



IACR Membership Meeting
CRYPTO 2013, 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"

Your Board ('13)

OFFICERS

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

DIRECTORS

- ✿ Michel Abdalla
- ✿ Josh Benaloh
- ✿ Tom Berson
- ✿ Shai Halevi
- ✿ Anna Lysyanskaya
- ✿ Matsuhiro 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
- ✦ (Shai Halevi)
- ✦ (Bart Preneel)
- ✦ (David Pointcheval)

Membership

- ✿ By attending this conference, 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





IACR Election

- ✿ There is an election for Board members **every year** in the Fall
 - ✿ at the end of 2013 the terms of the 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 2013 Election Committee) if you would like to know more, or are interested in standing for election

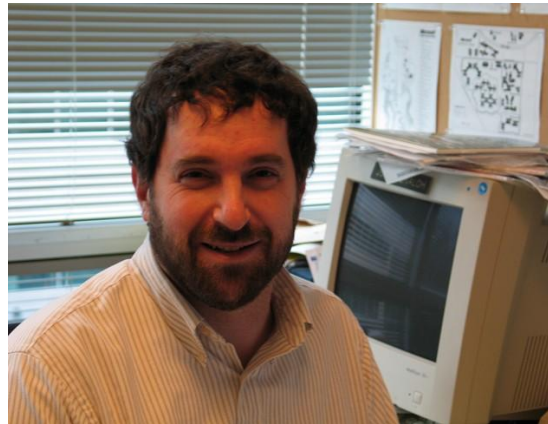
IACR Election Committee 2013

Michel Abdalla

(returning officer)



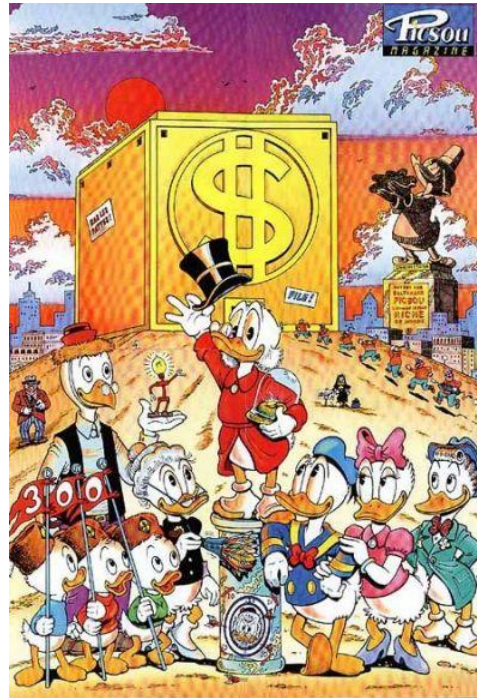
Josh Benaloh
(chair)



