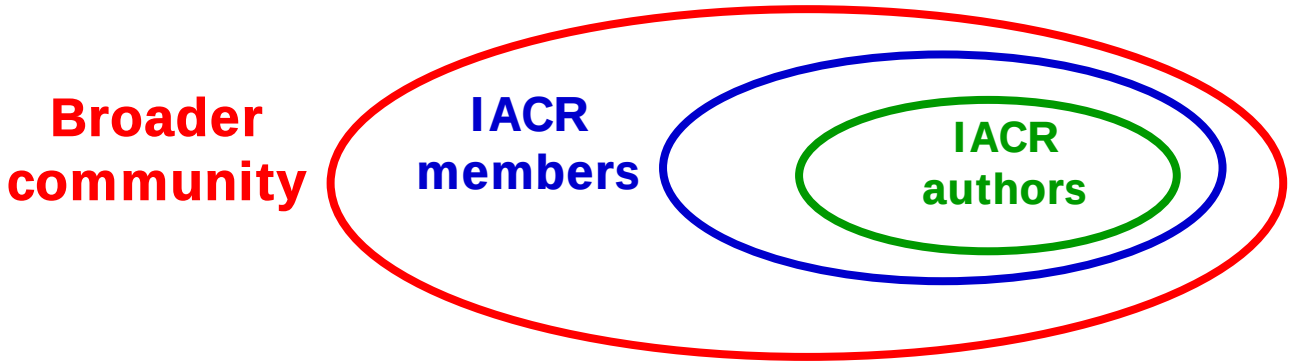
Free access to all Computer Science Journals

Access the entire contents

Current Board Activities

E-publishing

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



New 4-year contract signed with Springer-Verlag: 2013-2016

IACR Authors

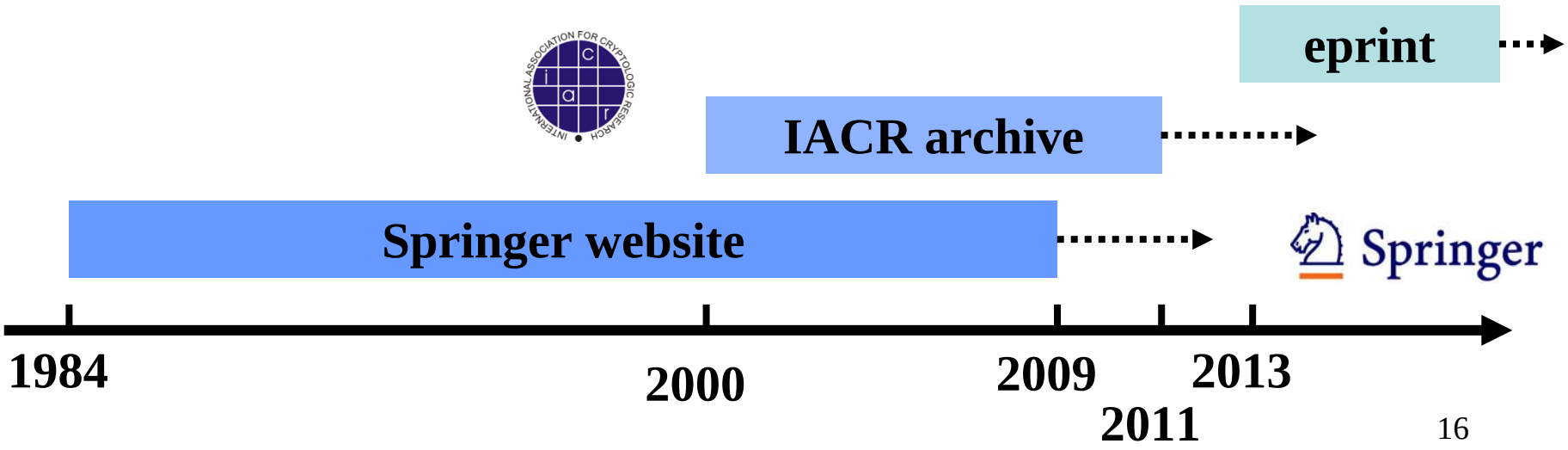
- **Springer version**: available in Springer's digital library
- **IACR version**
  - can be modified to mimick Springer version (except footnote)
  - can be uploaded on Eprint immediately (and also full version if it exists) – if you do not upload it, IACR will do so
  - copyright form will allow reuse for PhD thesis and for pictures
- **Subsequent version**: minor/major revisions (25%)
- Footnote for each version

IACR members/conference attendees

- access to all IACR content on Springer's website (starts 1 week before conference)
- printPDF on USB or conference website

Everyone: free access for many papers

Version	Where	Which papers
IACR	Eprint	2013-...
IACR	IACR archive	IACR papers from 2000 older than 2 years
Springer	Springer website	All IACR papers older than 4 years



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

- **Flagship conferences**
  - the Board encourages program co-chairs to take the necessary actions to ensure a balanced program
  - increase number of accepted papers (accommodate this with shorter talks, more half-days, longer days, parallel sessions)
- **Discussion forum will be added to iacr.org**
  - need for moderator
- **Ethical guidelines for authors and reviewers**
  - http://www.iacr.org/docs/
- **Recording of talks – only with presenter's permission**

Final announcement – for locals only

I will perform with my band in the Esplanada (Singapore) on **Thursday April 4 at 8pm**