

## MINUTES IACR MEMBERSHIP MEETING *CRYPTO'16*

UCSB, SANTA BARBARA, 18 AUGUST 2016

**Opening.** At 16.43 Cachin opens the meeting. He hands over to Rose.

**Treasurer's Report.** Rose presents the financial report of 2014.

**President's Overview.** Cachin gives an overview of the IACR, including its membership, publications, and activities. In particular he draws attention to a number of recent changes.

From a personnel perspective, he points out that there are four Officer positions and three Director positions up for election this year. He mentions that at the end of the year, Kenny Paterson will take over as Editor-in-Chief of the Journal of Cryptology from Ivan Damgård and he thanks Damgård for his service. Moreover, Tancrede Lepoint has joined as IACR's ePrint Archive editor in Nigel Smart's stead.

**Conferences and publications.** Cachin highlights the change from proceedings to the *Transactions of Symmetric Cryptology* for *FSE*.

Following a remark about the IACR archive, Naor points out that IACR bought the copyright for the Plenum Press published version of *Crypto*; however Desmedt believes Springer bought these rights. Cachin answers he will investigate.

Cachin explains that with the move to parallel sessions (for General Conferences), making available recordings of presentations and the presentation material become an increasingly useful service. For this reason, the Board suggests to make the recording and release of presentations mandatory. He opens the floor for comments.

- (1) Desmedt thinks that for contributed research papers it is a very good idea, but that for invited talks it should be possible to make an exception. Smart clarifies that the Board agrees with this perspective.
- (2) McCurley perceives a gender bias regarding the format presenters might prefer for the recordings; he believes that slides with audio is the preferable option. Moreover, he insists that "one talk one file" is the only viable format. Cachin personally prefers to have video for the presenters as well.
- (3) LaMacchia gives his perspective as General Chair of *Crypto'16*. He mentions that the format is currently up to the General Chair. He also mentions that for this conference only a few people opted out. He believes that releasing recordings and presentation material is part of the IACR's mission of making academic research available.
- (4) Kelsey supports the initiative. Even if he has seen the talk, when he later reads the paper he likes to be able to fall back on the original presentation. Kelsey points out that capturing the slides as they are sent to the screen misses the author's interaction with the slides, e.g. by using a laser pointer.
- (5) Ferguson believes in exceptions by common sense.
- (6) Keller believes that it should be possible to not publish talks if something unforeseen goes wrong during the talk.

Caching asks for a show of hand to indicate support for mandatory recording etc. There is a clear majority in favour, with only a handful of people explicitly against the initiative (abstentions were not explicitly asked for).

Cachin notes that providing this service does rely on people and calls for volunteers.

*Open Floor.*

- Desmedt wonders why *Crypto* attendees who only want to go to a few CHES presentations (yet still leave on Thursday), have to pay almost the full CHES registration fee. LaMacchia explains how registration fees are set for the respective conferences in order to break even. He explains that this includes fixed costs such as room rental. The discount for those fully attending both conferences is still sponsored.
- Teague thanks those IACR members who signed the petition against Australia's cryptology laws.

**Calendar.** Cachin gives an update of the future events sponsored by the IACR.

**Closing.** Cachin thanks everyone for their attendance and closes the meeting at 17.31.

**Postscript.** McCurley requests program chairs to use full names for program committee members and to clearly publish best paper awards.