Tom Berson



IACR Preliminary Financial Report 2013



Greg Rose

treasurer@iacr.org

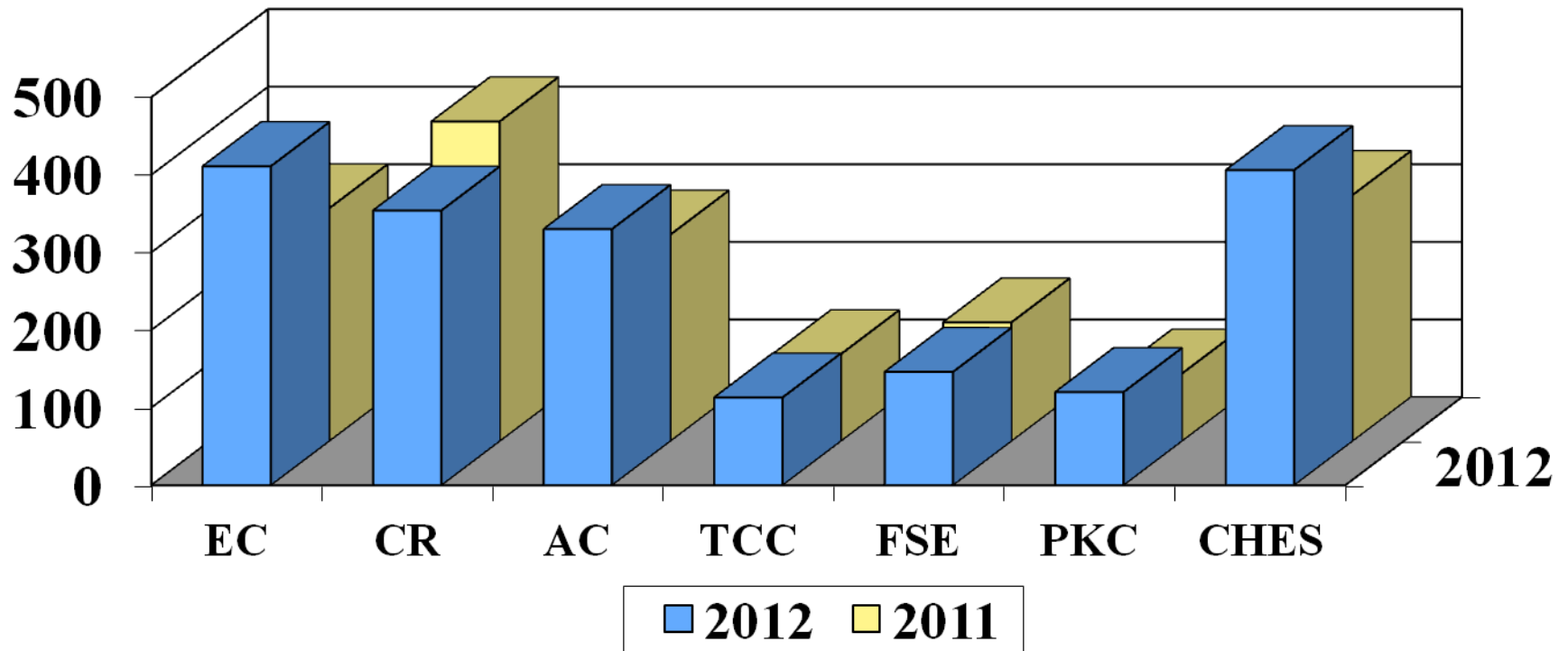
Financial Summary - 2012

- ⊕ US economy recovering, European? Asian?
- ⊕ Financial support from sponsoring organisations increasing greatly, maybe due to recruiting?

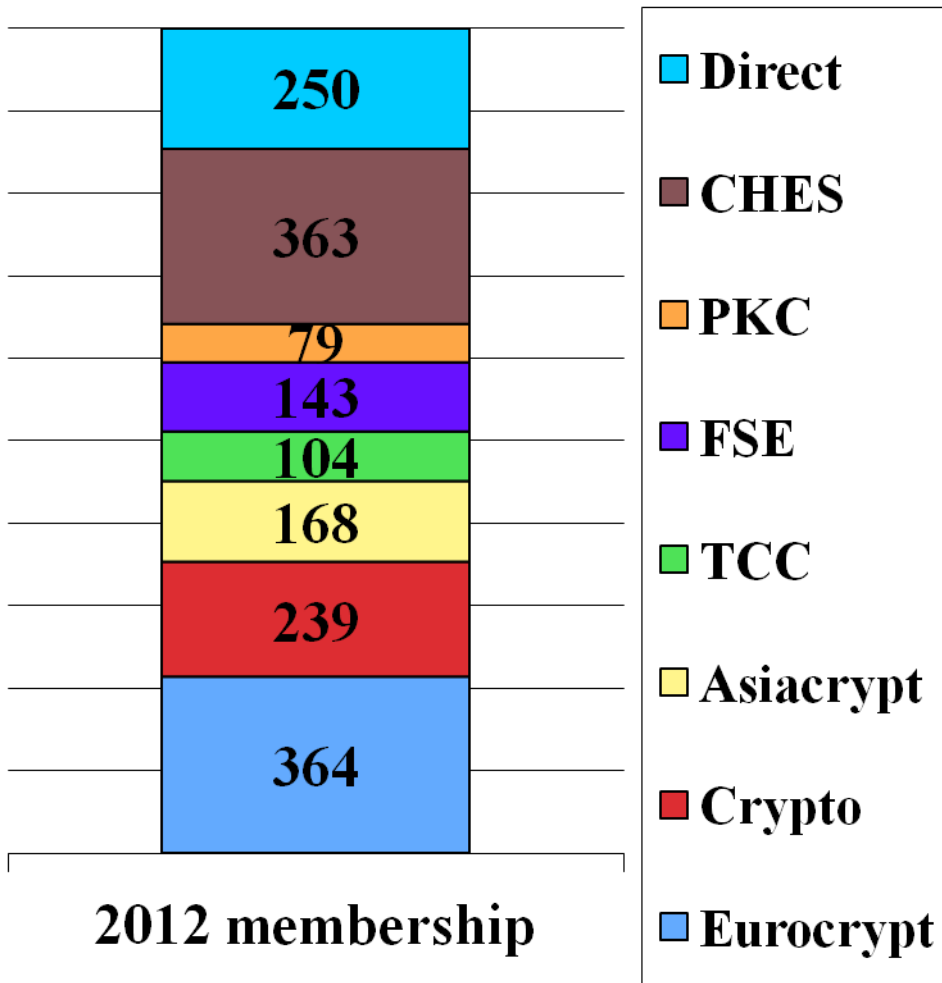
- ⊕ Attendance at our events stable or up, except Crypto
 - ⊠ PKC (87->128)
 - ⊠ TCC (112->113),
 - ⊠ FSE (153->146)
 - ⊠ CHES (317->416)
 - ⊠ Crypto (412->354)
 - ⊠ Eurocrypt (300->411)
 - ⊠ Asiacrypt (266->330)

