MINUTES IACR MEMBERSHIP MEETING *CRYPTO'13*

UCSB, 20 AUGUST 2013

Opening. At 16.41 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 and workshops is stable. 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 continue sponsorship of student speakers of the IACR conferences (not including the workshops).

The membership fee is currently 70/35 USD for members (or student members). At Eurocrypt there was a straw poll to reduce the membership fee for 2015 to 50/25 USD, based on a projected cost reduction by moving to an opt-in model for the Journal of Cryptology. Today he formally proposes said membership fees to the Assembly. With no votes against, five abstentions and all others in favour, the membership fees for 2015 are set to 50 USD for regular members and 25 USD for student members.

Preneel thanks Rose for doing an excellent job.

Membership Secretary. Preneel presents shelat's slides in his absence. There is a noticeable increase in the number of student members.

Awards. Preneel presents an award to *Crypto'13* Program co-Chairs Ran Canetti and Juan Garay for doing a great job. Preneel subsequently presents an award to *Crypto'13* General Chair Helena Handschuh, for organizing a great conference. Preneel recalls that this year seven new IACR Fellows have been inducted

Notices from the Board. Preneel draws attention to IACR's twitter and RSS feeds, as well as to recent calls by the Board and the fellowship committee.

- the Editor-in-Chief of the Journal calls for ideas for special issues, and Preneel points out that Franklin's term is drawing to a close and thanks him for his wonderful job.
- the newsletter editor calls for updates to the PhD Database.
- the fellowship committee is calling for nominations for new fellows.

Preneel explains the current situation regarding open access of the proceedings. A new contract for the proceedings has been signed with Springer 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. These changes have been incorporated in a new, more lenient copyright form. Preneel explains these in more detail, in particular the need to add clear footnotes indicating which version is involved.

Bylaws changes. 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 from 2015 onwards. Since the Bylaws are quite explicit regarding the distribution of the Journal, this requires a change in the Bylaws. A quick straw poll shows an overwhelming majority in favour with 2 votes against and 3 abstentions.

Preneel points out that Diffie has suggested to instigate a life membership for those senior members who have a long membership record. Again, this would require a change in the Bylaws. A quick straw poll shows a large majority with 3 votes against and 15 abstention.

The necessary Bylaws changes will be put to the ballot for the upcoming elections. In addition, Preneel explains a number of smaller proposed changes in the Bylaws that will also be put to a vote in the upcoming elections.

Parallel sessions. Previously the Board has encouraged program co-chairs to increase bandwidth and improve balance. The program co-chairs have been taking this up. For next year the Board strongly recommends to the Crypto 2014 program co-chairs to implement parallel sessions as an experiment.

Lange believes it sucks. Rabin thinks that damage will be created gradually, slowly creating a splintering of the community. She concludes that a one year experiment will not be representative. Ferguson observes that the separate workshops already caused some splintering. Lindell thinks that parallel sessions could increase the size of the conference and that accepting more papers would lead to a more inclusive experience.

There is a quick straw poll, which indicates about 20 members against the introduction of parallel session, about 50 members in favour, and about 30 members abstaining.

Future of Publications. Preneel explains that the Board has initiated a discussion to revisit IACR's publication pipeline. At Eurocrypt'13, Smart has presented a preliminary strawman proposal and a more detailed strawman proposal has been put online two weeks ago. Discussion of the proposal and alternatives is encouraged. Preneel explains the goals as identified by the Board, as well as some known issues with the strawman proposal. He then opens the floor for comments.

Open Floor.

- McCurley mentions that part of the change is motivated by the ISI's decision to index only journals, and not proceedings.
- Boneh proposes to submit a paper to eprint simultaneously (anonymously), and also to submit 5 reviews when submitting a paper. Ferguson remarks that PC members should not be chosen by the authors.
- Kelsey believes getting new people into the field is good, even though they are typically not the right ones to review papers.
- Lindell remarks that the Journal of Cryptology has a very long turnaround time and he wonders whether the Journal could be used for longer papers and Transactions for shorter papers. He thinks it is possible to fix any problems in a more local way. Preneel wonders whether people will review for possible Transactions.
- Schroeppel believes the anonymity of the current submission system does not provide proper anonimity as it is fairly easy to deanonymize.
- Dodis wants to look at the three major problems and find the simplest solution to it.
- Halevi thinks that any problems should be fixed in the smallest possible way.
- Canetti wants to emphasize the importance of independent academic processes. He believes currently the Board is too powerful as it chooses all program chairs. Having independent program committees should be valued as currently PC discussion leads to more than the sum of the parts. Preneel understands the concern, but notices there is limited independence.
- Orman strongly wants direct gold open access, but expresses scepticism about the possibility to realize this. Preneel explains that the Board is committed to increase control for authors and the IACR over its publications.
- Dodis asks how to go forward. Preneel responds that there is a discussion forum. Stam mentions that the minutes of Board and Membership meetings also contain valuable discussion.

Closing. With a standing ovation Preneel is thanked for his amazing service as President. Preneel thanks everyone for their attendance and closes the meeting at 17.46.