MINUTES IACR MEMBERSHIP MEETING *EUROCRYPT'14*

COPENHAGEN, 14 MAY 2014

Opening. At 16.55 Cachin opens the meeting. He begins by giving an overview of the IACR and its activities. In particular, he draws attention to IACR's new initiative to support Cryptology Schools. Prompted by a question by Vaudenay, Cachin confirms that IACR will ensure that any supported schools are not for profit.

Publications. Cachin discusses the future of IACR publications guided by a set of questions that were formulated in 2013.

1 Should IACR move to Gold Open Access?
There is mild interest for Gold Open Access and not just Green Open Access (as is currently the case), but equally there are some who do not support a move to Gold Open Access (given the likely cost involved).

1a Should IACR worry about ISI indexing?
There is a quick informal straw poll, where 19 think IACR should and 8 do not think so. Vaudenay suggests that those who worry most might not be here.

1b Who should pay for open access?
- Several people point out that the question is not independent of the cost.
- Yung thinks that the only fair option is that the authors pay themselves as he reckons that other options will result in a push towards fewer papers.
- Smart posits that payment by authors will lead to unfairness as richer universities will be advantaged.
- Meiklejohn wonders whether there will be an ACM-like option available and whether payment will be optional or mandatory for authors. Cachin answers that currently authors can already pay to make their article immediately (gold open) accessible, however this option is not widely advertized.
- Dunkelmann asks at least three years notice to put appropriate funding requests into grants. Smart remarks that a need for gold open access might come sooner. He also suggests a division of the costs.

A quick straw poll reveals 13 people who favour that authors should pay, 36 people who believe IACR members should pay, and 8 people who think that conference attendees should carry the costs.

2 Should we publish what is submitted?
- Stam believes the more accurate question is whether we should submit what we intend to publish.
- Nugent (representative from Springer) points out that longer papers still carry more cost, for instance open access will become more expensive. He also wonders whether the costs as presented by Cachin are based on the current status or on new information or even a concrete quote from Springer. Cachin clarifies that the numbers represent the current status.
- Preneel is concerned that the publication of 40 page papers will make it infeasible for the full published paper to be reviewed. He wonders what this means for the claim that papers are peer-reviewed.
- Smart opines that we currently effectively review and publish summaries instead of full papers.

There is a question from the audience why it is bad to have multiple versions of a single paper. Smart answers that apart from wasted effort, it leads to referencing problems (such as dilution).

• Should there be an enforced page limit on the full submission to IACR conferences and workshops?
- Lysyanskaya sees no point in such a limit.
- Dunkelmann believes that if there is no multi -round reviewing, one should not enforce a page limit.
- Bernstein believes there is a difference between content that will appear, and additional information useful to PCs to decide on acceptance or not. He believes the committee should not be responsible for the additional information.
- Ishai points out that expert reviewers do not necessarily need to read a full proof in order to check it. Instead the proof can be adaptively checked on points that are deemed most challenging. He also remarks that the quality of journal reviews is often below that of proceedings.
- Waters fears that some authors might use a length limitation as excuse not to include proofs.
- Smith remarks that in his field appendices often contain massive lists of polynomials or other material that noone would necessary value.
- Meiklejohn thinks that the current practice of submitting 80 page papers has the effect is that the full papers are never fully refereed. Putting a page-limit would trigger authors to submit to journals instead. Smart concurs (that if authors cannot write a short paper, submission should be to a journal).

There were some suggested page limits, but no straw poll took place.

- Should reviews be sticky?
  Cachin clarifies that the question is whether stickiness should be encouraged.

  Somewhat relatedly, Oswald wonders what the purpose is of the existing rebuttal process: Is it to improve the quality of the papers or of the reviews? She points out that for *Eurocrypt'14* the final papers (after the initial review and rebuttal) were not reviewed. Preneel mentions that program chairs have a responsibility to check the final version.

  A quick informal straw poll reveals about 40 people in favour of sticky reviews, and 5 against.

Treasurer's Report. Rose presents the current financial status, which is healthy. Attendance at the various conferences is stable, apart for a slight dip at *Asiacrypt'13*.

Membership Secretary. Cachin presents shelat's slides. Positively, the number of student members is growing. Cachin thanks abhi for the hard work he is doing.

Notices from the Board. Cachin explains that the Board of Director would like to keep track of gender statistics of conference attendence and suggests to collect this information as part of conference registration.

Clark wonders how putting this question on the registration will benefit the membership. Cachin responds that several members have asked for this information, to which Rose adds that in some countries grant support can be endangered unless these statistics are provided.

Leander believes that counting at an invited talk would be a good alternative to the Board's proposal.

There is a straw poll where 26 are in favour of the proposal with 15 against.

Open Floor.

- Rogaway takes the floor and asks the question whether the IACR as organisation should say or do something as a consequence of the recent revelation of mass surveillance. The Charter of the IACR explicitly mentions that the IACR should serve the public welfare and he believes as a community we have gone amiss by not publicly condemning mass surveillance. He proposes the IACR Membership makes the following statement.

  > **Statement of Principle from the IACR Membership on Mass Surveillance and the Subversion of Cryptography**
  > The membership of the IACR repudiates mass surveillance and the undermining of cryptographic solutions and standards. Population-wide surveillance threatens democracy and human dignity. We call for expediting research and deployment of effective techniques to protect personal privacy against governmental and corporate overreach.

  The statement is unanimously accepted and will be featured prominently on the website. Cachin asks what consequences acceptance of the statement will have for the IACR as an organization legally based in the USA. Rose remarks that he believes there will be none in that regard.
- Tripathy confesses the conference was a big surprise to him and he believes the IACR should be able to develop some subsidiary income scheme since the current reserve is tiny: the IACR needs to develop more of a business nose. Rose remarks that the IACR is a not-for-profit organization, which puts limits on the potential to generate income.
- Yung believes that, despite the possible negative tone at this meeting, we are a very successful field and there is every reason to be very optimistic.
- Clark notes that membership meetings inevitably run out of time. He requests slides to be made available in advance of the meeting to enable more discussion. Cachin responds that this was his first membership meeting as president and he will be better prepared for *Crypto'14*.

Closing. Cachin thanks everyone for their attendance and closes the meeting at 18.27.