- ⊕ Extremely low administration overhead : < 2%
- ⊕ ***Strong financial position for IACR ($\log_2(\$) \sim 20.25$)***

2010-12 Conferences and Workshops



2012 Membership



2013 Membership fees collected in 2012:

- ☒ Conferences and Workshops
- ☒ Directly through IACR
- ☒ Now US\$70/35
- ☒ 1710 up 12%



2013 Highlights

- ✿ Marconi grant has run out but sponsorships increasing
 - ✦ Thanks Ron Rivest!
 - ✦ Board agrees to subsidize students in budget process
- ✿ Target break-even (or slight loss) budgets
- ✿ Keep minimal overhead - less than 2%

- ✿ Membership fee currently \$70/35 US dollars
- ✿ Proposed
 - ✦ 2015 Membership fee \$50/\$25
 - ✦ Journal of Cryptology electronic for all; \$20 extra for paper copy

Questions for the Treasurer

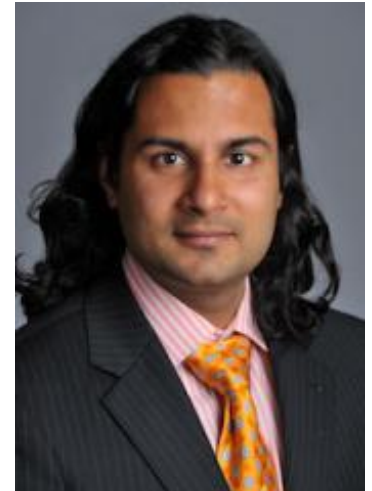




IACR Membership 2013



abhi shelat
iacrmemHEREATiacr.org





2013

1702

Members
(1580 in 2012)

