

# MINUTES IACR BOARD MEETING VIRTUAL-7 '20

8 SEPTEMBER 2020

## 1. OPENING MATTERS

**1.1. Welcome, roll of attendees, identification of proxies.** At 23h05 CEST Abdalla opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 18 full time attendees with Lysyanskaya holding proxy for Reyzin when absent and vice-versa: Reyzin joins at 00h19 and Lysyanskaya leaves at 00h30. 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); Nadia Heninger (Director 2019-2021); Tancrede 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)); Colin Boyd (*Eurocrypt'22* General Chair previously *Eurocrypt'21* General Chair (2020-2022)); Vladimir Kolesnikov (*Crypto'21* General Chair (2020-2021)). Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2020, *RWC* Steering Committee); 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). Marc Fischlin (Director 2020-2021);

*Absentees* (Appointed). Lejla Batina (*Eurocrypt'20/21* General Chair (2019-2021)); Jian Guo (*Asiacrypt'21* General Chair (2020-2021)); Kwangjo Kim, (*Asiacrypt'20* General Chair (2019-2020));

*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-6 '20.*

## 2. APPOINTMENTS, COMMITTEES, AND POLICIES

**2.1. Asiacrypt 2022.** Bo-Yin Yang presents the proposal by Kai-Min Chung and himself for *Asiacrypt 2020* in Taipei, Taiwan. The Presidents asks if the budget includes access to all rooms presented. This is confirmed by Yang, this includes access to the entire 3rd and 4th floor. Stebila remarks that we might need to accommodate up to 350 participants based on previous years.

**Decision 2** (unanimous). *The Board follows the recommendation from the Asiacrypt steering committee and accepts the proposal for Asiacrypt 2022 in Taipei, Taiwan with Kai-Min Chung and Bo-Yin Yang as General Co-Chairs.*

It is confirmed that Yang will join the board as a representative board member.

**2.2. Membership secretary (re-)appointment.** The President recalls that Stebila's term as Membership Secretary will end this year. He has been doing a really great job and the President already approached Stebila if he is interested to server another term. Stebila feels another full-term is too much but he is willing to stay for another 2 years.

**Decision 3** (unanimous). *Douglas Stebila is re-appointed as membership secretary for another two years (2021-2022).*

### 3. STATUS OF CONFERENCES

The President asks for various updates on the forthcoming conferences.

McCurley explains that everything is going smoothly for *CHES*. The videos are being transferred to YouTube. Schwabe agrees that everything is going as planned. The President remarks that the virtual booth for sponsors is a good exercise for the *RWC* symposium. McCurley remarked that the social application has changed quite significantly for *CHES*.

The *RWC* Steering Committee will meet this week. It is investigated if *RWC* will migrate to a virtual event. No decision has been taken.

Preneel recalls that *FSE* was one of the first conferences to be postponed. The event was postponed to November 2020. The hotel will open mid-September but is hard to reach. If we decide to go virtual then we will lose the down-payment. Yung remarks that it does not look wise to go for a physical event.

The President recalls that *Asiacrypt 2020* will be virtual.

For *TCC* everything is on schedule.

### 4. TOPICS

**4.1. IACR Online Seminars.** The President recalls that this topic was briefly mentioned in a previous Board meeting. The idea is to use the existing infrastructure to record interesting seminars. The Presidents thinks that, due to all the ongoing tasks and virtual events, this topic will not start before January. Lysyanskaya suggests that we could start with seminars with the newly selected Fellows. Reyzin remarks that live sessions have their benefits over recorded seminars and he wonders if we could have a live session for the IACR members. The President raises the issue of how to implement this in practice. Everyone can later watch the seminars on YouTube, even non- members. Not clear yet if we want to restrict this. The Membership Secretary and the President highlight that we want to be as inclusive as possible

**Decision 4.** *There is support for the IACR Online Seminars and the Board decides that we continue to investigate this initiative.*

**4.2. New journal subcommittee chair appointment.** The President has the action item to look for a chair of the New Journal Committee. There was some discussion who wants to chair this Committee but it seems nobody has time. Bos volunteered to co-chair but he states he prefers someone with publishing experience to co-chair with him. It is suggested to ask Christian Cachin to co-chair this New Journal Committee (Cachin subsequently accepted).

**4.3. IACR Financial Update.** The Treasurer gives an overview of the state of the financial situation. The IACR is doing fine, all the details have been shared in the repository. Heninger asks about the financial impact of going virtual this year. So far, the membership is at a record high and the virtual events are actually making money due to the arranged sponsorship agreements.

McCurley informs about the liability for *Eurocrypt* since he has not much confidence that physical events will be back to normal any time soon. The Treasurer explains that we paid a seed fund to the GC. We could be on the hook for large cancellation fees: details not at hand since the Treasurer does not have the details on the *Eurocrypt* contract. The Board agrees that we need to investigate the current contracts with respect to any potential fees for the postponed events. It is suggested that we need to add to the General Chair guidelines that a copy of the contract with the venue is shared with the Treasurer and the President.

**4.4. Online advertising discussion.** LaMacchia explains a request from an NSF SBIR recipient that is trying to develop Google advertising tools for non-profits that qualify for advertising grants from Google (for the Google platform). Their tools are aimed at managing a non-profit's advertising campaign to increase the effectiveness of Google grants. The company has suggested that they could help us use such an advertising grant to increase our outreach to researchers in underrepresented areas and minorities.

McCurley states that outreach is a good goal but advertisement might not be the right way to achieve this goal. Preneel agrees, we can potentially do a lot of things in this area. This is a very time-intensive task. Advertisement is not the right tool. Heninger also agrees. However, she suggests that outreach to underrepresented groups is part of the US NSF's broader impact requirements for grants. We could coordinate outreach activities with people who have NSF grants and who have an incentive to spend time on these things. Halevi states that if we want to be more active in this area then someone from the Board needs to invest some time to prepare a proposal.

LaMacchia concludes to not pursue this offer.

### 5. CLOSING MATTERS

Abdalla closes the meeting at 01h06 CEST.