

MINUTES IACR MEMBERSHIP MEETING *CRYPTO'14*

UCSB, 21 AUGUST 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.

He thanks Christopher Wolf, who resigned from his position, for his dedication as Newsletter Editor/Communications Secretary over the years. He welcomes Mike Rosulek and Yu Yu as the new Communications team.

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

- Reyzin argues against parallel sessions: It is human nature to form cliques, where scientific accomplishment is judged on social standing. Forcing people to listen to others helps to break up (and hinders the creation of) any cliques. He believes that cliques take time to grow, and with it a split in the community to form. From this perspective he considers the experiment a dangerous move as the implications will not be understood in one year. Dodis agrees with Reyzin and wonders why the experiment with longer days is not supported. (On a positive note, he guarantees that *TCC'15* will not have parallel sessions.)
- McCurley feels that the workshop are a form of parallel sessions already. Ferguson supports parallel sessions as he believes it would enable different cliques to all go to the same conference. Someone remarks that clique forming has already taken place because people skip talks and he believes there is no massive difference between parallel sessions or skipped sessions.
- Ishai suggests to let the program co-chairs decide on parallel sessions for their respective conference.
- Kelsey asks if we might get videorecording for all talks to facilitate catching up on missed talks. For *Crypto* this is already standard, for the other flagship conferences this is not yet the case.
- Desmedt likes *Eurocrypt*'s tendency to accept fewer papers (than *Crypto* and *Asiacrypt*) as he claims it leads to a good Google scholar ranking.

There is a quick show of hands indicating a clear majority in favour of a one year experiment with parallel session, but there this also a significant minority against. The experiment will be implemented, but it is stressed that after one year there will be membership vote on the continuation of parallel sessions.

Publications. Smart discusses the future of IACR publications, concentrating on the question of how conference submissions should be formatted. He argues that submissions should be as similar as possible to the final publication, including page limitations. Authors will still be able to submit supplementary material (e.g. proofs or source code) for the program committee's benefit. He gives the membership an opportunity to discuss.

Schroeppel remarks that the extent to which (various parts of the) supplementary material have been reviewed should be clearly marked. Bernstein believes it is a good idea not to put a (size) limit on the supplementary material, to avoid authors claiming a lack of space for including full proofs etc.

A number of quick straw polls demonstrate a clear majority in favour of a submission format that matches the publication, a reasonable majority supports a uniform page limit for all IACR conferences imposed by the Board. However there is no clear indication what would be a desirable page limit.

Smart concludes by presenting the Board's encouragement of sticky reviews, by allowing authors to submit a (partial) rebuttal of past reviews as part of the supplementary material of a resubmission in case their paper was previously rejected.

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

Membership Secretary. Cachin presents shelat's slides.

Open Floor. There are no further comments or questions from the floor.

Closing. Cachin thanks everyone for their attendance and closes the meeting at 17.46.