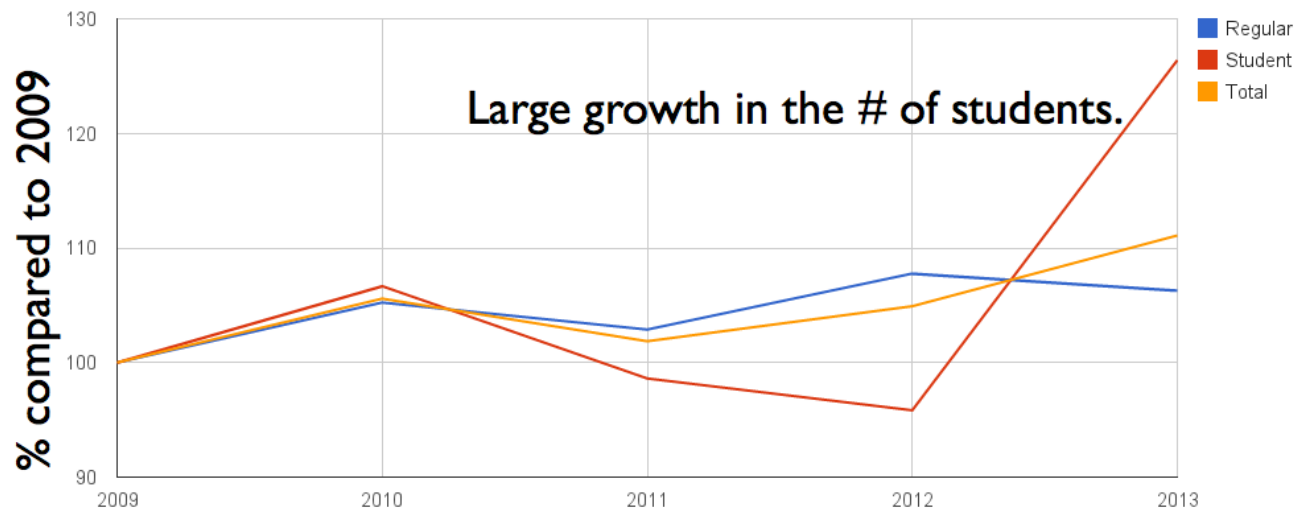
1245

Regular+

457

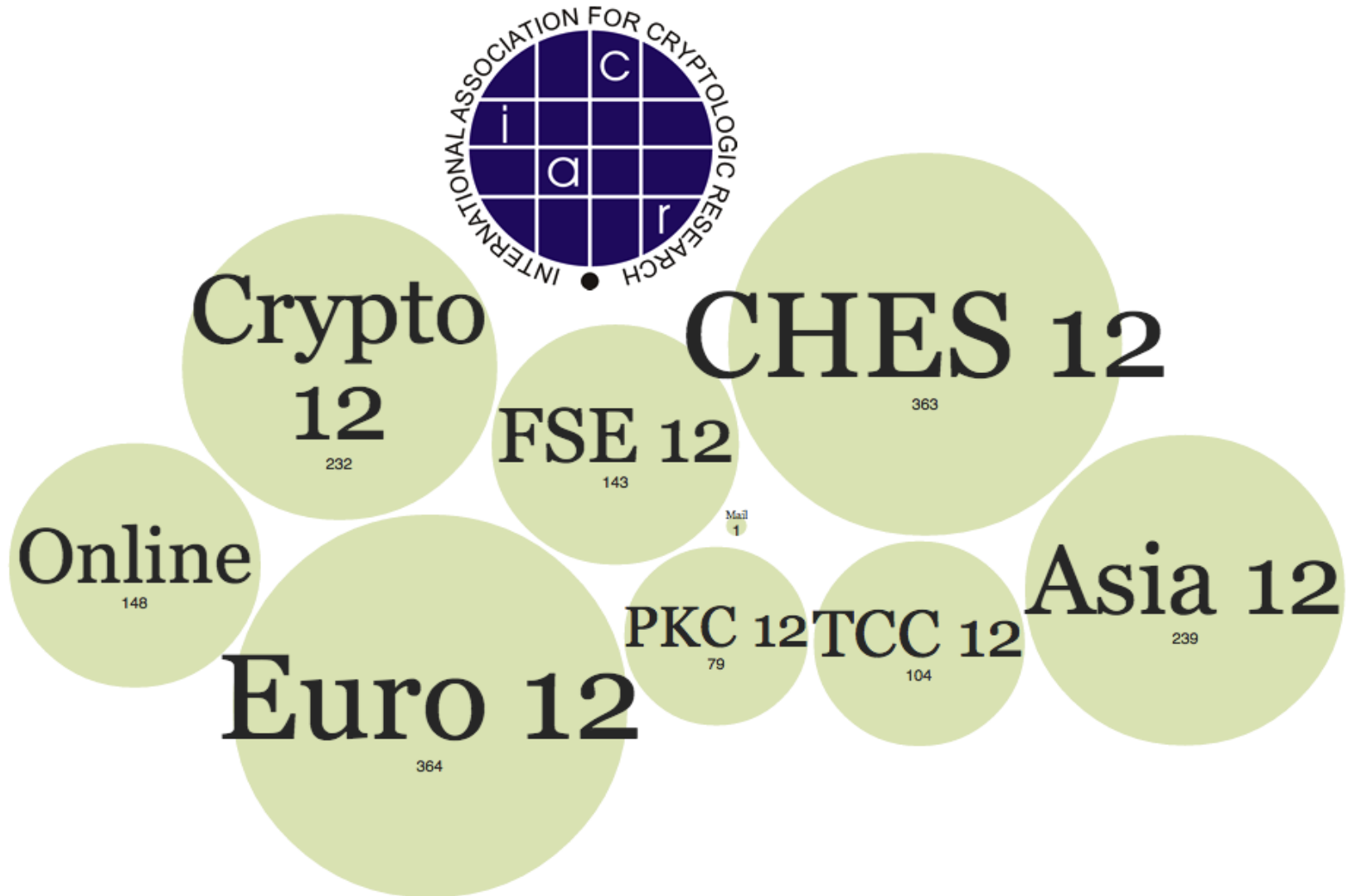
Students

Membership Demographics





IACR Membership Distribution By conference





Conferences & Workshops

2013 Conferences

- ❖ **Crypto'13: 18-22 Aug., UCSB, Santa Barbara, USA**
 - ❖ Helena Handschuh/Ran Canetti + Juan Garay

