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 ('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
- NN

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

Membership
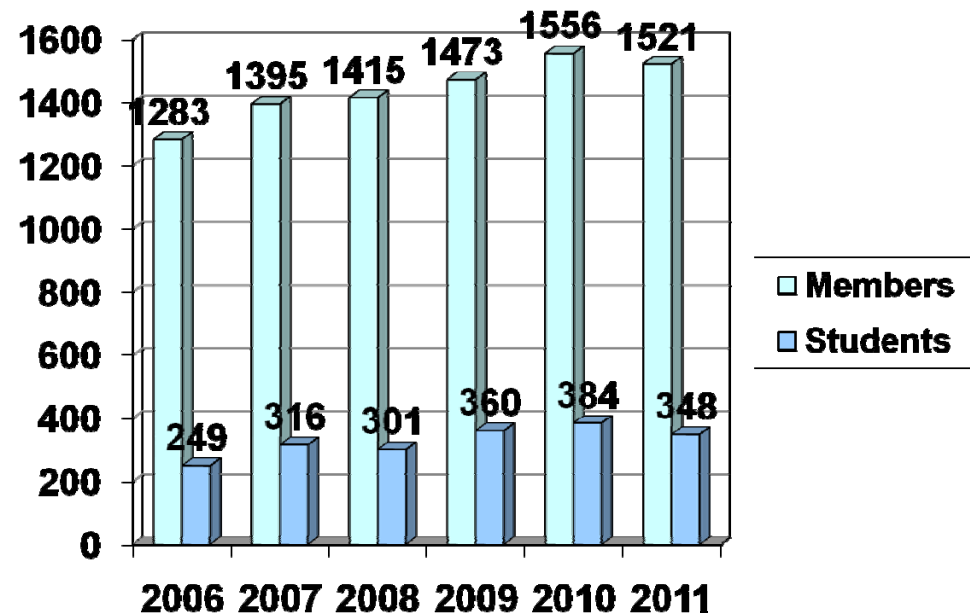
- By attending this conference, you will become a member of IACR for 2013

- If you attended one of our conferences or workshops last year, you are already a member for 2012

FSE

Steering committee

- Anne Canteaut, France, (2011-2014)
- Antoine Joux, France, (2010-2013)
- Mitsuru Matsui, Japan (-2012)
- Kaisa Nyberg, Finland (2012-2015)
- Bart Preneel, (IACR contact), Belgium (-2012)
- Vincent Rijmen, Belgium, (chair 2010-2013)
- Matt Robshaw, France, (2010-2013)
- Orr Dunkelman, Israel, (2009-2012)

FSE'12: 19-21 March, Washington DC, USA
- general chair: Bruce Schneier
- program chair: Anne Canteaut

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/

🐴 **Springer**

Computer Science

Select your subdiscipline ▾   Select a discipline ▾

Welcome to the IACR Reading Room

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 issues

- opt-in for paper
  - today for Journal of Cryptology
  - from 2012 for proceedings
- open access to conference proceedings from 2013
- ethical guidelines for authors and reviewers
- electronic voting with Helios
- Recording of talks – only with presenter's permission