MINUTES IACR MEMBERSHIP MEETING *EUROCRYPT'11*

Opening. At 17.01 Preneel opens the meeting. He begins with thanking the outgoing Officers, which is met by applause from the Assembly.

Treasurer's Report. Rose presents the current financial status, thanking his predecessor Helena Handschuh for the wonderful job she has done and her help ensuring a smooth transition. He mentions the Board's intentions to change the way reserves are held. No questions are asked.

Awards. Preneel presents an award to *Eurocrypt'11* General Chair Helger Lipmaa. Lipmaa thanks the people for coming and acknowledges the support he got from the ladies at the desk.

Preneel subsequently presents an award to *Eurocrypt'11* Program Chair Kenny Paterson.

Notices from the Board. In response to Preneel's presentation, Diffie informs whether IACR's genealogy website could support a feature. Wolf (web manager) answers that in principle the feature is supported, but that still a lot of data missing to use it effectively.

Preneel announces that Ueli Maurer will be the next chair of the Fellows committee and calls for nominations.

Preneel mentions the option to opt out of receiving the paper version of the Journal of Cryptology. Prompted by a question from Dodis, he clarifies that the opt out is personal, which might eventually lead to a differentiation in membership fees.

Elections. The past election is briefly evaluated and two issues for upcoming elections are discussed. Firstly, the election for Directors will in future be based on approval voting. This means that anyone can vote for as many candidates as desired (as before, the three candidates with the most votes are elected). It will not be possible to write in candidates. Yung warns that the procedure needs to be clearly explained on the ballot. The Board concedes that the current system is easier to use, but it leads to more invalid ballots.

Secondly, for the past election the ballots were anonymized to the extent that it was not even possible to see which members had voted at all. The question is whether encrypted ballots should be publicly linked to voters or not (obviously, the contents of the ballot remains hidden). A quick straw poll reveals a preference for the current system (12 for publishing, 33 for privacy).

Rolling Co-Chair System. Preneel explains the rolling co-chair system (for Eurocrypt, Crypto, and Asiacrypt) and the recent changes to its implementation. Yung remarks that the job of a program chair is not an error-free process and that even with co-chairs the same mistakes can be made. Moreover, he feels that prospective chairs will end up with a higher overall workload. The Board will monitor the new system closely and make changes where appropriate.

Open Floor.

- Diffie announces that he enjoyed Eurocrypt so much, that he would like it to move to Tallinn permanently.
- Dodis asks whether there is or should be an official policy with regards to student stipends, for instance by better guidelines and setting minimum amounts. Preneel answers that the student registration fee is only half the regular one, moreover for the flagship conferences, students who present their work get their fee waived altogether. There has been generous sponsorship in the past, some of it specifically earmarked to support students (e.g., by Qualcomm). Additionally, for certain countries additional funding is available from the IACR. Rose adds that general chairs have considerable freedom in the amount of student support they want to put into their budget (as long as they explicitly budget it). Lipmaa (GC *EC'11*) remarks that 30 out of the 64 students present at *Eurocrypt'11* received a stipend, to which Smart (GC *EC'12*) adds that for *Eurocrypt'12* he expects he can provide stipends for around 40 students (and possibly include central accommodation for a few). Wolf (general co-chair *EC'09*) chimes in that he does not recall denying any student stipend requests for *Eurocrypt'09*.
- Dodis brings up the (concept of) Best Paper Awards (BPA). In general it is good to have the award, but it is hard to determine at submission time which papers will stand the test of time. He suggests an award to span a period of time in the past, say an award for the best paper from 2000 to 2005.

  Wolf wonders whether such an award could be citation based, to which Dodis adds that then there would be no need for a committee. Kiayias observes that there is substantial overhead for a PC to make a

Date: Talinn, 14 May 2011.

good BPA decision; with the advantage of five year's hindsight it would be much easier for a PC. He also suggest it might be better to do a best student (as main author) paper award.

Lindell reminds people that one of the aims of the BPAs is to help students and young faculty to achieve tenure. It is important to avoid embarassing choices. Yung adds that it is the nature of science (that it is hard to predict eventual impact, say) and that the role is that somebody will win, but that the rest does not loose. Moreover, for very long term recognition, the IACR has introduced its Fellowship program.

Preneel suggests to close the discussion, but invites anyone with suggestions for other/additional awards to come up with a concrete proposal (including for instance sponsorship).

- Pieprzyk informs whether there have been any movements to integrate the CACR (Chinese Association for Cryptologic Research) and other local organizations into the IACR. Preneel responds that there are no recent movements, but that the IACR (and its Board) remains committed to assist when possible. A formal relationship is still far away.

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