- ❖ **Asiacrypt'13: 1-5 Dec., Bangalore, India**
 - ❖ Satyanarayana V. Lokam/Kazue Sako + Palash Sarkar



2014 Conferences

- ✿ Eurocrypt'14: 4-8 May, Copenhagen, Denmark
 - ✿ Lars R. Knudsen + Gregor Leander/Phong Nguyen + Elisabeth Oswald

- ✿ Crypto'14: 17-21 Aug, UCSB, Santa Barbara
 - ✿ Alexandra Boldyreva/Juan Garay + Rosario Gennaro
 - ✿ **IACR Distinguished Lecture: Mihir Bellare**

- ✿ Asiacrypt'14: 7-11 Dec, Kaohsiung, Taiwan
 - ✿ D. J. Guan/Palash Sarkar + Tetsu Iwata



2015 Conferences

- ✿ Eurocrypt'15: 4-8 May, Sofia, Bulgaria
 - ✚ Dimitar Jetchev + Svetla Nikova/Elisabeth Oswald + Marc Fischlin

- ✿ Crypto'15: Aug, UCSB, Santa Barbara
 - ✚ Thomas Ristenpart/Rosario Gennaro + NN

- ✿ Asiacrypt'15: 6-10 Dec, Auckland, New Zealand
 - ✚ Steven Galbraith/Tetsu Iwata + NN
 - ✚ **IACR Distinguished Lecture: Phil Rogaway**



2013 + 2014 Workshops

- ❁ CHES'13: 22-24 Aug, UCSB
 - ❁ Thomas Eisenbarth + Çetin Koç/Guido Bertoni + Jean-Sébastien Coron
- ❁ TCC'14: 24-26 February, UCSD, San Diego, CA, USA
 - ❁ Mihir Bellare + Daniele Micciancio/Yehuda Lindell
- ❁ FSE'14: 10-12 March, London, UK
 - ❁ Carlos Cid + Christian Rechberger
- ❁ PKC'14, 26-28 March, Buenos Aires, Argentina
 - ❁ Ariel Waissbein + Juan Garay/Hugo Krawczyk
- ❁ CHES'14: 23-26 September, Busan, Korea
 - ❁ Kwangjo Kim/Lejla Batina + Matt Robshaw

Conferences and Workshops

- ✦ Now hearing proposals for 2016 conferences and 2015 workshops
- ✦ Details on how to submit a proposal on www.iacr.org
- ✦ Or see a member of the Board/Steering Committee

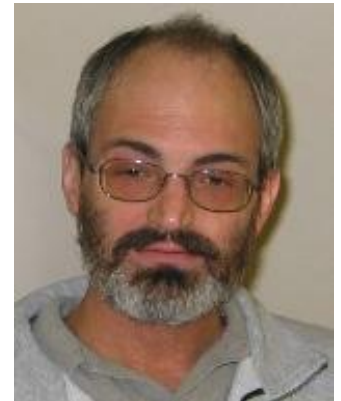


In particular: candidates for Crypto general chair



Journal of Cryptology

Editor in Chief – Matt Franklin
franklinHEREATcs.ucdavis.edu





Journal of Cryptology

- ❖ The premier Journal in cryptology
 - ❖ published by Springer-Verlag
 - ❖ available in reading room and via postal mail to IACR members (unless you opt-out)
- ❖ Overall health very good
- ❖ Submission pipeline steady and sustainable
- ❖ Send me your ideas for new special issues
 - ❖ practical topics especially welcome



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 (please submit!)**
- ⊕ via web but also
 - ⊠ **twitter** (http://twitter.com/#!/iacr_news)
 - ⊠ **RSS**
 - ⊠ **email subscription**
- ⊕ Submit to newsletter HEREATiacr.org



