MINUTES IACR MEMBERSHIP MEETING *EUROCRYPT'15* (FOR APPROVAL)

SOFIA, 29 APRIL 2015

Opening. At 16.02 Cachin opens the meeting. He begins by giving an overview of the IACR and its activities. In particular, he draws attention to Mike Rosulek joining as Communications Secretary and Yu Yu as webmaster. He highlights a number of areas where the IACR could benefit from additional volunteer.

Treasurer's Report. Rose presents a preliminary financial report for 2014, highlighting a wonderful grant from Cryptography Research Inc. and explaining how the Board intends to use the sponsorship for support of students.

Membership Secretary. Cachin presents shelat's membership report, highlighting some recent trends.

Conferences and publications. Cachin recalls that the field has grown a lot, leading to a number of changes.

Parallel Sessions. Cachin explains the Board's decision to organize parallel sessions as a trial for a year, followed by a membership vote. He gives the membership an opportunity to discuss.

Rijmen believes it is definitely good to have more papers but wonders whether parallel tracks are the only or best solutions to make it happen. However he has no idea about how to implement an increase of throughput differently.

Yung thinks that since we started the parallel sessions, there is a way to extend a little bit. It all depends on quality and it means there is more grey area to accept or reject papers by the committee. One thing that is avoided by a larger number of papers is infighting between different subcommunities within the PC.

Wichs wants to go back to single track. Many people prefer parallel tracks.

Submission Format. Cachin explains that the Board has decided to work with Program Chairs to harmonize the format of submissions. Submissions should have the same format as the publications, with a fixed page limit of 30 pages (shorter papers are still more than welcome). This would make it more transparent to readers what the submission was that was reviewed.

Smart explains that the Appendix will go before the bibliography, but authors can still send supplementary material.

Camenisch explains the FOCS model where one had to submit two versions: a 12 page version to review (and publish) plus a full version additionally. Yung believes that 12 page FOCS format is similar to 30 page LNCS.

Publisher. Cachin explains that the current contract with Springer runs out at the end of 2016. The FSE Steering Committee intends to move away from their current LNCS postproceedings model and instead use a journal model with four deadlines a year and an annual standing program committee. The review process will be multi-round, e.g. reviews and resubmissions of the paper.

PETS has adopted such a model in 2015. Orlandi was on the committee of PETS and wonders whether we should get feedback from them as they had some experience. Smart highlights the role of the FSE Steering Committee and that the FSE Steering Committee is already talking to PETS. Benaloh explains that JETS (Journal of Election Technology and Systems) is in the third year with such a model and the transition is a bit difficult but working well. Bernstein asks for clarification. Benaloh explains difficulties with getting a review system that allows resubmission, that people have to get used with the deadlines and that this implies a different approach for when you get to a conference.

Cachin explains VLDB has adopted the same model several years ago and this seems to work well.

Open Floor.

- Rose remarks that the organization is stable even though the field of security is growing. He wonders what we could do to achieve higher penetration. Smart thinks that attendees at schools could become members. Where are we missing part of the growth? There is a new event called Real World Crypto which is very popular. Paterson explains RWC is only a workshop not a publication venue. The steering committee is actively discussing how they would like to evolve. He mentions that their fees are a lot lower.

- DeGabriele recalls the Copenhagen resolution. Wonders whether IACR should acknowledge and thank Snowden for his efforts, possibly have a panel discussion. He believes we would need to think about it. Rose has a known opinion, but recalls that given the membership composition we would need to have a formal vote. Lange believes we can see what our feelings are. Smart notices there was a panel discussion at CT-RSA and suggests to badger the program chairs.

  There is a straw poll on whether such a political statement should be made, around 30 are in favor, one against, and the rest abstains.
- Bernstein mentions that there is a huge discussion on backdooring crypto. He believes IACR could make a helpful statement about that as well. Benaloh recalls that there will be a report.

Calendar. Cachin gives an update of the calendar.

Closing. Cachin thanks everyone for their attendance and closes the meeting at 16.58.