MINUTES IACR BOARD MEETING *VIRTUAL-5 '20*

1 JULY 2020

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h05 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 22 full time attendees with Reyzin holding proxy for Kolesnikov and LaMacchia holding proxy for Stebila. Yung holds the proxy for Standaert when he steps out.

1.2. **Review and approval of agenda.** The agenda is approved, with the understanding that the meeting will be held in an order slightly deviating from the agenda (as certain items have scheduling constraints). These minutes are reordered to the original agenda for consistency.

1.2.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2020-2022); Shai Halevi (Vice President 2020-2022, *TCC* Steering Committee); Brian LaMacchia (Treasurer 2020-2022); Joppe Bos (Secretary 2020-2022); Masayuki Abe (Director 2018-2020); Marc Fischlin (Director 2020-2021); Nadia Heninger (Director 2019-2021); Tancrède Lepoint (Director 2018-2020). Anna Lysyanskaya (Director 2019-2021); Bart Preneel (Director 2020-2022, *FSE* Steering Committee); Peter Schwabe (Director 2020-2022); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee); Moti Yung (Director 2018-2020, *PKC* Steering Committee).

Attendees (Appointed). Foteini Baldimtsi (Communications Secretary (2019-2022)); Lejla Batina (*Eurocrypt'20/'21* General Chair (2019-2021)); Colin Boyd (*Eurocrypt'22* General Chair previously *Eurocrypt'21* General Chair (2020-2022)); Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Kwangjo Kim, (*Asiacrypt'20* General Chair (2019-2020)); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2020, *RWC* Steering Committee); Leo Reyzin (*Crypto'20* General Chair (2019-2020));

Attendees (Representatives and Others). Kevin S. McCurley (Database Administrator). Yu Yu (Webmaster).

Absentees (Appointed). Douglas Stebila (Membership Secretary (2017-2020)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)).

Absentees (Representatives and Others). Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison);

1.3. **Approve minutes from last BoD virtual meeting.** The President thanks the Secretary for the completion of the minutes which have been shared before the Board Meeting. Abdalla calls for a vote to approve the minutes.

Decision 1 (unanimous)**.** *The Board approves the Minutes of the IACR Board Meeting Virtual-4 '20.*

2. Appointments, committees, and policies

2.1. ***CRYPTO* program co-chair appointment.** The President recalls that we need to appoint a Program Co-Chair for *Crypto'22* which serves together with Thomas Shrimpton. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 2. *Yevgeniy Dodis is appointed Program Co-Chair for Crypto'22. [Dodis subsequently accepted.]*

2.2. ***Asiacrypt* program co-chair appointment.** The President recalls that we need to appoint a Program Co-Chair for *Asiacrypt'22*, the second Program Co-Chair will be appointed in the next Board Meeting. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Shweta Agrawal is appointed Program Co-Chair for Asiacrypt'22. [Agrawal subsequently accepted.]*

3. STATUS OF CONFERENCES

3.1. **Update on *Crypto* and affiliated events.** Reyzin provides an update to the Board: things are moving forward and he is pleased that the Distinguished Lecture will take place. The Workshops will take place during the weekend before *Crypto* in order to avoid a clash with *Usenix*. Multiple directions are investigated how to best organize the social events. Even though the conference will be online the sponsorship looks good. The President asks if this means we can afford free registrations. Reyzin hopes so and will take this up with the Treasurer.

McCurley explains he performed a lot of changes to HotCRP for this *Crypto*. We need to discuss the way forward at the next Board Meeting.

The President provides a quick update regarding *TCC* which decided to go virtual as well.

4. TOPICS

4.1. **New journal proposal (Transactions of the IACR).** The President recalls that during the last Board Meeting there was no time to discuss this in detail. The current proposal was shared with the Board by Nigel Smart. The President gives a quick summary of the proposal and the motivations of the members behind the proposal.

The President asks Paterson as the JoC EiC about his opinion. Paterson recalls that this journal aims at providing a review in three months: JoC is not there yet. The quality bar is indeed higher for JoC but this proposal provides a useful complement.

Schwabe is concerned about the potential effect on IACR events and other smaller (non-IACR) conferences and workshops. The President states that we haven't had a new IACR journal for a long time and that the throughput of new papers has indeed increased. He really likes this initiative and idea but the implementation of it might be a problem.

Preneel states that we need to carefully consider this proposal because there might be a significant risk of competition. However, the current trend is to move to hybrid models (like for *CHES* and *FSE*). This proposal looks like the hybrid model but without a conference. We need to consider how this aligns with *CHES* and *FSE* since this looks like direct competition where presentation of the work is not required. Preneel is not concerned about small local events. Like in the mathematics community, these smaller workshops will survive with good invited speakers and serve a different purpose. The current guideline of accept by default even if there are no reviews submitted is unacceptable and a show stopper.

Heninger is generally in favor of this new proposal. She is also less concerned about the impact on smaller events. *RWC* shows that talks do attract people. She agrees with Preneel about the default accept rule when reviewers do not respond: this sounds wrong. Also the requirement to resubmit by the next deadline sound suboptimal: think for instance about maternity leave. It is, however, good to disconnect the papers from the conferences.

Lysyanskaya supports this proposal in spirit. She wonders what the next steps are.

Halevi is supportive to try different publication methods. This proposal looks like ePrint with light reviewing and is an interesting approach. Yung agrees, this can be good when implemented right. Schwabe is worried that if we decouple giving presentations from accepted papers then some people might have trouble traveling. Moreover, just selecting good presenters to give talks might discriminate against non-native English speakers. As he understood, the plan for the reviewing for this journal is quite serious so no light reviewing. This is realized by avoiding sub-reviewers.

McCurley wonders about the operational aspects. What software will be used to realize all this new requirements and wishes? The Treasurer also recalls that there is no financial model provided (including secondary effects to our conferences). He is worried about reduction of travel to conferences from industry. This is possibly better integrated with our current transaction model.

The President thanks the Board for this discussion and summarizes the opinion of the Board: there is general support for this proposal but there are general concerns about implementation aspects and impact. He will start a Committee to work this out in more detail. People interested in joining this Committee are invited to contact the President.

5. CLOSING MATTERS

Abdalla closes the meeting at 18h01 CEST.