IACR Fellows

New IACR Fellows in 2013

- ✦ Dan Boneh
- ✦ Ronald Cramer
- ✦ Claude Crépeau
- ✦ Lars Knudsen
- ✦ Hugo Krawczyk
- ✦ Victor S. Miller
- ✦ Rafail Ostrovsky

Selection committee members:

- Arjen Lenstra (chair), Ueli Maurer, Kevin McCurley, Tatsuaki Okamoto, Ron Rivest

Rafail Ostrovsky

IACR Fellow, 2013

- ✿ For numerous contributions to the scientific foundations of cryptography and for sustained educational leadership in cryptography





Procedures

- ❁ Candidates, nominators, and endorsers must be IACR members. Verify membership by corresponding with iacrmemHEREATiacr.org
- ❁ Deadline: December 31, 2013
- ❁ Instructions: <http://www.iacr.org/fellows/>
- ❁ Submit to fellowsHEREATiacr.org
- ❁ Selection committee members:
 - ❁ Gilles Brassard, Arjen Lenstra, Ueli Maurer, Kevin McCurley (chair), Phil Rogaway



Publications



Springer-Verlag

- ❖ Publisher of IACR's conference and workshop proceedings in the LNCS series and the Journal of Cryptology
- ❖ LNCS: new contract has been signed for 2013-2016

Multiple versions of a paper

✦ Springer version (has DOI)

- ✦ NN and NN (Eds.): CRYPTO 2013, LNCS xxxx, pp. xx-xx, 2013. © International Association for Cryptologic Research 2013

✦ IACR version (minor differences)

- ✦ "© IACR <year>. This article is the final version submitted by the author(s) to the IACR and to Springer-Verlag on <date>. The version published by Springer-Verlag is available at <DOI>."

✦ Minor revision

- ✦ "© IACR <year>. This article is a minor revision of the version published by Springer-Verlag available at <DOI>."

✦ Full version (more than 25% difference)

- ✦ "This article is based on an earlier article: <bibliographic data>, © IACR <year>, <DOI>."



Access for IACR members


- ✿ PrintPDF on USB stick or conference website
- ✿ Full access to Journal of Cryptology and all proceedings at <http://www.iacr.org/services/springer.php>



<http://www.iacr.org/services/springer.php>

IACR Publications at Spring x

www.iacr.org/services/springer.php



IACR Publications at Springer

IACR and Springer are pleased to offer you free access to the Journal of Cryptology and the IACR proceedings volumes for CRYPTO, EUROCRYPT, ASIACRYPT, FSE, CHES, PKC, and TCC. Simply use the links below to access these publications.

Access to Recent Proceedings and the Journal

IACR members can get access to proceedings from the last four years using their IACR reference number and password.

IACR Reference Number: Password: [Get Access](#) (credentials sent over https)

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



Firefox | www.iacr.org/services/springer.php?tok=springer5214f4b2e804c&val=cd2ecc1cd663a5df86eedc1eda0e607e33cabd4 | Tom Ristenpart

IACR Publications at Springer



IACR Publications at Springer

IACR and Springer are pleased to offer you free access to the Journal of Cryptology and the IACR proceedings volumes for CRYPTO, EUROCRYPT, ASIACRYPT, FSE, CHES, PKC, and TCC. Simply use links below to access these publications.

Journal of Cryptology

- [Journal of Cryptology](#)

Advances in Cryptology - CRYPTO

- [CRYPTO 2012](#)
- [CRYPTO 2011](#)
- [CRYPTO 2010](#)
- [CRYPTO 2009](#)
- [CRYPTO 2008](#)
- [CRYPTO 2007](#)
- [CRYPTO 2006](#)
- [CRYPTO 2005](#)
- [CRYPTO 2004](#)
- [CRYPTO 2003](#)
- [CRYPTO 2002](#)
- [CRYPTO 2001](#)
- [CRYPTO 2000](#)
- [CRYPTO 1999](#)



