MINUTES IACR MEMBERSHIP MEETING *EURORYPT'13*

ATHENS, 29 MAY 2013

Opening. At 16.32 Preneel opens the meeting. He begins by giving an overview of the IACR and its activities.

Treasurer's Report. Rose presents the current financial status, which is healthy. Attendance at the various conferences is stable, with a little dip for *Crypto'12*. He mentions that the Marconi grant has run out and he thanks Ron Rivest for his generous gift enabling stipends for students to attend IACR events. The Board has decided to keep the scheme in play using IACR's budget.

Rose mentions statutory he has to propose a membership fee for the coming year and would like the membership's opinion on the matter. He suggests three different proposals for a membership fee.

Option A: Add an optional 20 USD fee for the Journal of Cryptology
Option B: As A, but lower the base membership fee accordingly
Option C: As the current breakdown (70 USD for full members/35 USD for students).

Preneel provides some further background behind the proposals, which is followed by a brief discussion.

- Andy Clark asks for a rationale of option A, as financially the IACR does not need to charge for the Journal of Cryptology. Rose clarifies that he likes to discourage members to have paper versions.
- Moti Yung thinks the IACR is working fine and that nothing is broken. To him there is no need to correct something that works and he believes option C looks perfectly fine.
- Serge Vaudenay expresses that options A and B are very similar in nature.
- Josh Benaloh remarks that currently the largest part of the membership fee is used to cover the expenses of a printed journal sent to the members; the 20USD does not fully cover the JoC costs. If this cost is taken away, the fee seems quite high.
- abhi shelat posits that the higher fee (with an opt-in journal) will create a small surplus on the budget that could be used for an increase in IACR-sponsored student stipends.

After the discussion there is an informal show of hands. In the first round, there are roughly a 35, 45, and 25 supporters for each of the proposals A, B, and C, respectively. In a second round between proposals A and B, there are roughly 35 supporters for option A and 55 for option B.

Membership Secretary. Although abhi shelat (the membership secretary) is present, Preneel presents his slides in the interest of time. On a positive note, the number of student members is growing. Preneel thanks abhi for the hard work he is doing.

Awards. Preneel presents an award to *Eurocrypt'13* General Chair Aggelos Kiayias, who did an excellent job with his team. Kiayias thanks the generous sponsors of *Eurocrypt'13*, who made possible a good number of stipends and student support. He also thanks his three adjudants and the conference helpers. Kiayias continues with the prize-giving for the scytale competition.

Preneel subsequently presents an award to *Eurocrypt'13* Program co-Chairs Thomas Johansson and Phong Nguyen. Thomas Johansson presents the *Eurocrypt'13* Best Paper Award to Sanjit Garg, Craig Gentry, and Shai Halevi. Garg receives the plaque, the remaining two coauthors are awarded a scytale.

Notices from the Board. Preneel mentions that the IT systems of the IACR are ageing; the Board has initiated a project to upgrade and revise the current infrastructure.

Preneel draws attention to IACR's twitter and RSS feeds, as well as to recent calls by the Board:

- the Editor-in-Chief of the Journal calls for ideas for special issues, and
- the newsletter editor calls for updates to the PhD Database.

Preneel mentions that there will be seven new Fellows of the IACR this year. They have all opted to receive their plaque at *Crypto* this year. [Lars Knudsen later opted for *Asiacrypt'13* instead.] The fellowship committee is calling for nominations for new fellows.

Publications. Preneel explains the current situation. A new contract for the proceedings with Springer has been signed that will be valid for the period 2013–2016. This contract will provide green open access to IACR authors (allowing publication of the paper in a format very close to the official Springer paper, but *not* the actual Springer PDF) as long as authors follow certain rules. Preneel explains these in more detail, in particular the need to add clear footnotes indicating which version is involved.

Preneel notices that Opt-In for paper copies of the proceedings is working well, and the Board is moving towards Opt-In for the journal too.

Open Floor. Preneel continues with possible options for future publications, refering to yesterday's Rump Session talk by Nigel Smart (who presented a straw man proposal to move to a publishing model where the current conference proceedings become a journal called Proceedings with fully refereed papers and decoupling to a degree publication and presentation).

- Chris Peikert has a few comments that came to mind. He is concerned that if a full version has to be submitted directly, this might incur a slowdown on dissemination of new results. There ought to be a mechanism for preliminary results. Secondly, there is a culture change required related to reviewing, where more timely and more rigourous reviews are required. He is not convinced that changing the mechanism will lead to a change in culture. He believes we should converge quite quickly on a more concrete model. It is unclear to him whether the PVLDB community has a similar need of rigourous reviewing of theorems and proofs.

  Preneel agrees that the Board (together with the Membership) will have to work out the details of any proposed publication model.
- Ben Smith asks for a clarification what the supposed role of the Journal of Cryptology will be: How does he decide where to submit? Preneel acknowledges that there is no clear answer yet. However, the Journal is established and has an impact factor, so we should not stop it.
- Orr Dunkelman refers to the San Francisco Declaration on Research Assessment, related to (the abolishment of) impact factors and suggests IACR might want to become a signatory.

  Dunkelman reckons that at the moment IACR publishes around 220~250 papers a year. The new model might well lead to a significant increase in accepted papers. He wonders what it would mean for the non-IACR conferences (SAC, CTRSA, etc.) it the IACR would accept around 500 papers a year. He believes these workshops might die and poses the question: do we want to terminate these conferences or coordinate with them?

  Preneel acknowledges is a pertinent question and assures that the IACR is not intent on killing anything. One possible suggestion would be workshops without publications.

  Dunkelman's final point is a model where the IACR adds a layer to the current Journal of Cryptology based on subfield. The reviews from the conferences and workshop could be maintained for the Journal reviewing process.
- Yevgenyi Dodis has a few comments. Overall he supports the idea and he does hope that the major conferences will stay. He sees it as a relatively small step, not a big step. It would ensure journal status of many more papers. He likes that it would encourage a global picture of the field and that there will be one place for the paper and its revisions.

  He wants to encourage a more interactive review process to make participation a more rewarding experience. He advocates a mechanism to make reviews publicly available as it will help junior people to see what are considered the strong points in a paper. Preneel considers public reviews orthogonal to the current publication discussion.
- Yvo Desmedt would like to remind that James Massey suggested in 1986 for all papers from EC and C to go to the Journal. If this would be done now, it would result in a high impact factor. Preneel says the impact factor might also be damaged in the short run due to the increased volume of papers over which the index is calculated.
- Tanja Lange agrees that it is good to have a more open version control. Although it is good to have some memory, she would not want a paper to be killed at the first submission.

  She agrees with Dunkelman that the new model might pose a danger to other conferences.
- Andy Clark thinks we have a fantastic community. He likes to congratulate the Board for facing this problem and trying to tackle it. He refers to the mission of the IACR: "Our role is to advance cryptologic research and the interest of its members" He thinks it would be helpful to determine at the beginning what would constitute success and concentrate on making things better, rather than fixing what is broken.
- Dan Bernstein imagines an author who gets rejected again and again. He does not see how the new proposal will change this, as submissions are not public so there is no embarassment. Cachin responds

that the new system would have to come with a journal style resubmission policy: if you get rejected you should not resubmit within a year.

A show of hands indicated a clear majority in favour of moving away from the current model. The Board asks everyone to contribute to (fleshing out) the details of the proposal(s), for instance by using the forum. The Board will then come up with a more concrete proposal.

Closing. Preneel thanks everyone for their attendance and closes the meeting.