MINUTES IACR BOARD MEETING *VIRTUAL-6 '20*

13 AUGUST 2020

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 16h06 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 19 full time attendees with Batina holding proxy for Schwabe, Yung for Standaert and Stebila for Paterson. Reyzin joins the meeting from 17h15 to 17h45 to participate in the *Crypto 2020* update.

Kim requests to add a status update of *Asiacrypt'20* to the agenda.

These minutes are reordered to the original agenda for consistency.

1.1.1. *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); 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)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)). Leo Reyzin (*Crypto'20* General Chair (2019-2020)); Douglas Stebila (Membership Secretary (2017-2020));

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

Absentees (Elected). Peter Schwabe (Director 2020-2022); Francois-Xavier Standaert (Director 2020-2022, *CHES* Steering Committee);

Absentees (Appointed). Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2020, *RWC* Steering Committee);

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

1.2. **Approve minutes from last BoD virtual meeting.** The President thanks the Secretary for the completion of the minutes which have been shared before the current 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-5 '20.*

2. Appointments, committees, and policies

2.1. ***Asiacrypt 2022* program co-chair appointment.** The President recalls that we need to appoint a second Program Co-Chair for *Asiacrypt'22* who will serve with Shweta Agrawal. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 2. *Dongdai Lin is appointed Program Co-Chair for Asiacrypt'22. [Lin subsequently accepted.]*

2.2. ***Crypto 2022* General Chair appointment.** The President recalls that we need to appoint a General Chair for *Crypto'22*. Several excellent candidates are nominated, and after discussion a candidate is selected.

Decision 3. *Allison Bishop is appointed Genercal Chair for Crypto'22. [Bishop subsequently accepted.]*

3. Status of conferences

3.1. **Update on *Crypto 2020* and affiliated events.** McCurley summarizes there are no pending issues. Currently they are busy with the uploading and preparing of the videos of the presentations.

The affiliated events are more work than expected. There are some concerns about the mandatory registration for *Crypto* in order to attend the affiliated events. Yung suggests that the university professors who run the affiliated events should host this on the university domain. The President disagrees, the affiliated events and the main event should look as unified as possible. McCurley suggests we need guidelines for the people running the affiliated events to avoid confusion.

For *Crypto 2020* we just reached 900 registrations and received substantial sponsorship. Thanks to the previous experience of running virtual events all is going very well.

LaMacchia wonders what it means to be an affiliated event, is this officially part of the IACR or not? Heninger suggests that for the invited talks at the affiliated events it might come as a surprise that they need to pay for the IACR membership fee in order to attend. There follows a discussion if we can use the sponsorship money to cover for the invited speakers. The President suggests to move on and discuss this in the *Crypto* meeting later this week.

3.2. ***Asiacrypt 2020* Update.** Kim summarizes that everything is under way for *Asiacrypt 2020*. They have found local sponsors and the plan is to have a hybrid model with both local and remote attendance. Stebila states that we should avoid having part of the scientific program not being available for everybody. McCurley highlights that the organizers should choose a timeline that is favorable for the people in Asia. He thinks the hybrid model sounds very scary, how can we realize this in practice? Do we foresee interactions between the physical and virtual attendees? The President recalls that the idea is to have an additional social event for the people who physically attend. Heninger asks if the venue for *Asiacrypt* is shifted by one year since we go virtual this year? Kim cannot answer this question right now.

4. Other Topics

4.1. **IACR Financial Update.** The Treasurer gives a quick update due to time-constraints. *Eurocrypt 2020* made money because of the additional sponsorship. This will be used to cover for expenses in 2021. No other urgent matters to report.

4.2. **IACR dissertation award program.** Fischlin provides a summary of his proposal for an IACR dissertation award which was shared with the Board. This should be easy to accomplish and not much work. We probably need a Committee which selects the dissertations and hand out certificates. The President agrees that this should be easy to do and supports this initiative. Lepoint asks if this is one award a year or if multiple dissertations can win? The details of this proposal need to be worked out.

Decision 4 (unanimous)**.** *The Board wants to pursue the idea of creating the IACR dissertation award program.*

A Committee needs to be formed. Besides Fischlin, Abe volunteers to be part of this Committee.

4.3. **HotCRP.** McCurley summarizes that we cannot support any changes in HotCRP: the current situation is a real mess. The main conclusion is that we may need to choose between giving up some IACR features in a conference management software, or pursue another system altogether, neither of theses options is desirable

4.4. **New journal update (Transactions of the IACR).** The President recalls that a subcommittee has been created but not much has happened so far. It is important to decide on next steps and choose a Chair and Co-Chair to move this forward. The President suggests Preneel to lead this Committee. Preneel mentions that the JoC EiC-elect is also from the KU Leuven and they don't want to appear as if they want to take over IACR publishing.

Lysyanskaya suggests Yung. Yung thanks but he has no time to take on this additonal role.

The President suggests he will try and find a good chair offline. It is also important to invite some members of the proposal to join this committee: it will be up to them who can join. McCurley suggests we first select a chair and form the committee before sending this invitation. The President agrees and mentions he will talk about this proposal in the *Crypto* Membership Meeting.

5. Closing Matters

Abdalla closes the meeting at 18h07 CEST.