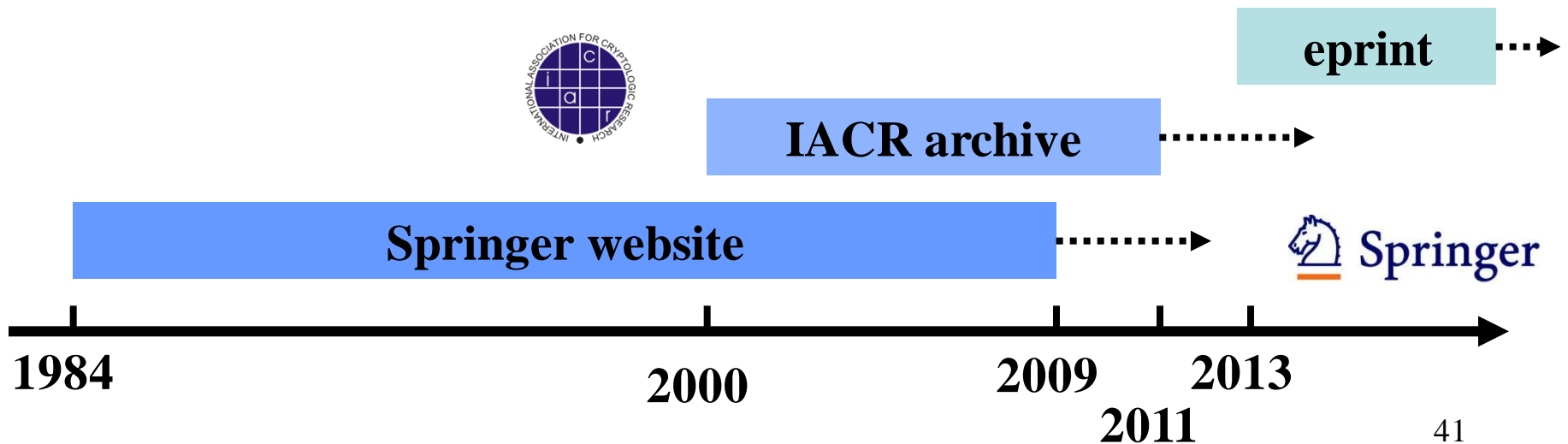
Advances in Cryptology - EUROCRYPT

- [EUROCRYPT 2013](#)
- [EUROCRYPT 2012](#)
- [EUROCRYPT 2011](#)
- [EUROCRYPT 2010](#)
- [EUROCRYPT 2009](#)
- [EUROCRYPT 2008](#)
- [EUROCRYPT 2007](#)
- [EUROCRYPT 2006](#)
- [EUROCRYPT 2005](#)
- [EUROCRYPT 2004](#)
- [EUROCRYPT 2003](#)
- [EUROCRYPT 2002](#)
- [EUROCRYPT 2001](#)
- [EUROCRYPT 2000](#)



Access of broader community

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



Authors

✚ Copyright form revised

- ✚ submit IACR version to eprint
- ✚ reuse of pictures and parts
- ✚ inclusion in Master/PhD thesis
- ✚ give license for slides/video/extra content

✚ Eurocrypt authors: please sign again

<https://secure.iacr.org/websubrev/ec2013/submit/copyright.php>



Current Board Activities

E-publishing

Opt-In for paper

- ⊕ Proceedings: since 2011
- ⊕ Journal of Cryptology: from 2015 onwards



Change of Bylaws: October vote

- ✪ Journal of Cryptology electronic for all; paper for extra fee
- ✪ Members who are 65 years or older and who have been members for 20 years can apply for senior membership (no membership fee)
- ✪ Delay start of election from October 1 to October 15 (end stays at November 15)
- ✪ The Board at its discretion may appoint a limited number of additional non-voting members
- ✪ Rename Newsletter Editor to Communications Secretary



Proposal for Article III: Membership

- ✦ Membership is open to any person subscribing to the purposes of the IACR.
- ✦ There are three categories of membership: regular, student, and senior. Student members must be enrolled as a student in an institution of learning.
- ✦ A person becomes a regular or student member or renews his or her regular or student membership either of two ways: 1) upon acceptance by the IACR Membership Secretary of his or her personal membership application form and payment of one year's dues or 2) notification to the IACR Membership Secretary by the General Chairperson of attendance at any one of the IACR Conferences or IACR Workshops.
- ✦ A member can become a senior member in any calendar year following the year in which he or she has reached the age of 65, provided that he or she has been a regular or student member for at least twenty years (not necessarily consecutive). Members can apply for senior membership by submitting a request in writing to the IACR Membership Secretary. A senior membership does not need to be renewed and no membership dues need to be paid.
- ✦ All members have electronic access to the Journal of Cryptology and to recent IACR Conference publications. A print subscription of the Journal of Cryptology is available at an extra cost.
- ✦ Membership period as a result of attending an IACR Conference or IACR Workshop is for the calendar year following the workshop. The calendar year begins on January 1 and ends on December 31.
- ✦ Membership applications (other than as a result of attending an IACR Conference or IACR Workshop) processed on or before August 31 in any given year will apply to that calendar year. Membership applications processed from September 1 onward will apply to the following calendar year. Regardless of the time of application and becoming a member, the membership fee for the full calendar year has to be paid

