MINUTES IACR MEMBERSHIP MEETING *CRYPTO'12*

UCSB, 22 AUGUST 2012

Opening. At 16.55 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. He mentions that sponsorship has gone up and is used primarily for stipends for students to attend IACR events. He thanks Yiqun Lisa Yin (general chair *Crypto'12*) for doing a wonderful job pursuing NSF funding and for distributing a large number of student fee waivers.

Membership Secretary. Preneel mentions that abhi shelat (the current membership secretary) could not make it. He thanks the previous membership secretary Shai Halevi for his dedicated and continued service to the IACR.

Website. Preneel draws attention to the recently revised website. He thanks Kevin McCurley, Christian Cachin, Nigel Smart, and Christopher Wolf for the efforts that went into designing and implementing the changes.

Awards. Preneel presents an award to *Crypto'12* General Chair Yiqun Lisa Yin. Preneel subsequently presents an award to *Crypto'12* Program co-Chairs Rei Safavi-Naini and Ran Canetti. On behalf of the Program co-Chairs, Rei Safavi-Naini briefly reports on the process that led to the scientific program of *Crypto'12*. She thanks the program committee for its hard work, as well as advisors Shai Halevi, Tal Rabin, and Phil Rogaway, general chair Yiqun Lisa Yin, and all authors, presenters, and participants.

Publications. Preneel explains the current situation and thanks archivist Hilarie Orman and Journal Editor-in-Chief Matthew Franklin for their hard work. He continues with the plans for future publications. Negotiations with Springer for a new contract for the proceedings will be completed by August 31. This contract will provide green open access to IACR authors.

Board decisions. Preneel draws attention to a few recent Board decisions, related to the bandwidth and balance of the conference programs, the availability of ethics guidelines, and the recent institution of an audit committee.

Open Floor.

- McCurley thanks Preneel for his extensive work related to the (re)negotiation of a publishing contract, as well as Alfred Hofmann from Springer for his constructive position towards IACR.
- Orman expresses her disagreement with the currently proposed agreement as she is disappointed in the outcome and the rate of progress. She believes clear, open access is an important way of satisfying the needs of the academic community.
- Rivest notes that many professional societies are experimenting with merging journals and proceedings (aka journferences). Preneel responds that the Board is aware of this development, but that it has been deemed too early to move to this model. There will be a gap in ISI indexing and significant uncertainty how severe this gap will be. Cachin mentions that VLDB has adopted a journference publication model.
- Diffie notices that to become a fellow you need to be IACR member which means senior, retired people often have to be made members anew, despite having paid their (financial) dues, e.g., through years of conference attendance. He suggests to consider a life time IACR membership. Preneel thinks this is a good suggestion. It might combine well with the anticipated reduction in the membership fee when paper versions of the Journal become opt-in.
- Ferguson asks whether the Board has considered to buy out Springer for the back catalogue. Preneel answers that this has been attempted, but in vain. The option for authors to pay for golden open access for their papers will be for new publications only.
- Kelsey refers to Desmedt's rump session talk related to authors citing eprint versions instead of formal publications. He suggests that reviewers should check citations to include the official publication. Preneel responds that there will be a mandated footnote in the author's version to the official publication. Canetti mentions that in the online *Crypto'12* program there are links to the full version.
- Kelsey notes that there are many cryptanalytic attacks that are hard to verify in full and wonders whether there are guidelines about how authors can verify part of the attack. Preneel answers that this is an academic issue and he refers Kelsey to the various Program Chairs.

Closing. Preneel thanks everyone for their attendance and closes the meeting at 17:58.