Ethics, Responsible Disclosure and Injunctions

- ✿ Ethics guidelines for authors and reviewers
<http://www.iacr.org/docs/>
 - ✦ responsible disclosure guidelines will be added
- ✿ Resisting injunctions? (e.g., Usenix 2013)
 - ✦ submit accepted papers to eprint
 - ✦ suggestion by Whitfield Diffie/Ross Anderson:
when program is announced, submit to eprint a
version encrypted with a 50-bit key



Flagship conferences

❁ **2011 and 2012:**

- ❁ 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)

- ❁ **2013:** The Board strongly recommends the Crypto 2013 program co-chairs to implement **parallel sessions** as an experiment

Revisiting the IACR publication strategy

⊕ Multi-dimensional problem

- ⊠ Quality
- ⊠ Speed
- ⊠ Reputation
- ⊠ Review load
- ⊠ Bandwidth limitation
- ⊠ Complexity

⊕ Discussion forum

<http://eprint.iacr.org/forum/list.php?14>

Multi-channel strategy

- ✚ Eprint – immediate
- ✚ Conferences – faster but not fully reviewed
- ✚ Journal of Cryptology

Goals

- ✦ Full open access (gold)
- ✦ Referee and publish full papers (or publish what has been refereed)
- ✦ Journal (“Proceedings of the IACR”)
 - ✦ acknowledge we do multi-round refereeing
 - ✦ credit outside our community
- ✦ Remove deadline rush
- ✦ Speed up review/publication process
- ✦ Deal with bandwidth limitations
- ✦ Simplify the publication model and the supporting infrastructure (by removing multiple version problem)

Mechanism

- ❖ Decouple publication from conference presentation
- ❖ Sticky reviews with rebuttal and revision by authors could be used immediately

Issues

- ❖ Deviate from computer science tradition; align with most of science (incl. math/engineering)
- ❖ New adversarial models and optimizations
- ❖ Much less radical alternatives: for each conference/workshop a special issue for Journal of Cryptology (limited number of papers)

Open Discussion





Implications

For Authors:

- You submit to journal at any time
- Guaranteed first response in 2 months (Accept, Reject, Maybe)
 - could be longer for longer papers
- For Maybe's you have 1 month to respond and **make changes**
- Final decision in another 2 months
- **All acceptable papers are published**
- **(Top?)** papers are asked to **present** at either AC, EC or CR.
- Authors can “**request**” consideration for presentation at specific venue (cannot be guaranteed)
- A conference paper cannot be resubmitted in full version to JoC. Since the full version is already published



Implications

For Referees

- A “PC” member (called referee below) is appointed for 2 years
- Instead of agreeing to referee 20 papers in 6 weeks, asked to referee (with sub-referees) over a period of 2 years 20 papers with a delay of 6 weeks (plus 2 weeks for discussion)
- A year’s PC is “run” by a committee of six co-chairs. To replicate our current AC, EC, CR PC chair model
- Each co-chair appoints a set of referees, who themselves appoint sub-referees (keep the pyramid structure)
 - Alternative: pool of referees can be shared by all co-chairs
- Referees chosen to represent geographic and subject diversity
- Idea is to **reduce** reviewing burden

Implications

For Conferences

- PC Chairs pick the papers for a conference of those which have been accepted in last 6 (or 12) months
- Taking into account
 - Author preferences
 - Diversity of Programme
 - Which papers would make good talks
 - Celebrate the best work
- Conferences become about exchanging ideas and learning
- Stop short talks which no one listens to and no one understands
- Encourage industry/government back into the fold

Knock On Questions

Should PKC, TCC, FSE and CHES stick to their current conference/LNCS model?

- If not what happens to them?

Would suspect CHES would continue due to industrial interest

- Others less sure about. Is this a problem?

What about short papers can we create a very fast turnaround

- e.g. a “Bulletin of the IACR”